MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE

KHARKIV NATIONAL
UNIVERSITY OF RADIO ELECTRONICS

RADIOTEKHNIKA

All-Ukrainian
interdepartmental scientific and technical collection

ISSN 0485-8972
eISSN 2786-5525

Founded in 1965

I S S U E 2 2 1

Kharkiv
Kharkiv National
University of Radio Electronics
2025

UDC 621.3

The collection is included in the List of scientific professional publications of Ukraine, category «Б», technical and physical-mathematical sciences (approved by orders of the Ministry of Education and Science from 17.03.2020 № 409; from 02.07.2020 № 886; from 24.09.2020 № 1188) by specialties: 105 – Applied Physics and Nanomaterials; 125 – Cybersecurity and information protection; 163 – Biomedical Engineering; 171 – Electronics; 172 – Electronic communications and Radio Engineering; 173 – Avionics; 174 –Automation and Computer-Integrated Technologies and Robotics; 175 – Metrology and information-measuring technique; 176 – Micro- and Nanosystem Technology.

Website: rt.nure.ua

Registration certificate KV № 12098-969 PR dated 14. 12. 2006.

The authors are responsible for the content of the article.

Responsible for the issue: *S.O. Sheiko, PhD, Assoc. prof., I.D. Gorbenko, Dr. Sc. (Tech.), prof.*
Technical Secretary: *O.S. Polyakova.*

Recommended by the Scientific and Technical Council of Kharkiv National University of Radio Electronics, protocol № 5 dated 19.06.2025.

Address of the editorial board: Kharkiv National University of Radio Electronics (NURE), ave. Nauky, 14, Kharkiv, 61166, tel. (0572) 7021-397.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ
УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ

РАДІОТЕХНІКА

Всеукраїнський
міжвідомчий науково-технічний збірник

ISSN 0485-8972
eISSN 2786-5525

Засновано в 1965 р.

В И П У С К 2 2 1

Харків
Харківський національний
університет радіоелектроніки
2025

УДК 621.3

Збірник включено до Переліку наукових фахових видань України, категорія "Б", технічні та фізико-математичні науки (затверджено наказами МОНУ від 17.03.2020 № 409; від 02.07.2020 № 886; від 24.09.2020 № 1188) за спеціальностями: 105 – Прикладна фізика та наноматеріали; 125 – Кібербезпека та захист інформації; 163 – Біомедична інженерія; 171 – Електроніка; 172 – Електронні комунікації та радіотехніка; 173 – Авіоніка; 174 – Автоматизація, комп'ютерно-інтегровані технології та робототехніка; 175 – Метрологія та інформаційно-вимірювальні технології; 176 – Мікро- та наносистемна техніка.

Сайт: rt.nure.ua

Реєстраційне свідоцтво КВ № 12098-969 ПР від 14. 12. 2006.

За зміст статті відповідальні автори.

Відповідальні за випуск: *С.О. Шейко, канд. техн. наук, доц., І.Д. Горбенко, д-р техн. наук, проф.*
Технічний секретар: *О.С. Полякова.*

Рекомендовано Науково-технічною радою Харківського національного університету радіоелектроніки, протокол № 5 від 19.06.2025.

Адреса редакційної колегії: Харківський національний університет радіоелектроніки (ХНУРЕ), просп. Науки, 14, Харків, 61166, тел. (0572) 7021-397.

CONTENT

SYSTEMS AND METHODS OF INFORMATION PROTECTION

INFORMATION TECHNOLOGY

RADIO ELECTRONIC SYSTEMS

PHYSICS OF DEVICES, ELEMENTS AND SYSTEMS

ЗМІСТ

СИСТЕМИ І МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

РАДІОЕЛЕКТРОННІ СИСТЕМИ

ФІЗИКА ПРИЛАДІВ, ЕЛЕМЕНТІВ І СИСТЕМ

УДК 004.056.5 **DOI:10.30837/rt.2025.2.221.01**

І.Д. ГОРБЕНКО, д-р техн. наук О.Г. КАЧКО, канд. техн. наук, Я.А. ДЕРЕВ'ЯНКО

ОПТИМІЗАЦІЯ ОПЕРАЦІЙ ОБЧИСЛЕННЯ ТА ПЕРЕВІРКИ ЦИФРОВОГО ПІДПИСУ ДЛЯ СТАНДАРТУ FIPS 205

Вступ

Наразі суттєві зусилля на міжнародному та національному рівнях зосереджені на створенні практичних квантово-стійких механізмів цифрового підпису (ЦП). Проведено перший етап міжнародного конкурсу PQC [1], підсумком якого являється створення та стандартизація рекомендованих в якості міжнародних таких фіналістів 3 раунду конкурсу постквантових стандартів, але уже в якості федеральних стандартів США:

- FIPS 204, Стандарт ЦП на основі модульної решітки (алгоритм Crystals-Dilithium) [2];
- FIPS 205, Стандарт ЦП без стану на основі геш функції (алгоритм SPHINCS+) [3].

Вказані стандарти визначають схеми ЦП, які покликані протистояти майбутнім квантовим та класичним атакам квантових комп'ютерів, що загрожують безпеці існуючих стандартів. Оскільки ці алгоритми уже стандартизовано, то важливим завданням є дослідження їх побудови та практичної реалізації вимог до складових стандартів: побудови параметрів, генерування ключових пар, вироблення ЦП та їх верифікації тощо. Суттєво його вирішення залежить від покращення цих алгоритмів з точки зору складності (швидкодії), що може бути зведено до оптимізації базових операцій.

У даній статті розглядаються та пропонуються практичні удосконалення щодо оптимізації ЦП для алгоритму FIPS 205 на основі застосування паралельних обчислень, що зводяться в основному до оптимізації алгоритмів гешування shake256, sha256 та sha512. Важливість оптимізації обчислення геш значень пов'язана з тим, що гешування є основною операцією ЕП FIPS 205, а також використовується для FIPS 205.

1. Порівняння продуктивності базових алгоритмів

Аналіз показав, що згідно з класифікацією NIST алгоритми гешування забезпечують криптографічну стійкість алгоритму FIPS-204 на 2, 3, 5 рівнях та 1, 3, 5 рівнях для алгоритму FIPS 205.

Для порівняння стандартизованих алгоритмів ЕП зазвичай застосовують розміри ключових даних, насамперед відкритого ключа, розмір електронного підпису та час виконання основних операцій: генерації ключів, обчислення та перевірки електронного підпису. В табл. 1 та 2 наведені відповідні розміри параметрів для алгоритмів FIPS 204 та FIPS 205. В алгоритмі FIPS 205 передбачено два режими оптимізації[4]:

- за розміром цифрового підпису (режим позначено літерою s);
- часом обчислення цифрового підпису (режим позначено літерою f).

В табл. 2 наведені розміри цифрового підпису для обох режимів.

Таблиця 1

Алгоритм FIPS 204. Розміри ключів та цифрового підпису [2]

Параметри	Криптостійкість λ		
	2	3	5
Довжина секретного ключа	2560	4032	4896
Довжина відкритого ключа	1312	1952	2592
Довжина підпису	2420	3309	4627

Таблиця 2

Алгоритм FIPS 205. Розміри ключів та цифрового підпису [3]

Параметри	Криптостійкість λ					
	1		3		5	
	S	f	s	f	S	F
Довжина секретного ключа	64	64	96	96	128	128
Довжина відкритого ключа	32	32	48	48	64	64
Довжина підпису	7856	17088	16224	35664	29 792	49 856

Порівняння табл. 1 та 2 показує, що криптографічна стійкість для обох алгоритмів приблизно співпадає. При цьому розмір відкритого ключа для алгоритму FIPS 205 суттєво менший, що особливо важливо, оскільки саме відкриті ключі зберігаються в сертифікаті відкритого ключа чи передаються разом з підписаним повідомленням. Розмір ЦП для алгоритму FIPS 205 суттєво більший ніж для алгоритму FIPS 204, що також важливо враховувати, оскільки підпис передається разом з самим повідомленням.

Інформація щодо продуктивності алгоритмів FIPS 204 та FIPS 205, взята з технічної документації авторських реалізацій [5, 6] відповідно, наведена в табл. 3 (FIPS 204), 4 та 5 (FIPS 205). Продуктивність виміряється кількістю тактів процесора, що забезпечує мінімальну залежність від тактової частоти процесору.

Таблиця 3

Алгоритм FIPS 204. Продуктивність (Для AVX2 (Skylake)) [5]

Параметри	Криптостійкість λ		
	2	3	5
Медіана циклів для генерації	124031	256403	208050
Медіана циклів для підпису	259172	428587	538986
Середня кількість циклів для підпису	333013	529106	642192
Медіана циклів для перевірки	118412	179424	279936

Таблиця 4

Алгоритм FIPS 205. Продуктивність (3.1 GHz Intel Xeon E3-1220 CPU (Haswell), AVX2). Shake [6]

Параметри	Криптостійкість λ					
	1		3		5	
	s	f	s	s	f	s
Генерація	143 900 796	2 249 444	206 105 502	3 220 902	136 190 230	8 535 534
Підписання	1 102 470 520	56 933 788	1 910 461 606	89 875 552	1 650 717 926	176 951 378
Перевірка підпису	1 189 102	3 346 068	1 653 314	4 783 424	2 559 892	5 030 988

Таблиця 5

Алгоритм FIPS 205. Продуктивність (3.1 GHz Intel Xeon E3-1220 CPU (Haswell), AVX2). SHA2 [6]

Параметри	Криптостійкість λ					
	1		3		5	
	s	f	s	f	s	f
Генерація	84 964 790	1 334 220	125 310 788	1 928 970	80 943 202	5 067 546
Підписання	644 740 090	33 651 546	1 246 378 060	55 320 742	1 025 721 040	109 104 452
Перевірка підпису	861 478	2 150 290	1 444 030	3 492 210	1 986 974	3 559 052

Для алгоритму FIPS 204 кількість тактів для обчислення ЦП залежить від кількості повернень, тому в таблиці наведено мінімальне значення (Медіана циклів для підпису, немає повернень) та середнє значення (Середня кількість циклів для підпису).

Для алгоритму FIPS 205 кількість тактів для усіх операцій суттєво залежить від базового алгоритму для обчислення, тому результати наведені для обох варіантів:

- в табл. 4 – для варіанту застосування shake;
- в табл. 5 – для варіанту застосування sha2.

Не зважаючи на те, що результати отримані для різних процесорів, порівняння результатів показує, що за продуктивністю алгоритм FIPS 205 суттєво поступається алгоритму FIPS 204 для будь якої базової операції.

У наступному пункті розглядається оптимізація обчислення ЦП для алгоритму FIPS 205 за рахунок застосування паралельних обчислень.

2. Алгоритм обчислення ЦП для FIPS 205

У алгоритмі ЦП застосовуютьсяє наступні параметри:

n – довжина рядка байтів;

d – кількість рівнів розширених дерев Merkle (далі дерев Merkle).

h' – висота дерева Merkle;

h – загальна висота гіпер дерева (h = h' · d);

m – довжина дайджесту повідомлення, включає:

- інформацію для k листів завдовжки a бітів для кожного листа, всього k · a бітів;
- біти для завдання номеру найнижчого рівня гіпер дереву, який дорівнює h - h';
- біти для завдання номеру листа (максимальний номер h' - 1) .

len – загальна кількість листів в дереві Merkle;

k – кількість дерев в лісі.

a – Визначає загальну кількість листків t = 2^a для дерева FORS.

Вхідні дані в алгоритм :

msg – повідомлення довжини msg_len;

sk – секретний ключ. який включає:

- *SK_seed* (seed, випадковий рядок байтів завдовжки n),
- *SK_prf* (prf, випадковий рядок байтів завдовжки n)),
- *PK_seed* (seed, випадковий рядок байтів завдовжки n),
- *PK_root* (корінь геш дерева, рядок байтів завдовжки n)
- *opt_rand* – випадковий рядок байтів або PK_seed

Вихідні дані алгоритму:

sig – електронний підпис, який складається з:

- рандомізованого повідомлення *R;*
- підпису для лісу завдовжки $k \cdot (1 + a) \cdot n$ байтів;
- підпису для гіпер дерева завдовжки $(h + d \cdot len) \cdot n$ байтів.

Виконання алгоритму здійснюється у такій послідовності:

1. Рандомізація вхідного повідомлення (функція PRF_{msg} Стандарту).

Для рандомізації *msg* застосовують компонент секретного ключа *SK_prf, opt_rand*

$R = PRF_{msg}$ *(SK_prf, opt_rand, msg)*

2. Обчислення дайджесту для повідомлення (функція H_{msg} Стандарту) – рядок байтів завдовжки *m*

3 Обчислення по дайджесту *k* листів, номера рівня гіпердерева (номер дерева), та номера листа. Формування інформаційної структури, в яку записуються значення типу, яке відповідає *FORS_TREE*, значення номера дереву та номера листа в дереві (кроки 6-13 Стандарту)

4. Обчислення підпису для лісу SIG_{fors} (функція *fors_sign* Стандарту). Отримане значення записується як компонент електронного підпису. Цей підпис для дерева гешів включає значення вузлів і шляху аутентифікації

5. Обчислення відкритого ключа для гіпердерева за електронним підписом SIG_{fors} (функція *fors_pkFromSig* Стандарту). Ця функція за значеннями вузлів та шляху аутентифікації обчислює корінь відповідного дерева.

6. Обчислення підпису для гіпердерева (функція *ht_sign* Стандарту) Цей підпис додається як останній компонент електронного підпису.

Кожний наступний крок застосовує результат обчислення попереднього кроку, тому усі кроки необхідно виконувати послідовно. Необхідно розглянути можливість оптимізації кожного кроку окремо.

В наступному пункті розглянуто можливість паралельного виконання для базових операцій алгоритму FIPS 205.

3. Базові операції алгоритму FIPS 205

В якості базових операцій алгоритм застосовує операції, які в стандарті позначені як PRF_{msg}, H_{msg}, *PRF, Tl, H і F*. Їх виконання базується на обчисленні геш значень (алгоритми SHA2-256 та SHA2-512) або на алгоритмі SHAKE256.

Для алгоритму обчислення ЦП було визначено кількість застосовування базових операцій в залежності від параметрів алгоритмів (табл. 6).

Таблиця 6

Обчислення електронного підпису. Кількість викликів базових функцій

Функція	n = 16		n = 24		n= 32	
	s	f	s	f	s	F
PRF_{msg}	1	1	1	1	1	1
PRF	182784	8272	461312	17424	497664	36144
Tl	3584	176	3584	176	2048	272
H	60898	2230	282079	8566	362458	18136
F	1938674	94212	3019883	142683	2418193	290770
H_{msg}	1	1	1	1	1	1

Як видно з табл. 6, функції PRF_{msg}, H_{msg} викликаються тільки один раз, а функції PRF, Tl, H, F викликаються багаторазово, тому далі буде розглянуто оптимізацію саме цих функцій.

3.1. Алгоритм shake та його оптимізація

Для усіх наборів параметрів застосовують алгоритм shake256. Розмір блоку BLOCKSIZE (BS) для цього алгоритму дорівнює 136 байтів, внутрішній стан задається масивом s з 25 порцій даних завдовжки 64 біта.

Алгоритм shake є компонентом алгоритмів SHA3. Для завдання даних застосовується формат LITTLE-ENDIAN.

Усі операції запису в масив s фактично виконують операцію додавання по модулю 2 нового значення до поточного.

1. Ініціалізація (init).
   s[i] = 0 (I = 0, 1, 2, …, 25)
2. Накопичення для повних блоків (*absorb*)
   Поки розмір вхідних даних перевищує *BS* то
   Запис наступної порції в масив *s ^= por[i]*
   Перемішування для масиву *s*:
   s = KeccakF1600_StatePermute(s);
   Коректування масиву s з урахуванням неповної порції
   s ^= por
3. Кінцева обробка *(finalize).*
   Запис значення 0x1f безпосередньо після останнього біту неповної порції
   s[i] ^= 0x1F
   Запис в *s[16]* значення 2^{63}
   s[16] ^= 2^{63}
   Перемішування для масиву *s*

В оригінальній реалізації алгоритму враховується можливість завдання довжини вхідних даних в бітах, що суттєво ускладнює процес накопичення даних в масиві *s*, в даному оптимізованому алгоритмі довжина даних задається тільки в байтах, тому усі обчислення, пов’язані

з накопиченням даних суттєво спрощуються. Розмір рядка байтів для результату може бути більше, ніж розмір блоку, в даному алгоритмі це неможливо, розмір блоку завжди перевищує розмір рядка результату.

Для оптимізації обчислення для алгоритму *shake* також враховується, що для функцій *PRF, H, F* розмір вхідних даних не перевищує розміру блоку BS (Максимальна довжина вхідного блоку дорівнює $3 \cdot n + 32$, що дорівнює 128 *для* $n = 32$), тому не треба виконувати кроки 1, 2 алгоритму, достатньо в масив s записати вхідні дані, а для решти елементів масиву задати значення *0. Значення 0x1f записується в s[inlen / 8*].

В разі, якщо є більше одного блоку даних (функція **Tl**), при перемішуванні даних для кожного кроку дані спочатку копіюються в локальний масив, а потім виконується відновлення масиву. Якщо заздалегідь буде відома кількість блоків, є можливим виконання цих копіювань тільки для останньої ітерації.

В табл. 7 наведено параметри для оптимізації обчислень базових функцій для SHAKE256.

Таблиця 7

Параметри для оптимізації обчислень базових функцій для SHAKE256

Функція	Загальний розмір даних	Кількість повних блоків	Розмір неповного блоку
PRF	n + 32 + n	0	n + 32 + n
Tl	n + 32 + l · n (l = LEN, K)	(n + 32 + LEN · n)/BS (n + 32 + K · n)/BS	(n + 32 + LEN · n) mod BS (n + 32 + K · n) mod BS
H	n + 32 + 2 · n	0	(n + 32 + 2 · n)
F	n + 32 + n	0	n + 32 + n

Для функцій PRF та F довжина вхідного повідомлення співпадає, функція для обробки вхідного повідомлення теж співпадає, тому далі функція F не розглядається.

3.2. Алгоритм функцій sha256, sha512 та його оптимізація

Алгоритми є компонентами SHA-2.

1. Вхідні дані розглядаються як масив *32 (64)* бітних даних відповідно для *sha256, sha512*. Вхідні дані записуються з урахуванням формату *BIG-ENDIAN*. Перетворення для даних може виконуватись паралельно

2. Вхідні дані діляться на блоки розміром *64 (128)* байтів для *sha256, sha512* відповідно. Блоки обробляються послідовно, результат обробки попереднього блоку застосовують як вхідні дані для наступного. При обробці блоку паралелізм також недопустимий

3. Для решти даних розміром менше *64* байтів виконується доповнення до *64* байтів та обробка останнього блоку або двох блоків.

Таблиця 8

Параметри для оптимізації обчислень базових функцій для SHA256-SHA512

Функція	Загальний розмір даних	Кількість повних блоків	Розмір неповного блоку
PRF	BS + 22+ n	0	22+ n
Tl	BS + 22 + l · n (l = LEN, K)	(22 + LEN · n)/BS (22 + K · n)/BS	(22 + LEN · n) mod BS (22 + K · n) mod BS
H	BS + 22 + 2 · n	(BS + 22 + 2 · n)/BS	(BS + 22 + 2 · n) mod BS
F	BS + 22 + l · n (l = LEN, K)	(22 + LEN · n)/BS (22 + K · n)/BS	(22 + LEN · n) mod BS (22 + K · n) mod BS

Розмір блоку *(BS)* дорівнює *64* байти для *SHA256* та *128* байтів для *SHA512*.

В усіх функціях значення гешу для першого блоку визначається значенням *PK_seed* і може бути обчислене заздалегідь.

Кількість додаткових блоків та розмір неповного блоку залежать тільки від параметрів. Вони можуть бути попередньо обчислені, що спростить обробку доповнення останнього блоку.

4. Результати оптимізації

Результати оптимізації представлено в табл. 9 (SHAKE) та 10 (SHA256, SHA512). Перший рядок – кількість тактів до оптимізації, другий – після оптимізації. Для кожного значення, приведеного в таблицях, обчислюється мінімальне значення з 256 експериментів, що забезпечує мінімальну залежність від випадкових факторів переключення потоків. При порівнянні значень має сенс враховувати тільки дві старші цифри з врахуванням округлення.

Функція Tl викликається для вхідних даних розміром $LEN \cdot n$ та K · n, тому кількість тактів визначається для обох випадків.

Таблиця 9

Результати оптимізації (SHAKE)

Функція	128s	128f	192s	192f	256s	256f
PRFTime	1476 1277	1616 1471	1634 1462	1637 1480	1694 1454	1643 1448
TlTime (LEN)	(LEN = 35) 7200 6076	(LEN = 35) 8034 6950	(LEN = 51) 14951 13361	(LEN = 51) 14831 13310	(LEN = 67) 24297 22170	(LEN = 67) 24284 22184
TlTime (K)	(K = 14) 4720 3940	(K = 33) 8046 6952	(K = 17) 6820 5637	(K = 33) 10994 9504	(K = 22) 9567 8162	(K = 35) 13677 12132
Htime	1515 1310	1618 1450	1617 1466	1643 1474	1663 1480	1657 1449

Таблиця 10

Результати оптимізації (SHA)

Функція	128s	128f	192s	192f	256s	256f
PRFTime	1834 834	1810 890	1833 835	1917 839	1870 837	1872 866
TlTime (LEN)	(LEN = 35) 9977 7992	(LEN = 35) 9946 7973	(LEN = 51) 11942 10088	(LEN = 51) 11994 9780	(LEN = 67) 19821 17264	(LEN = 67) 19810 17420
TlTime (K)	(K = 14) 4674 3343	(K=33) 9060 7211	(K = 17) 6272 4203	(K = 33) 9151 7004	(K = 22) 8298 6152	(K = 35) 12252 9977
Htime	1827 825	1802 821	2356 1106	2320 1079	2343 1159	2341 1103

В табл. 11 наведено коефіцієнти прискорення (покращення), які обчислюються як відношення кількості тактів для стандартної оптимізованої версії до кількості тактів з урахуванням оптимізації авторів. В першому рядку задається коефіцієнт прискорення для алгоритму SHAKE, другий – для алгоритмів SHA.

Таблиця 11

Прискорення для базових операцій за використання різних функцій для алгоритму FIPS 205

Функція	128s	128f	192s	192f	256s	256f
PRFTime	1.16 2.2	1.1 2.03	1.12 2.2	1.11 2.28	1.17 2.23	1.13 2.16
TlTime (LEN)	LEN = 35 1.18 1.25	(LEN = 35) 1.16 1.25	(LEN = 51) 1.12 1.18	(LEN = 51) 1.11 1.23	(LEN = 67) 1.1 1.15	(LEN = 67) 1.1 1.14
TlTime (K)	(K = 14) 1.2 1.4	(K = 33) 1.26	(K = 17) 1.21 1.49	(K = 33) 1.16 1.31	(K = 22) 1.17 1.35	(K = 35) 1.13 1.23
Htime	1.16 2.2	1.12 2.2	1.10 2.13	1.11 2.15	1.12 2.02	1.14 2.12

Висновки

З отриманих у роботі результатів оптимізації можна зробити наступні висновки:

1 Операції для SHAKE при застосовуванні стандартних функцій, виконуються трохи скоріше, ніж відповідні операції для **SHA**, але останні можуть бути оптимізовані за рахунок постійного першого блоку для більшості базових операцій. Після оптимізації операції для SHA виконуються скоріше, ніж відповідні операції для SHAKE.

2 Застосування оптимізації забезпечує мінімальне прискорення для усіх операцій і всіх параметрів – 10 %.

3 Базова операція PRF, еквівалентна їй по списку параметрів та операцій функція F та функція H, згідно з табл. 6, викликаються найбільшу кількість разів. Прискорення для цих функцій в разі застосування SHA є не меншим ніж вдвічі.

4 Алгоритм FIPS 205 в якості базового формату застосовує формат *BIG-ENDIAN*, аналогічний формат застосовують функції групи SHA2. Для застосування однакового формату в подальших розширеннях алгоритму рекомендується застосовувати саме алгоритми SHA256 та SHA512.

Список літератури:

1. National Institute of Standards and Technology. (2017, January) // Post-Quantum Cryptography [Online]. Available: https://csrc.nist.gov/Projects/post-quantum-cryptography

2. Module-Lattice-Based Digital Signature Standard, FIPS 204, 2024 [Online]. Available: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.204.pdf

3. Stateless Hash-Based Digital Signature Standard, FIPS 205, 2024 [Online]. Available: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.205.pdf

4. D. Moody, R. Perlner, A. Regenscheid, A. Robinson, and D. Cooper. Transition to Post-Quantum Cryptography Standards // NIST Internal Report 8547 (Initial Public Draft) [Online], November 2024. Available: https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf

5. National Institute of Standards and Technology. (2020, October) // Post-Quantum Cryptography. Round 3 Submissions. CRYSTALS-DILITHIUM. [Online]. Available: https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-3-submissions

6. J.-P. Aumasson, D. J. Bernstein, W. Beullens, C. Dobraunig, M. Eichlseder, S. Fluhrer, S.-L. Gazdag, A. Hülsing, P. Kampanakis, S. Kölbl, T. Lange, M. M. Lauridsen, F. Mendel, R. Niederhagen, C. Rechberger, J. Rijneveld, P. Schwabe, and B. Westerbaan //"SPHINCS+: Submission to the NIST Post-Quantum Project, v3.1 [Online], June 2022. Available: https://sphincs.org/data/sphincs+-r3.1-specification.pdf

Надійшла до редколегії 06.03.2025

Відомості про авторів:

Горбенко Іван Дмитрович – д-р техн. наук, 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; АТ «Інститут інформаційних технологій», Голова наглядової ради; Україна; e-mail: i.d.gorbenko@karazin.ua; ORCID: https://orcid.org/0000-0003-4616-3449

Качко Олена Григорівна – канд. техн. наук, Харківський національний університет радіоелектроніки, професор кафедри програмної інженерії, факультет комп'ютерних наук; АТ «Інститут інформаційних технологій», член наглядової ради; Україна; e-mail: iit@iit.kharkov.ua, ORCID: https://orcid.org/0000-0001-9249-0497

Дерев'янко Ярослав Андрійович – Харківський національний університет імені В. Н. Каразіна, аспірант кафедри кібербезпеки інформаційних систем, мереж і технологій, навчально-науковий інститут комп'ютерних наук та штучного інтелекту, АТ «Інститут Інформаційних технологій», науковий співробітник-консультант; Україна; e-mail: yarik0009258@gmail.com; ORCID: https://orcid.org/0000-0002-3290-3373

УДК 004.056.5:004.8 **DOI:10.30837/rt.2025.2.221.02**

Є.О. ЛОГАЧОВА, М.В. ЄСІНА, канд. техн. наук, Д.Ю. ГОЛУБНИЧИЙ, канд. техн. наук

ДОСЛІДЖЕННЯ ТА АНАЛІЗ МІЖНАРОДНИХ СТАНДАРТІВ ТА РЕГУЛЯТОРНИХ ВИМОГ ЩОДО БЕЗПЕКИ ШТУЧНОГО ІНТЕЛЕКТУ, РОЗРОБКА МОДЕЛІ БЕЗПЕКИ ДЛЯ УКРАЇНИ

Вступ

В епоху сучасних технологій надважливо забезпечити їх необхідним рівнем безпеки для збереження належного функціонування бізнесу, різноманітних структур тощо. Також необхідно запобігти порушенню прав та свобод звичайних громадян і користувачів. Штучний інтелект (ШІ) – відносно нова технологія на ринку, що завоювала прихильність як звичайних користувачів, так і великих корпорацій. Розумні машини на основі штучного інтелекту допомогли у стрімкому розвитку багатьох галузей, таких як медицина, освіта, транспорт, сільське господарство, фінанси тощо. Разом з тим ШІ почали використовувати і для покращення рівня кібершахрайств. Для того щоб не відмовлятись від даних прогресивних технологій та не уповільнювати прогрес, багато країн вже почали вводити різноманітні рішення щодо безпеки використання штучного інтелекту. Україна наразі знаходиться на початковій стадії у даному питання, тому розгляд міжнародного досвіду допоможе зробити нормативно-правові регулювання в Україні ефективними та безпечними для усіх ланок держави.

1. Кібербезпека в епоху штучного інтелекту

Штучний інтелект радикально трансформує цифровий світ: автоматизація процесів, аналіз великих даних, прогнозування загроз. Спершу ШІ використовували для маленьких повторюваних задач, на зараз штучний інтелект використовується для діагностики здоров'я, організації бізнесу, навчання. Тобто технологія розвивається стрімко і використовується майже у всіх сферах життя, чи неабияк полегшує життя своїх користувачів.

За даними IBM, середня вартість витоку даних у 2023 р. становила понад 4,45 млн доларів, і ШІ дедалі частіше використовується як захисний, так і атакуючий інструмент [1]. А вже у 2024 р., згідно з IBM Cost of a Data Breach Report 2024, середня вартість витоку даних зросла до 4,88 млн доларів США, що на 10 % більше порівняно з 2023 р. Та при цьому штучний інтелект та автоматизація допомогли компаніям знизити витрати на усунення наслідків витоку даних у середньому на 2,2 млн доларів [2]. ШІ допомагає вирішувати декілька основних проблем інформаційної безпеки: виявлення загроз у реальному часі, автоматичне реагування на інциденти, прогнозування атак та інші.

Але з розвитком ШІ зростають і виклики – зокрема в сфері кібербезпеки. Відтак зловмисники можуть використати технології штучного інтелекту для створення deepfake контенту, автоматизації фішингових атак, атак соціальної інженерія нового рівня тощо. Окрім цього дана технологія може бути задіяна і у автоматизації шкідливого програмного забезпечення (ПЗ). Один із показових прикладів – дослідницький експеримент фахівців з кібербезпеки компанії Hyas, які створили умовний вірус під назвою BlackMamba. Цей шкідливий код мав здатність динамічно змінювати свою поведінку за допомогою ChatGPT, генеруючи частини свого функціоналу в режимі реального часу. Під час випробувань BlackMamba демонстрував здатність адаптуватися до різних середовищ та залишатися непоміченим більшістю популярних антивірусних систем [3].

У лютому 2024 р. в Гонконзі стався один із наймасштабніших випадків шахрайства із використанням штучного інтелекту. Співробітник міжнародної компанії отримав завдання надіслати 25 млн доларів США від імені свого нібито директора з Великої Британії. Після сумнівного електронного листа із запрошенням на відеоконференцію чоловік почав підозрювати фішинг. Проте участь кількох «знайомих колег» у відеодзвінку знизила його настороженість. Протягом кількох транзакцій, що охоплювали п'ять різних банківських рахунків,

працівник переказав загалом понад 200 млн гонконзьких доларів (приблизно 25 млн). Як згодом з'ясувалося, усі інші учасники відеоконференції були глибоко реалістичними штучними двійниками, створеними зловмисниками з використанням технологій штучного інтелекту та deepfake [4].

Усе це ставить непросту задачу перед спеціалістами з інформаційної безпеки, адже дана технологія неабияк підвищує рівень безпеки та при цьому ж може бути використана кіберзлочинцями для здійснення атак. Хорошим рішенням є впровадження необхідних стандартів та регуляторних вимог для безпечного використання ШІ. Для України це питання стоїть доволі серйозно, адже в умовах війни кількість фейків та кібератак все збільшується.

2. Огляд міжнародних стандартів та регуляторних вимог безпеки ШІ

Існує багато підходів і думок щодо нормативно-правових регулювань штучного інтелекту. У одних країнах до цієї технології ставляться з обережністю, а у інших вбачають у ній великий прогресивний поштовх для розвитку цифровізації.

Варто почати з Європейського Союзу (ЄС) та введеного ними EU AI Act, який фактично став першим офіційним і повноцінним документом з регулювання ШІ. EU AI Act встановлює чіткі правила для використання штучного інтелекту, враховуючи рівень потенційного ризику, який можуть нести різні типи систем ШІ. Залежно від цього рівня, як провайдери, так і користувачі зобов'язані дотримуватися певних вимог. Навіть у випадках, якщо ризик від технології вважається низьким, вона має пройти оцінювання, щоб гарантувати прозорість та відповідність етичним стандартам [5].

До категорії неприйнятного ризику потрапляють застосунки ШІ, які заборонені в ЄС, оскільки становлять загрозу для базових прав і свобод людини. Це включає штучний інтелект, що маніпулює поведінкою людей – особливо вразливих груп, таких як діти. Наприклад, голосові іграшки, які можуть спонукати до небезпечної поведінки. Також заборонені системи соціальної оцінки (оцінювання людей за поведінкою чи статусом), біометрична ідентифікація в публічних просторах у реальному часі, а також категоризація людей за біометричними ознаками [5].

У деяких випадках, як-от діяльність правоохоронних органів, можливе обмежене використання систем з високим ризиком. Наприклад, дистанційна біометрична ідентифікація в реальному часі дозволяється лише у виняткових ситуаціях та після попереднього дозволу суду. Ідентифікація «постфактум», тобто із затримкою, може застосовуватися для розслідування тяжких злочинів, але також лише за наявності юридичного схвалення [5].

Системи штучного інтелекту, які становлять високий ризик, охоплюють сфери, що мають прямий вплив на безпеку чи фундаментальні права громадян. Вони поділяються на дві ключові категорії. Перша – це ШІ, інтегрований у продукти, що регулюються європейським законодавством щодо безпеки. Наприклад, медичне обладнання, автомобілі, іграшки, ліфти. Друга – системи, які функціонують у чутливих галузях: управління критичною інфраструктурою, освіта, зайнятість, доступ до державних послуг, правоохоронна діяльність, а також процеси міграції й правозастосування [5].

Всі ці системи підлягають обов'язковому контролю як до їхнього впровадження на ринку, так і протягом усього життєвого циклу. Крім того, громадяни матимуть право подавати скарги на ШІ-системи до національних наглядових органів, що зміцнює принцип прозорості та підзвітності в епоху технологічного прогресу.

Ще одним важливим принципом є прозорість. Так, наприклад ChatGPT не вважається технологією з високим рівнем ризику, проте має відповідати законодавству ЄС, зокрема законодавству щодо авторського права. Таким чином, увесь контент, згенерований ChatGPT, має бути маркований спеціальним знаком, це допомагає запобігати поширенню фейкових зображень, відео та іншого контенту з шахрайською метою. Більш досконала модель штучного інтелекту GPT-4 повинна проходити ретельну оцінку, а про будь-які серйозні інциденти потрібно повідомляти Європейську комісію [5].

Перші норми, зокрема заборона на використання систем із неприйнятним рівнем ризику, набули чинності вже 2 лютого 2025 р. Інші елементи, як-от кодекси практики та вимоги до прозорості для універсальних моделей ШІ, почнуть діяти через 9 та 12 місяців відповідно [5].

Системи з високим рівнем ризику, включно із тими, що використовуються у сфері охорони здоров'я, освіти, критичної інфраструктури або правоохоронній діяльності, матимуть більше часу на адаптацію. Для них вимоги набудуть чинності через 36 місяців, що дозволить розробникам і користувачам належним чином підготуватися до впровадження нових стандартів.

NIST AI Risk Management Framework – це стратегічний документ, розроблений Національним інститутом стандартів і технологій США (NIST) з метою допомогти організаціям ефективно управляти ризиками, пов'язаними з впровадженням та використанням штучного інтелекту. Він є добровільним, але широко рекомендованим інструментом, який сприяє розробці безпечних, надійних, прозорих і етично обґрунтованих систем ШІ. За цим документом прийнято розподілити можливу нанесену шкоду на три категорії: шкода людям, шкода організації та шкода екосистемі. Шкода людям включає у себе фізичну, психологічну, соціальну або економічну шкоду. Наприклад, фальшиві медичні поради, неправдиві новини, або контент, що провокує насильство. ШІ також може бути використаний для дискримінації, упередженого оцінювання, неправомірного спостереження або цензури – особливо у випадках автоматизованих рішень без належного контролю, що призводить до порушення прав та свободи громадян [6].

Друга категорія під назвою «шкода організації» окреслює такі наслідки, як витіснення творчих професій, або недобросовісну конкуренцію через масове створення фальшивого або дезінформаційного контенту, збої на ринку праці та інших операцій, шкода репутації та інші потенційні ризики безпеці [6].

Третя категорія включає збої у глобальних фінансових системах або системах ланцюга поставок і шкоду навколишньому середовищу та природним ресурсам. Дані категорії створені для запобігання шкодам та ризикам описаним у них, що допомагає сконцентрувати увагу на актуальних проблемах [6].

Документ включає сім основних характеристик для надійних систем штучного інтелекту, яким вони мають відповідати. Першими є валідність та надійність, які означають, що система виконує свою функцію точно, стабільно і в межах запланованого контексту. Вона має бути перевірена на відповідність заявленим цілям і демонструвати передбачувану поведінку навіть в умовах змін середовища чи вхідних даних. Безпечність доповнює цю характеристику, адже система не повинна створювати фізичної або психологічної шкоди користувачам, і має бути захищеною від зловмисного впливу [6].

Неупередженість системи також дуже важлива – це здатність системи уникати дискримінаційних рішень або упередженості. Модель повинна однаково справедливо взаємодіяти з усіма користувачами незалежно від статі, раси, віку чи соціального статусу. Наступною є прозорість – користувачі повинні мати доступ до інформації про те, як система працює, на яких даних вона навчалась, і які можливі обмеження її застосування [6].

Іншою критично важливою характеристикою є пояснюваність – здатність системи та її розробників надати чітке пояснення, чому було прийнято те чи інше рішення. Це особливо актуально у сферах з високим ступенем відповідальності, наприклад, у медицині, фінансах чи юридичній сфері. Також важливою є здатність до захисту конфіденційності, що передбачає дотримання принципів збору, зберігання та обробки персональних даних відповідно до етичних та правових стандартів [6].

Останньою є стійкість – здатність системи зберігати свою функціональність навіть за наявності помилок, атак чи непередбачуваних ситуацій. Надійні системи повинні мати вбудовані механізми відновлення та захисту від зовнішніх загроз [6].

Документ базується на п'яти ключових функціях: Govern, Map, Measure, Manage і Improve [6]. Ці функції утворюють узгоджену систему, яка допомагає організаціям забезпе-

чити надійність, безпечність і етичність ШІ-систем протягом усього їхнього життєвого циклу – від початкового проєктування до постійного оновлення.

Перший етап – Govern, він полягає у створенні чіткої організаційної структури та політик, що регулюють впровадження ШІ. Це включає визначення відповідальних осіб, розподіл повноважень, прозорість процесів і формування внутрішніх стандартів. Добре організоване управління дозволяє приймати обґрунтовані рішення, враховуючи етичні, правові та соціальні аспекти використання технологій [6].

Далі йде Map – функція, що допомагає оцінити контекст, у якому працює система. На цьому етапі організації ідентифікують можливі загрози, враховують потреби користувачів і визначають потенційний вплив ШІ на людей та навколишнє середовище. Важливо не лише знати, як працює система, а й розуміти, для кого і з якою метою вона створена [6].

Measure забезпечує вимірювання ризиків та надійності системи [6]. Це можуть бути кількісні та якісні показники. Наприклад, точність, стабільність, справедливість або захищеність моделі. Регулярна оцінка допомагає виявляти слабкі місця до того, як вони спричинять шкоду, і дає змогу приймати обґрунтовані рішення щодо подальших кроків.

Функція Manage передбачає реалізацію конкретних заходів для мінімізації виявлених ризиків [6]. Це може включати зміни в алгоритмах, обмеження доступу до деяких функцій, захист персональних даних або навіть перегляд стратегії впровадження. Важливо, що управління ризиками не є разовим завданням, а триває протягом усього періоду використання ШІ.

Завершує цей цикл функція Improve, яка зосереджена на постійному аналізі та вдосконаленні практик управління ризиками. Організації мають враховувати досвід, нові знання, технологічний розвиток та зміни в нормативному середовищі, щоб адаптувати свої ШІ-системи до нових викликів [6].

Ще одним документом є стандарт ISO/IEC 23894:2023. Це перший міжнародний стандарт, що надає рекомендації з управління ризиками, пов'язаними з використанням штучного інтелекту. Документ адаптує загальні принципи управління ризиками до специфіки ШІ-систем, враховуючи їхню складність, динамічну поведінку, етичні виклики та вплив на права людини. Головна мета стандарту – допомогти організаціям мінімізувати можливу шкоду, підвищити довіру до ШІ та зробити його застосування безпечнішим і більш передбачуваним [7].

У стандарті ISO/IEC 23894:2023 окреслюється структура ефективного управління ризиками штучного інтелекту, що охоплює весь життєвий цикл систем ШІ. Одним із перших і ключових етапів є ідентифікація ризиків, яка передбачає глибоке розуміння того, як система ШІ буде використовуватися на практиці. Тут організації повинні враховувати як передбачувані сценарії застосування, так і потенційні випадки неправильного або зловмисного використання. Важливо також ретельно проаналізувати дані, на яких навчалась модель, способи прийняття нею рішень та ймовірний вплив її функціонування на різні групи користувачів і суспільство загалом [7].

Після виявлення потенційних ризиків стандарт пропонує провести їх оцінку, як у кількісному, так і у якісному вимірі. Оцінювання має охоплювати не лише ймовірність виникнення проблеми, але й масштаб можливих наслідків [7]. Особливо підкреслюється необхідність врахування каскадних ефектів – тобто того, як одна проблема може спричинити інші, пов’язані ризики. Це дозволяє побудувати більш повну картину загроз, які може створювати система ШІ у взаємодії з іншими технологіями або соціальними процесами.

Наступним кроком є обробка ризиків, тобто розробка практичних стратегій для їх зменшення. Це може включати перегляд архітектури самої моделі, посилення технічного або організаційного контролю, страхування ризиків або ж свідоме прийняття певного рівня залишкової небезпеки. Головне, щоб вибрані підходи відповідали як характеру загрози, так і загальній стратегії організації щодо етики та безпеки [7].

Завершальним елементом системи управління ризиками є постійний моніторинг і перегляд. Оскільки системи ШІ розвиваються у часі та взаємодіють з динамічним середовищем,

ISO/IEC 23894 наголошує на необхідності регулярної переоцінки ризиків. Це включає встановлення ключових індикаторів ризику (KRI), перевірку ефективності раніше впроваджених заходів і оперативне оновлення стратегій у відповідь на зміни в технологічному або соціальному контексті [7].

Найбільш відкритими до технологій штучного інтелекту є Об'єднані Арабські Емірати (ОАЕ). ОАЕ демонструють швидкий і стратегічний підхід до регулювання штучного інтелекту. Країна прагне не лише використовувати ШІ у своїй економіці, але й стати глобальним лідером у сфері інноваційного управління. У 2017 р. ОАЕ першими у світі призначили міністра штучного інтелекту, підкреслюючи політичну волю до активного розвитку цієї галузі. Відтоді в країні діє Національна стратегія ШІ 2031, що ставить за мету зробити ШІ ключовим інструментом підвищення ефективності урядових послуг, охорони здоров'я, транспорту та освіти [8].

На відміну від багатьох інших юрисдикцій, ОАЕ не приймають детального законодавчого акту, подібного до європейського AI Act. Натомість, держава діє через галузеве регулювання та ініціативи публічно-приватного партнерства. Наприклад, у сфері фінансових послуг Центральний банк ОАЕ та інші регулятори вже впровадили політики використання ШІ, спрямовані на запобігання зловживанням, шахрайству та упередженості в автоматизованих рішеннях [8].

Цікаво, що в ОАЕ також активно діє Dubai International Financial Centre (DIFC) – спеціальна юрисдикція, яка самостійно впроваджує власні цифрові стандарти. У межах ініціативи DIFC AI and Data Protection Guidelines пропонується фреймворк із використанням ШІ, який поєднує етичні принципи, прозорість та відповідальність розробників. ОАЕ, таким чином, рухаються у напрямку «гнучкого регулювання», яке дозволяє адаптуватися до швидких технологічних змін без надмірної бюрократії [8].

Однак відсутність єдиного національного закону щодо ШІ створює ризик фрагментації правового середовища, особливо для міжнародних компаній, які працюють в різних еміратах або секторах. У перспективі ОАЕ можуть розглянути ухвалення більш цілісного законодавства, яке б забезпечило узгодженість підходів у всіх сферах і дало більше впевненості бізнесу щодо вимог до відповідального впровадження технологій штучного інтелекту.

3. Поточна ситуація регулювання штучного інтелекту в Україні

Україна розробила поетапну дорожню карту для впровадження регулювання штучного інтелекту, орієнтуючись на інтеграцію в європейський цифровий простір та імплементацію майбутніх стандартів ЄС, зокрема AI Act. Основною метою документа є створення такого підходу до ШІ, який поєднує захист прав людини, розвиток інноваційної економіки та підвищення міжнародної конкурентоспроможності українських компаній [9].

Документ пропонує bottom-up підхід, тобто рух від м'яких, позазаконодавчих механізмів до поступового впровадження законодавства. На першому етапі (планується два-три роки) передбачається створення регуляторного середовища: тестові механізми, добровільні кодекси поведінки, оцінка ризиків та публікація «Білої книги» – аналітичного документа з рекомендаціями для держави й бізнесу [9]. Це дозволить учасникам ринку адаптуватися до майбутніх вимог без надмірного тиску.

Другий етап передбачає поступову імплементацію положень європейського AI Act, зокрема в момент, коли це стане вимогою для подальшої інтеграції України до ЄС [9]. Планується адаптація найвимогливіших стандартів захисту прав людини, прозорості та етики у використанні ШІ, але з урахуванням специфіки національного ринку. Такий підхід дозволить Україні не лише забезпечити відповідність міжнародним вимогам, але й залишитись гнучкою та конкурентною на глобальному ринку.

У «Білій книзі» окреслено три стратегічні цілі: забезпечення прав людини, підтримка конкурентоспроможності бізнесу та євроінтеграція. Україна прагне гармонізувати майбутнє законодавство із нормами ЄС, аби надати українським ШІ-продуктам вільний доступ до рин-

ку Європи. Водночас у сфері оборони регулювання ШІ не передбачається, з огляду на військовий стан і потребу в інноваціях для захисту держави [10].

Особливу увагу в «Білій книзі» приділено балансу між правами людини та інноваційністю. Міністерство цифрових трансформацій України визнає: надмірне регулювання може загальмувати розвиток ШІ-індустрії, а його повна відсутність – створити загрози для прав і свобод громадян. Тому Україна орієнтується на сервісну модель держави, яка не тисне, а допомагає – через створення публічних інструментів, як-от веб-портал відповідального ШІ, платформа юридичної допомоги, інструмент добровільного маркування систем [10].

Методологія оцінки впливу ШІ на права людини стане базовим інструментом: вона допоможе визначити рівень ризику продукту і стане передумовою для участі в регуляторній пісочниці або отримання консультацій. Регуляторна пісочниця, своєю чергою, дозволить стартапам і компаніям тестувати свої рішення під наглядом держави, готуючись до майбутніх вимог. Також планується система добровільного маркування ШІ, подібна до етикеток на продуктах – аби користувачі знали, як саме працює система, і могли оцінити її надійність, безпеку та етичність.

4. Модель безпеки використання штучного інтелекту для України

Одним із ключових елементів регулювання штучного інтелекту є побудова системи безпеки, яка гарантує відповідальне, етичне та надійне використання ШІ. Для України така модель повинна враховувати як світові стандарти, так і національні виклики, пов’язані з війною, цифровою трансформацією та інтеграцією в європейський правовий простір. У цьому розділі подано узагальнений підхід до формування моделі безпеки використання ШІ в українських умовах, модель наведено на рис. 1.

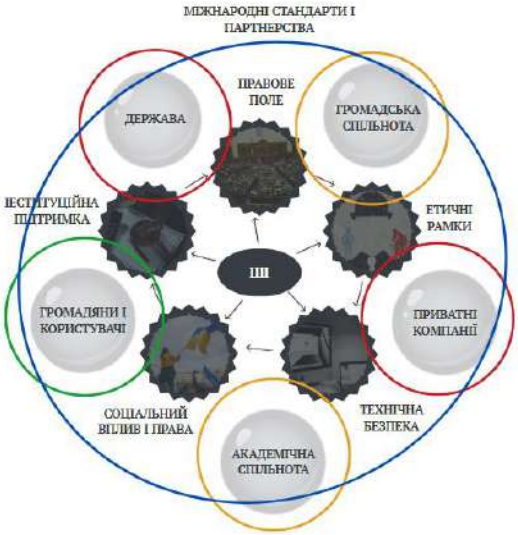

Рис. 1. Модель регулювання безпеки штучного інтелекту в Україні

Запропонована модель безпеки використання штучного інтелекту базується на системному підході, який передбачає взаємодію різних зацікавлених сторін і ключових сфер впливу. У центрі моделі знаходиться ШІ як технологічне ядро, довкола якого формуються міжсекторальні механізми регулювання, етики та технічної підтримки.

У моделі закладено взаємодію між державою, академічною спільнотою, громадянським суспільством, приватними компаніями, міжнародними партнерами та самими користувачами. Такий формат дозволяє не лише регулювати ШІ, а й формувати довіру до нього як до інструменту для розвитку, а не загрози. Україна – країна, що веде активну цифровізацію і не боїться впроваджувати нові технології. У цьому плані український громадський сектор та законодавча база є більш гнучкою і готовою до змін, аніж у сусідніх країнах Європейського Союзу.

Відповідно до рівня ризику, який може виникнути у тій чи іншій складовій її позначено відповідним кольором (де зелений – допустимий, жовтий – високий, червоний – підвищений). За концепцією, схожою з AI Act, цей поділ є необхідним для оцінки кожної моделі ШІ, яка використовується у тій чи іншій галузі. Україна могла б створити «відкритий етичний реєстр ШІ», куди кожна компанія добровільно додала б свою модель. І де кожна модель має власний «паспорт прозорості» – хто її створив, як навчав, які ризики враховані. Додатково кожна система проходила б оцінку на рівень ризику, відповідно до цього її власники мали б забезпечувати певний рівень безпеки, який відповідав би українському стандарту. Це не цензура, це – цифрова культура, адже користувачі мають знати, що саме використовують. Відповідно в уряді має бути створено спеціальний департамент з питань штучного інтелекту, який видавав би ліцензії безпеки та розглядав би і приймав усі потрібні нормативно-правові рішення. Також одним із важливих рішень має бути обов'язкове маркування продуктів та контенту, створеного штучним інтелектом, задля запобігання шахрайства та недоброчесності.

Окрему роль у цій моделі може відігравати громадська спільнота, залучена до моніторингу та аудиту ШІ-систем. Запровадження публічних механізмів контролю, таких як цифрові платформи для фіксації порушень або несправедливих рішень, дозволить забезпечити не лише технічну, а й соціальну безпеку. Водночас державні сервіси – зокрема платформа «Дія» – можуть стати прикладом прозорого, етичного використання ШІ в публічному управлінні, де кожен громадянин має доступ до зрозумілих пояснень рішень, прийнятих алгоритмом.

Ключову роль також відіграє академічна спільнота, яка здатна не лише досліджувати ризики, а й формувати освітню культуру довкола ШІ. Впровадження національного освітнього треку з етики та технологій, інтеграція відповідних курсів у навчальні програми та підтримка молодих дослідників допоможе створити критичну масу спеціалістів, здатних формувати відповідальне майбутнє ШІ в Україні.

В українському контексті приватні компанії не обмежуються впровадженням технологій – вони стають співавторами національної цифрової безпеки. Особливо у сфері штучного інтелекту бізнес має не лише комерційні, а й моральні зобов'язання: перед клієнтами, державою, суспільством і навіть перед власними працівниками. Українські компанії вже довели, що можуть бути лідерами в етичному програмуванні, відкритих кодах, благодійних проєктах та безпечних цифрових рішеннях.

Майбутнє моделі безпеки ШІ в Україні передбачає особливий соціальний договір між державою та бізнесом: не через штрафи чи контроль, а через довіру, сертифікацію, кооперацію та інноваційне партнерство. Компанії, які добровільно дотримуються стандартів прозорості, маркують свої моделі, відкривають алгоритми на ревізію, можуть отримати «цифрову довіру» – умовне етичне маркування, схоже на ISO, але у сфері штучного інтелекту. Водночас важливо підтримати компанії не тільки вимогами, а й ресурсами та середовищем. Наприклад, держава може створити інкубатори відповідального ШІ, де стартапи отримуватимуть доступ до відкритих даних, консультацій з етики, шаблонів політик – без тиску, без формальностей, з орієнтацією на співпрацю.

Ще однією важливою частиною запропонованої моделі безпеки використання ШІ є відкритість до міжнародної співпраці. Це включатиме обмін даними, впровадження міжнародних стандартизацій та регуляторних актів у інтегрованому для України форматі.

У контексті безпеки штучного інтелекту особливу увагу слід приділяти технічним практикам розробки та впровадження ШІ-рішень у приватному секторі, зокрема в компаніях, які створюють системи для використання в соціально чутливих сферах: оборона, фінанси, охорона здоров'я, освіта. Український бізнес сьогодні має справу не лише з комерційними викликами, а й із загрозами кібератак, викрадення моделей, отруєння даних та спробами маніпулювання алгоритмами. Ключовими напрямами технічної безпеки в межах української моделі ШІ можуть стати: безпечне навчання моделей, моніторинг поведінки моделей у

реальному часі, розмежування доступу до компонентів ШІ систем, впровадження explainable AI та контейнери для тестування.

Окремої уваги заслуговує питання інфраструктурної стійкості: більшість українських IT-компаній розміщують свої сервіси в хмарі, часто – за кордоном. В умовах воєнних ризиків важливо створити резервні дата-центри, енергонезалежні вузли або використовувати «розподілену відповідальність» за безпеку з партнерами по хмарним сервісам, із обов'язковим аудитом.

Таким чином, запропонована модель безпеки використання ШІ надаватиме простір для розвитку та новаторства, але при цьому увесь процес від створення моделей штучного інтелекту до їх подальшого безпечного використання буде контрольованим та безпечним. Відкритість до міжнародної співпраці тільки підкреслює намір України підтримувати європейські стандарти безпеки та при цьому дасть можливість ділитись власним досвідом з міжнародними партнерами.

Висновки

У результаті проведеного дослідження було проаналізовано міжнародні підходи до регулювання та управління безпекою штучного інтелекту, зокрема стандарти ЄС, США, ISO/IEC та моделі, що впроваджуються в Об'єднаних Арабських Еміратах. Встановлено, що кожна з цих систем має свої сильні сторони, але не є універсальною для застосування в українському контексті. Найбільш прийнятним для України є гібридний підхід, який поєднує сервісну, гнучку модель співрегулювання з орієнтацією на права людини та прозорість, характерну для європейського AI Act.

Особливої уваги потребує побудова власної національної моделі безпеки ШІ, яка враховуватиме специфіку воєнного часу, цифрової трансформації, високої ролі громадянського суспільства та унікального українського досвіду цифрового спротиву. Запропонована модель взаємодії між державою, бізнесом, академічною спільнотою, громадянами та міжнародними партнерами створює основу для формування довіри до ШІ та ефективного управління ризиками на всіх етапах життєвого циклу технологій.

Окрема роль у цій системі належить приватному сектору, який може не лише впроваджувати етичні стандарти, а й бути рушієм цифрової культури безпеки. Важливо, щоб держава підтримувала інноваційні ініціативи через інкубатори відповідального ШІ, сертифікування та механізми прозорості, що спростять адаптацію бізнесу до майбутнього регулювання.

Таким чином, Україна має реальну можливість не лише гармонізувати своє законодавство із міжнародними стандартами, а й запропонувати власний – інноваційний та адаптивний – підхід до безпеки штучного інтелекту. Це дозволить країні стати повноцінним учасником глобального цифрового ринку, водночас зберігаючи пріоритет прав людини, технологічну відкритість та національну стійкість.

Список літератури:

1. Cost of a Data Breach Report 2024. [Електронний ресурс]. Режим доступу: https://www.ibm.com/reports/data-breach.

2. IBM Report: Escalating Data Breach Disruption Pushes Costs to New Highs. [Електронний ресурс]. Режим доступу: https://newsroom.ibm.com/2024-07-30-ibm-report-escalating-data-breach-disruption-pushes-costs-to-new-highs?utm_source=chatgpt.com.

3. Атаки на основі штучного інтелекту: нові виклики для кібербезпеки. [Електронний ресурс]. Режим доступу: https://wezom.com.ua/ua/blog/ataki-na-osnovi-shtuchnogo-intelektu-novi-vikliki-dlya-kiberbezpeki.

4. 5 реальних прикладів хакерських атак за допомогою ШІ. [Електронний ресурс]. Режим доступу: https://dev.ua/news/5-prykladiv-khakerskykh-atak-ai.

5. EU AI Act: first regulation on artificial intelligence. [Електронний ресурс]. Режим доступу: https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence.

6. Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile. [Електронний ресурс]. Режим доступу: https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf.

7. Information technology – Artificial intelligence – Guidance on risk management [Електронний ресурс]. Режим доступу: https://cdn.standards.iteh.ai/samples/77304/cb803ee4e9624430a5db177459158b24/ISO-IEC-23894-2023.pdf.

8. AI Watch: Global regulatory tracker – United Arab Emirates. [Електронний ресурс]. Режим доступу: https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-uae.

9. Дорожня карта з регулювання штучного інтелекту в Україні Bottom-Up Підхід. [Електронний ресурс]. Режим доступу: https://surli.cc/tyzbug.

10. Біла книга з регулювання ШІ в Україні: бачення Мінцифри. Режим доступу: https://thedigital.gov.ua/storage/uploads/files/page/community/docs/Регулювання%20ШІ.pdf.

Надійшла до редколегії 02.02.2025

Відомості про авторів:

Логачова Єлизавета Олегівна – Харківський національний університет імені В. Н. Каразіна, студентка кафедри кібербезпеки інформаційних систем, мереж і технологій, навчально-науковий інститут комп'ютерних наук та штучного інтелекту; Україна; e-mail: lohachova2020kb11@student.karazin.ua; ORCID: https://orcid.org/0000-0002-9815-466X

Єсіна Марина Віталіївна – канд. техн. наук, доцент, Харківський національний університет імені В. Н. Каразіна, в.о. завідувача кафедри кібербезпеки інформаційних систем, мереж і технологій, навчально-науковий інститут комп'ютерних наук та штучного інтелекту, АТ Інститут Інформаційних Технологій", науковий співробітник-консультант; Україна; e-mail: m.v.yesina@karazin.ua; ORCID: https://orcid.org/0000-0002-1252-7606

Голубничий Дмитро Юрійович – канд. техн. наук, доцент, АТ "Інститут Інформаційних Технологій", начальник наукового відділу; Україна; ORCID: https://orcid.org/0000-0002-6873-7004

УДК 004.056:519.2 **DOI:10.30837/rt.2025.2.221.03**

А.М. ОЛЕКСІЙЧУК, д-р техн. наук, Ю.Р. КІНДРАТ

УДОСКОНАЛЕНИЙ АЛГОРИТМ ЛЕВІНА ДЛЯ ОБМЕЖЕНИХ ЙМОВІРНІСНИХ ПСЕВДОБУЛЕВИХ ФУНКЦІЙ

Вступ

У статті О. Гольдрайха та Л. Левіна [1] доведено теорему, яку можна сформулювати таким чином. Нехай h – функція, задана на множині V_n двійкових векторів довжини n, $s \in V_n$ – невідомий фіксований вектор. Припустимо, що існує ймовірнісний алгоритм, який для довільного $x \in V_n$ знаходить за значеннями x та $h(s)$ оцінку (0 або 1) булевого скалярного добутку векторів s та x за T операцій з імовірністю (відносно випадкового рівноймовірного вибору x, а також випадкових даних, що використовуються в алгоритмі) $1/2 \cdot (1+\varepsilon)$, $\varepsilon \in (0,1)$. Тоді існує ймовірнісний алгоритм, якій відновлює значення s за значенням $h(s)$ з імовірністю помилки $\delta \in (0,1)$ зі складністю, що поліноміально залежить від T, ε^{-1} та $\log \delta^{-1}$ (тут і далі $\log$ позначає логарифм за основою 2). Для доведення теореми в [1] запропоновано поліноміальний алгоритм, який, говорячи мовою теорії кодування, здійснює списочне декодування коду Адамара – лінійного блокового коду, що складається з векторів значень усіх лінійних булевих функцій від n змінних. Зазначений алгоритм, що носить сьогодні прізвища Гольдрайха та Левіна, а також однойменна теорема відіграють важливу роль у криптології, зокрема, при встановленні взаємоз'язку між важкооборотними (one-way) функціями та псевдовипадковими генераторами. Більш того, теорема Гольдрайха–Левіна суттєво використовується при побудові сучасних обґрунтовано стійких потокових шифрів [2 – 5], а відповідний алгоритм або його модифікації – для знаходження лінійних наближень булевих функцій [6 – 12].

Нагадаємо, що остання задача полягає в тому, щоб сформувати для довільної булевої функції f від n змінних та числа $\varepsilon \in (0,1)$ список усіх лінійних булевих функцій, які співпадають з функцією f не менше ніж на $2^{n-1}(1+\varepsilon)$ двійкових наборах. Найбільш відомим алгоритмом розв'язання цієї задачі є алгоритм швидкого перетворення Адамара, який обчислює усі лінійні наближення булевої функції від n змінних за $O(n2^n)$ операцій додавання та віднімання цілих чисел (див., наприклад, [13]). Зазначений алгоритм не є оптимальним за складністю, навіть у класі детермінованих алгоритмів [14].

Суттєве зменшення трудомісткості побудови лінійних наближень можливо за рахунок застосування модифікацій алгоритму Гольдрайха–Левіна [6 – 12], серед яких відзначимо вдосконалений алгоритм Левіна [7] зі складністю $\widetilde{O}(n\varepsilon^{-2}\log\delta^{-1})$ операцій над цілими числами, де $\widetilde{O}$ позначає оцінку з точністю до логарифмічних множників від n та ε^{-1}. Зауважимо, що цей алгоритм (поряд з викладеним в [12]) є на сьогодні найшвидшим серед відомих алгоритмів побудови лінійних наближень булевих функцій.

Метою цієї статті є узагальнення вдосконаленого алгоритму Левіна на випадок обмежених ймовірнісних псевдобулевих функцій, тобто певних випадкових відображень множини V_n у множину дійсних чисел. Основним результатом є теорема, яка встановлює нижню межу ймовірності потрапляння кожного шуканого наближення до випадкового списку, який формується з використанням наведеного алгоритму. (Зауважимо, що подібний результат відсутній у роботі [7], а його доведення проводиться за той самою схемою, що і у [10, п. 4.4], але більш простим способом).

Результати статті надають змогу отримати більш ефективну редукцію (tight reduction) задач у відомих доведеннях псевдовипадковості генераторів гами за умови високої обчислю-

вальної складності декодування випадкових лінійних блокових кодів або розв'язання випадкових систем нелінійних булевих рівнянь [2 – 5].

1. Постановка задачі

Для будь-яких натуральних чисел n,t позначимо V_n множину двійкових векторів довжини n, $F_{t\times n}$ – множину $t\times n$-матриць над полем $F=\mathbf{GF}(2)$. Надалі позначатимемо $\alpha x=\alpha_1 x_1\oplus\cdots\oplus\alpha_n x_n$ булев скалярний добуток довільних двійкових векторів $\alpha=(\alpha_1,...,\alpha_n)$ та $x=(x_1,...,x_n)$.

Ймовірнісна псевдобулева функція від n змінних визначається як випадкове відображення $g:V_n\to\mathbf{R}$ (де $\mathbf{R}$ – множина дійсних чисел) з такою властивістю: для будь-яких (не обов'язково різних) векторів $x_1,...,x_t\in V_n$ значення $g(x_1),...,g(x_t)$ є незалежними однаково розподіленими випадковими величинами. Типовим прикладом такої функції є відображення, яке задається за допомогою випадкового оракула – ймовірнісного алгоритму, який обчислює значення функції, використовуючи певні параметри, значення яких, у свою чергу, вибираються випадково та незалежно від аргументів функції з певної скінченної множини згідно з деяким законом розподілу ймовірностей, причому вибір цих значень відбувається кожен раз незалежно від того, як вони були обрані при попередніх зверненнях до функції (див., наприклад, [15, п. 3.2]). Іншим (тривіальним) прикладом ймовірнісної функції є довільна звичайна (не випадкова) псевдобулева функція.

Зафіксуємо *обмежену* ймовірнісну функцію $g:V_n\to\mathbf{R}$, тобто таку, що для деякого $C>0$ нерівність $|g(x)|\le C$ виконується для кожного $x\in V_n$ з імовірністю 1. Надалі, не обмежуючи загальності міркувань, вважатимемо $C=1$.

Позначимо $\bar{g}$ математично сподівання випадкової функції g, тобто звичайну псевдобулеву функцію, кожне значення $\bar{g}(x)$ якої отримується шляхом усереднення значень випадкової величини $g(x)$ за її розподілом ймовірностей, $x\in V_n$.

Нарешті, позначимо

$$\hat{g}(\alpha)=2^{-n}\sum_{x\in V_n}(-1)^{\alpha x}\bar{g}(x),\ \alpha\in V_n$$

перетворення Фур'є функції $\bar{g}$ та розглянемо для будь-яких $\varepsilon\in(0,1)$, $C_\varepsilon>0$ множину

$$L_{\bar{g},\varepsilon}=\{\alpha\in V_n:\ \hat{g}(\alpha)\ge C_\varepsilon\}. \tag{1}$$

Задача полягає у розробці ймовірнісного алгоритму, який формує за вхідними даними $(g,\varepsilon,C_\varepsilon,\delta)$, де $\delta\in(0,1)$, випадковий список $\Lambda_{g,\varepsilon}\subseteq V_n$ такий, що

$$\forall\alpha\in V_n:\ \alpha\in L_{\bar{g},\varepsilon}\Rightarrow\mathbf{P}\{\alpha\in\Lambda_{g,\varepsilon}\}\ge 1-\delta, \tag{2}$$

де ймовірність $\mathbf{P}$ обчислюється відносно розподілу функції g та випадкових даних, які використовуються в самому алгоритмі.

Як приклад, розглянемо важливий окремий випадок, в якому функція g визначається за формулою $g(x)=(-1)^{f_\omega(x)}$, якщо $x\in M$; $g(x)=0$, якщо $x\in V_n\setminus M$, де $f_\omega:M\to\{0,1\}$ – часткова булева функція, задана на певній множині $M\subseteq V_n$ потужності T, ω – випадковий елемент, розподілений на певній скінченній множині Ω. В цьому випадку для будь-якого $\alpha\in V_n$ виконується рівність

$$\mathbf{P}_X\{f_\omega(X)=\alpha X\}=1/2\cdot\left(1+T^{-1}\sum_{x\in M}(-1)^{f_\omega(x)\oplus\alpha x}\right),$$

де X – випадковий вектор з рівномірним розподілом на M. Звідси випливає, що

$$\mathbf{P}_{X,\omega}\{f_\omega(X)=\alpha X\}=1/2\cdot\left(1+T^{-1}\sum_{x\in V_n}(-1)^{\alpha x}\overline{g}(x)\right)=1/2\cdot(1+2^nT^{-1}\hat{g}(\alpha)).$$

Отже, при $C_\varepsilon=2^{-n}T\varepsilon$ множина (1) збігається з сукупністю всіх векторів $\alpha\in V_n$, які задовольняють умову $\mathbf{P}_{X,\omega}\{f_\omega(X)=\alpha X\}\geq 1/2(1+\varepsilon)$. Зокрема, якщо $|\Omega|=1$, $M=V_n$ і $C_\varepsilon=\varepsilon$, то поставлена вище задача зводиться до побудови списку "високоймовірних" лінійних наближень звичайної булевої функції f, тобто таких лінійних функцій $l_\alpha(x)=\alpha x$, $x\in V_n$, які збігаються з f не менше ніж на $2^{n-1}(1+\varepsilon)$ вхідних наборах. Для розв'язання останньої задачі можна скористатися одним з відомих ймовірнісних алгоритмів [6 – 12].

2. Отримані результати

Алгоритм побудови множини $\Lambda_{g,\varepsilon}$, який викладено нижче, є узагальненою версією вдосконаленого алгоритму Левіна [7]. Він залежить від натуральних параметрів l, t і має такий вигляд.

1. Згенерувати незалежні в сукупності випадкові вектори $X_1,...,X_t$ та Z_{ij} ($i\in\overline{1,n}$, $j\in\overline{1,l}$), кожен з яких має рівномірний розподіл на множині V_n.

2. Сформувати таблицю розміром $2ln\times 2^t$, рядки якої занумеровані трійками $(i,\ j,\ \nu)$, де $i\in\overline{1,n}$, $j\in\overline{1,l}$, $\nu\in\{0,1\}$, а стовпці – векторами $u\in V_t$, таку, що на перетині будь-якого рядка з номером $(i,\ j,\ \nu)$ і стовпця з номером u знаходиться елемент

$$g_{i,j,\nu}(u)=\begin{cases}g(uX\oplus Z_{ij}\oplus\nu e_i),\ \text{якщо}\ u\neq 0;\\ 0,\ \text{якщо}\ u=0,\end{cases}\qquad(3)$$

де X – матриця з рядками $X_1,...,X_t$, e_i – двійковий вектор довжини n, усі координати якого, за виключенням i-ї, дорівнюють нулю.

3. Помножити кожен рядок зазначеної таблиці на матрицю Адамара H_t, використовуючи алгоритм швидкого перетворення Адамара, та отримати нову таблицю з елементами

$$h_{i,j,\nu}(a)=\sum_{u\in V_t}g_{i,j,\nu}(u)(-1)^{ua},\qquad(4)$$

де $i\in\overline{1,n}$, $j\in\overline{1,l}$, $\nu\in\{0,1\}$, $a=(a_1,...,a_t)\in V_t$; покласти

$$s_{i,j,\nu}(a)=\begin{cases}0,\ \text{якщо}\ h_{i,j,\nu}(a)\geq 0;\\ 1,\ \text{якщо}\ h_{i,j,\nu}(a)<0\end{cases}\qquad(5)$$

для будь-яких $i\in\overline{1,n}$, $j\in\overline{1,l}$, $\nu\in\{0,1\}$ та $a\in V_t$.

4. Для кожного $a\in V_t$ виконати таку процедуру:

4.1. Для кожного $i\in\overline{1,n}$ обчислити

$$s_{i,1,0}(a)\oplus s_{i,1,1}(a),\ s_{i,2,0}(a)\oplus s_{i,2,1}(a),\ \ldots,\ s_{i,l,0}(a)\oplus s_{i,l,1}(a)\qquad(6)$$

та покласти α_i рівним елементу (0 або 1) з найбільшою частотою зустрічаємості в послідовності (6).

4.2. Додати отриманий вектор $\alpha = (\alpha_1, \ldots, \alpha_n)$ до списку $\Lambda_{g,\varepsilon}$, що формується.

Отже, в результаті виконання алгоритму буде побудовано випадковий список, який складається з 2^t (не обов'язково різних) двійкових векторів α довжини n.

Наступне твердження випливає безпосередньо з опису наведеного алгоритму.

Твердження. Для будь-якої ймовірнісної функції $g: V_n \to [-1,1]$ та довільного числа $\varepsilon \in (0,1)$ алгоритм формує список $\Lambda_{g,\varepsilon}$, використовуючи $T_g 2^{t+1} nl + O(2^t tnl)$ операцій (додавання, віднімання та порівняння з нулем дійсних чисел або двійкових векторів довжини n), де T_g – максимальна складність обчислення одного значення функції g.

Доведемо теорему, яка встановлює нижню межу ймовірності події $\{\alpha \in \Lambda_{g,\varepsilon}\}$ для будь-якого $\alpha \in L^-_{g,\varepsilon}$ та надає змогу з'ясувати, яким чином слід вибирати параметри l і t алгоритму для заздалегідь означених $g, \varepsilon, C_\varepsilon, \delta$.

Теорема. Нехай $g: V_n \to [-1,1]$ – ймовірнісна функція, $\varepsilon \in (0,1)$, $\theta \in (0, 1/4)$ і $L^-_{g,\varepsilon}$ – множина вигляду (1). Позначимо $\tilde{Z}$ набір випадкових векторів Z_{ij}, які генеруються на першому кроці алгоритму. Тоді для будь-якого $\alpha \in L^-_{g,\varepsilon}$ виконується нерівність

$$\mathbf{P}_{g,X,\tilde{Z}}\{\alpha \in \Lambda_{g,\varepsilon}\} \geq (1 - \exp\{-8l\theta^2\})^n \left(1 - \frac{1}{(2^t - 1)C_\varepsilon^2 (1/4 - \theta)}\right) \tag{7}$$

за умови, що кожен з двох співмножників у правій частині є додатним числом.

Доведення. Введемо випадкові величини

$$\xi_\alpha(X, Z) = (2^t - 1)^{-1} \sum_{u \in V_t \setminus \{0\}} (-1)^{(uX \oplus Z)\alpha} g(uX \oplus Z),\ \alpha \in V_n, \tag{8}$$

$$\eta_a(X, Z) = (2^t - 1)^{-1} \sum_{u \in V_t \setminus \{0\}} (-1)^{ua} g(uX \oplus Z),\ a \in V_t, \tag{9}$$

де Z – випадковий вектор з рівномірним розподілом на множині V_n, який не залежить від випадкових функції g та матриці X. Для будь-яких $x \in F_{t \times n}$ (значення випадкової матриці X) та $a \in V_t$ задамо ймовірнісну булеву функцію

$$f_{x,a}(z) = \begin{cases} 0, \text{ якщо } \eta_a(x,z) \geq 0; \\ 1, \text{ якщо } \eta_a(x,z) < 0,\ z \in V_n. \end{cases} \tag{10}$$

Зауважимо, що на підставі рівностей (3) – (5) для будь-яких $i \in \overline{1,n}$, $j \in \overline{1,l}$, $\nu \in \{0,1\}$, $a \in V_t$ виконуються рівності

$$h_{i,j,\nu}(a) = (2^t - 1)\eta_a(X, Z_{ij} \oplus \nu e_i),\ s_{i,j,\nu}(a) = f_{X,a}(Z_{ij} \oplus \nu e_i). \tag{11}$$

Зафіксуємо довільний вектор $\alpha \in L_{g,\varepsilon}$ та доведемо низку допоміжних тверджень.

1⁰. Справедлива нерівність

$$\mathbf{P}_{g,X,Z}\{f_{X,X\alpha}(Z) = \alpha Z\} \geq 1 - \frac{1}{(2^t - 1)\, C_\varepsilon^2}. \tag{12}$$

Дійсно, на підставі рівностей (8), (9)

$$\eta_{X\alpha}(X,Z)=(2^t-1)^{-1}\sum_{u\in V_t\setminus\{0\}}(-1)^{(uX)\alpha}g(uX\oplus Z)=(-1)^{\alpha Z}\xi_\alpha(X,Z).$$

Крім того, згідно з формулою (10), $\eta_{X\alpha}(X,Z)=|\eta_{X\alpha}(X,Z)|(-1)^{f_{X,X\alpha}(Z)}$. Отже, подія $\{\xi_\alpha(X,Z)>0\}$ тягне подію $\{f_{X,X\alpha}(Z)=\alpha Z\}$, звідки випливає, що

$$\mathbf{P}_{g,X,Z}\{f_{X,X\alpha}(Z)=\alpha Z\}\ge\mathbf{P}_{g,X,Z}\{\xi_\alpha(X,Z)>0\}. \tag{13}$$

Далі, випадкові вектори $uX\oplus Z$ ($u\in V_t\setminus\{0\}$) є попарно незалежними та рівноймовірними, звідки на підставі означення ймовірнісної функції випливає, що доданки у правій частині рівності (8) є попарно незалежними та однаково розподіленими випадковими величинами. Звідси, враховуючи обмеженість функції g, отримаємо такі співвідношення: $\mathbf{E}\xi_\alpha(X,Z)=\hat g(\alpha)$, $\mathbf{D}\xi_\alpha(X,Z)\le(2^t-1)^{-1}(1-\hat g(\alpha)^2)\le(2^t-1)^{-1}$, де символи $\mathbf{E}$ та $\mathbf{D}$ позначають відповідно математичне сподівання та дисперсію відносно розподілу $\mathbf{P}_{g,X,Z}$. Отже, згідно з нерівністю Чебишова отримаємо, що

$$\mathbf{P}_{g,X,Z}\{|\xi_\alpha(X,Z)-\hat g(\alpha)|\ge C_\varepsilon\}\le C_\varepsilon^{-2}\mathbf{D}\xi_\alpha(X,Z)\le C_\varepsilon^{-2}(2^t-1)^{-1}. \tag{14}$$

Нарешті, оскільки $\alpha\in L_{g,\varepsilon}$, тобто $\hat g(\alpha)\ge C_\varepsilon$, то

$$\mathbf{P}_{X,Z}\{\xi_\alpha(X,Z)\le 0\}\le\mathbf{P}_{X,Z}\{|\xi_\alpha(X,Z)-\hat g(\alpha)|\ge C_\varepsilon\}. \tag{15}$$

З нерівностей (13) – (15) випливає формула (12).

2^0. Для будь-якого $\theta\in(0,1/4)$ виконується нерівність

$$\mathbf{P}_X\{\mathbf{P}_{g,Z}\{f_{X,X\alpha}(Z)=\alpha Z\}\ge 3/4+\theta\}\ge 1-\frac{1}{(2^t-1)\,C_\varepsilon^2(1/4-\theta)}. \tag{16}$$

Для доведення нерівності (16) скористаємося співвідношеннями

$$\mathbf{P}\{\xi\le C\}=1-\mathbf{P}\{\xi>C\}\ge 1-C^{-1}\mathbf{E}\xi,\ C>0,$$

справедливими для будь-якої невід'ємної випадкової величини ξ, вважаючи

$$\xi=1-\mathbf{P}_{g,Z}\{f_{X,X\alpha}(Z)=\alpha Z\},\ C=1/4-\theta.$$

В результаті отримаємо, що

$$\mathbf{P}_X\{\mathbf{P}_{g,Z}\{f_{X,X\alpha}(Z)=\alpha Z\}\ge 3/4+\theta\}\ \ge\ 1\ -\ \frac{\mathbf{E}_X(1-\mathbf{P}_{g,Z}\{f_{X,X\alpha}(Z)=\alpha Z\})}{1/4-\theta}\ =$$

$$=\ \frac{\mathbf{P}_{g,X,Z}\{f_{X,X\alpha}(Z)=\alpha Z\}-3/4-\theta}{1/4-\theta}.$$

Звідси на підставі формули (12) випливає нерівність (16).

3^0. Нехай значення x випадкової матриці X є таким, що $\mathbf{P}_{g,Z}\{f_{x,x\alpha}(Z)=\alpha Z\}\ge 3/4+\theta$, де $\theta\in(0,1/4)$. Тоді ймовірність $\pi_{n,l}(\theta)$ події, яка полягає в тому, що для кожного $i\in\overline{1,n}$ елемент $\hat\alpha_i$ з найбільшою частотою зустрічаємості у випадковій послідовності

$$\xi_j^{(i)}=f_{x,x\alpha}(Z_{ij}\oplus e_i)\oplus f_{x,x\alpha}(Z_{ij}),\ j\in\overline{1,l}, \tag{17}$$

дорівнює α_i, є не менше ніж $(1-\exp\{-8l\theta^2\})^n$.

Для доведення помітимо, що на підставі означення ймовірнісної функції випадкові величини $\xi_j^{(i)}$ ($i \in \overline{1,n}$, $j \in \overline{1,l}$) є незалежними в сукупності. Отже,

$$\pi_{n,l}(\theta) = \prod_{i=1}^{n} \mathbf{P}\{\hat{\alpha}_i = \alpha_i\}. \tag{18}$$

Далі, для будь-якого $i \in \overline{1,n}$

$$\xi_j^{(i)} \oplus \alpha_i = (f_{x,x\alpha}(Z_{ij} \oplus e_i) \oplus \alpha(Z_{ij} \oplus e_i)) \oplus (f_{x,x\alpha}(Z_{ij}) \oplus \alpha(Z_{ij})),\ j \in \overline{1,l}, \tag{19}$$

звідки випливає, що

$$\mathbf{P}_{g,\tilde{Z}}\{\xi_j^{(i)} \neq \alpha_i\} \le \mathbf{P}_{g,\tilde{Z}}(\{f_{x,x\alpha}(Z_{ij} \oplus e_i) \oplus \alpha(Z_{ij} \oplus e_i) = 1\} \cup \{f_{x,x\alpha}(Z_{ij}) \oplus \alpha(Z_{ij}) = 1\}) \le$$
$$\le 2\mathbf{P}_{g,Z}\{f_{x,x\alpha}(Z) \neq \alpha Z)\} \le 2(1/4 - \theta) = 1/2 - 2\theta,\ j \in \overline{1,l}. \tag{20}$$

Крім того, елемент з найбільшою частотою зустрічаємості в послідовності (17) не збігається з α_i тоді й тільки тоді, коли число одиниць в послідовності (19) є більше за число нулів, тобто виконується умова $\sum_{j=1}^{l}(\xi_j^{(i)} \oplus \alpha_i) > l/2$. При цьому послідовність (19) є схемою Бернуллі з параметрами (l, p_i), де за формулою (20) $p_i = \mathbf{P}_{g,\tilde{Z}}\{\xi_j^{(i)} \neq \alpha_i\} \le 1/2 - 2\theta$, $i \in \overline{1,n}$. Звідси на підставі відомої оцінки Чернова випливає, що

$$\mathbf{P}_{g,\tilde{Z}}\{\hat{\alpha}_i = \alpha_i\} = \mathbf{P}_{g,\tilde{Z}}\left\{\sum_{j=1}^{l}(\xi_j^{(i)} \oplus \alpha_i) - lp_i > l(1/2 - p_i)\right\} \le$$
$$\le \exp\{-2l(1/2 - p_i)^2\} \le \exp\{-8l\theta^2\},\ i \in \overline{1,n}. \tag{21}$$

Таким чином, внаслідок формул (18) та (21) виконується нерівність $\pi_{n,l}(\theta) \ge (1 - \exp\{-8l\theta^2\})^n$, що й треба було довести.

Перейдемо до доведення співвідношення (7). Для будь-якого $\alpha \in L_{g,\varepsilon}^{-}$ розглянемо такі події:

$$A_\alpha = \{x \in F_{t\times n} :\ \mathbf{P}_{g,Z}\{f_{x,x\alpha}(Z) = \alpha Z\} \ge 3/4 + \theta\},$$
$$B_\alpha(x) = \{(g, \tilde{z} = (z_{ij} \in V_n : i \in \overline{1,n}, j \in \overline{1,l})) :\ \forall\, i \in \overline{1,n}\ \textit{елемент}$$
$$\textit{з найбільшою частотою зустрічаємості в послідовності}$$
$$f_{x,x\alpha}(z_{ij} \oplus e_i) \oplus f_{x,x\alpha}(z_{ij}),\ j \in \overline{1,l},\ \textit{дорівнює}\ \alpha_i\},\ x \in F_{t\times n}.$$

З наведеного опису алгоритму та рівностей (11) випливає, що подія $\{\alpha \in \Lambda_{g,\varepsilon}\}$ настає у випадку, коли відбувається подія $\{X \in A_\alpha, (g, \tilde{Z}) \in B_\alpha(X)\}$. Отже,

$$\mathbf{P}_{g,X,\tilde{Z}}\{\alpha \in \Lambda_{g,\varepsilon}\} \ge \mathbf{P}_{g,X,\tilde{Z}}\{X \in A_\alpha, (g, \tilde{Z}) \in B_\alpha(X)\} = \sum_{x \in A_\alpha} \mathbf{P}_{g,X,\tilde{Z}}\{X = x, (g, \tilde{Z}) \in B_\alpha(x)\} =$$
$$= \sum_{x \in A_\alpha} \mathbf{P}_X\{X = x\} \mathbf{P}_{g,\tilde{Z}}\{(g, \tilde{Z}) \in B_\alpha(x)\}.$$

Далі, згідно з твердженням 3^0, для будь-якого $x \in A_\alpha$ справедлива нерівність

$$\mathbf{P}_{g,\tilde{Z}}\{(g, \tilde{Z}) \in B_\alpha(x)\} \ge (1 - \exp\{-8l\theta^2\})^n. \tag{22}$$

При цьому на підставі твердження 2^0

$$\mathbf{P}_X\{X \in A_\alpha\} \geq 1 - \frac{1}{(2^t - 1)\, C_\varepsilon^2 (1/4 - \theta)}. \tag{23}$$

Отже, за умови додатності виразів у правих частинах нерівностей (22), (23) справедлива нерівність (7). Таким чином, теорему повністю доведено.

Безпосередньо з теореми та твердження перед нею випливає такий результат.

Наслідок. Нехай $g(x) = (-1)^{f(x)}$, $x \in V_n$, де f – ймовірнісна булева функція від n змінних, $l = \left\lceil 8\ln(2n\delta^{-1}) \right\rceil$, $t = \left\lceil \ln(16\varepsilon^{-2}\delta^{-1} + 1) \right\rceil$, $\varepsilon, \delta \in (0,1)$. Тоді наведений алгоритм будує випадковий список $\Lambda_{g,\varepsilon}$ розміру 2^t, який задовольняє умову (2), використовуючи $T_f 2^{t+1} nl + O(2^t tnl)$ операцій (додавання, віднімання та порівняння з нулем цілих чисел або двійкових векторів довжини n), де T_f – максимальна складність обчислення одного значення функції f.

Для доведення достатньо покласти у формулі (7) $\theta = 1/8$, $C_\varepsilon = \varepsilon$ та скористатися оцінкою

$$(1 - \exp\{-8l\theta^2\})^n \left(1 - \frac{1}{(2^t - 1)C_\varepsilon^2 (1/4 - \theta)}\right) \geq 1 - n\exp\{-8l\theta^2\} - \frac{1}{(2^t - 1)C_\varepsilon^2 (1/4 - \theta)}.$$

Висновки

У статті представлено узагальнення вдосконаленого алгоритму Левіна [7] на випадок обмежених ймовірнісних псевдобулевих функцій. Основним результатом є теорема, яка встановлює нижню межу ймовірності потрапляння кожного шуканого наближення до випадкового списку, що формується з використанням наведеного алгоритму. Розгляд таких функцій є необхідним для розповсюдження можливості застосування вдосконаленого алгоритму Левіна (замість оригінального алгоритму Гольдрайха–Левіна [1]) у відомій схемі доведення стійкості потокових шифрів [2 – 5]. Зокрема, результати статті надають можливість отримати більш ефективну редукцію задач у доведеннях псевдовипадковості деяких відомих генераторів гами за умови високої обчислювальної складності декодування випадкових лінійних блокових кодів або розв'язання випадкових систем нелінійних булевих рівнянь. Отримані результати також можуть бути використані для знаходження лінійних апроксимацій шифрувальних перетворень блокових шифрів, що є важливим при побудові лінійних атак на них.

Список літератури:

1. Goldreich O., Levin L.A. A hard core predicate for all one-way functions // Proc. 21st ACM Symposium on Theory of Computing. 1989. P. 25–32.
2. Fischer J.-B., Stern J. An efficient pseudo-random generator provably as secure as syndrome decoding // EUROCRYPT'96: Proc. 15th International Conference on Theory and Application of Cryptographic Techniques. Springer, 1996. P. 245–255.
3. Gaborit Ph., Laudaroux C., Sendrier N. SYND: a very fast code-based cipher stream with a security reduction // IEEE International Symposium on Information Theory (ISIT'07). Nice, France, July 2007. P. 186–190.
4. Meziani M., Hoffmann G., Cayrel P.-L. Improving the performance of the SYND stream cipher // Progress in Cryptology – AFRICACRYPT 2012. Berlin : Springer, 2012. P. 99–116.
5. Berbain C., Gilbert H., Patarin J. QUAD: A multivariate stream cipher with provable security // Journal of Symbolic Computation. 2009. Vol. 44, № 12. P. 1703–1723.
6. Levin L.A. Randomness and non-determinism // Journal of Symbolic Logic. 1993. Vol. 58, № 3. P. 1102–1103.
7. Bshouty N., Jackson J., Tamon C. More efficient PAC-learning of DNF with membership queries under the uniform distribution // Proc. 12th Annual Conference on Computational Learning Theory. 1999. P. 286–295.
8. Goldreich O., Rubinfeld R., Sudan M. Learning polynomials with queries: the highly noisy case // SIAM Journal on Discrete Mathematics. 2000. Vol. 13, № 4. P. 535–570.

9. Kabatiansky G., Tavernier C. List decoding of Reed-Muller codes // Proc. 9th International Workshop on Algebraic and Combinatorial Coding Theory. 2008. P. 230–235.
10. Trevisan L. Some applications of coding theory in computational complexity : препринт № cs/0409044v1 / Luca Trevisan. Cornell University, 2004. 17 с. (arXiv:cs/0409044v1).
11. Fourquet R., Loidreau P., Tavernier C. Finding good linear approximations of block ciphers and its application to cryptanalysis of reduced round DES // Proc. WCC 2009. P. 501–515.
12. Abdouli A. S., Dumer I., Kabatiansky G., Tavernier C. The Goldreich-Levin algorithm with reduced complexity // Thirteenth International Workshop on Algebraic and Combinatorial Coding Theory (ACCT 2012). Pomorie, Bulgaria, June 15–21, 2012. P. 7–14.
13. Олексійчук А. М., Курінний О. В. Методи криптоаналізу потокових шифрів : навч. посіб. Київ : КПІ ім. Ігоря Сікорського, 2023. 172 с.
14. Dumer I.I., Kabatiansky G.A., Tavernier C. List decoding of binary first-order Reed-Muller codes // Problems of Information Transmission. 2007. Vol. 43, № 3. P. 225–232.
15. Kopparty S., Saraf S. Local list decoding and testing of random linear codes from high-error // SIAM Journal on Computing. 2013. Vol. 42, № 3. P. 1302–1326.

Надійшла до редколегії 11.03.2025

Відомості про авторів:
Олексійчук Антон Миколайович – доктор технічних наук, професор, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", професор спеціальної кафедри № 1; Україна; e-mail: alex-dtn@ukr.net; ORCID: https://orcid.org/0000-0003-4385-4631
Кіндрат Юлія Русланівна – здобувачка вищої освіти ступеня магістра, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Україна; e-mail: kindrat0407@gmail.com

УДК 004.056 **DOI:10.30837/rt.2025.2.221.04**

Д.М. МОРГУЛЬ, О.П. НАРЄЖНІЙ, канд. техн. наук, Т.О. ГРІНЕНКО, канд. техн. наук

МОДЕЛЬ ПОРУШНИКА ТА МОДЕЛЬ ЗАГРОЗ ДЛЯ ВЕБ-СЕРВІСУ QRNG

Вступ

У сучасних інформаційних системах генерація випадкових чисел є критично важливою для забезпечення криптографічної стійкості, автентичності та цілісності даних. Квантові генератори випадкових чисел (QRNG, quantum random number generator) використовують фундаментальні принципи квантової механіки для створення істинної випадковості, яка не може бути передбачена або відтворена класичними засобами [1]. Завдяки цьому QRNG стають ключовим компонентом у побудові високонадійних криптографічних систем, особливо в контексті постквантової безпеки.

Зі зростанням популярності хмарних рішень та сервісної моделі розгортання QRNG (наприклад, через Application Programming Interface (API) або як частину сервісів "random-as-a-service") постає необхідність комплексного аналізу безпекових ризиків. Веб-сервіси QRNG, незважаючи на високу якість джерела випадковості, залишаються вразливими до традиційних та спеціалізованих кіберзагроз, зокрема атак на канал передачі, підробки API, компрометації QRNG тощо [2, 3].

Незважаючи на існування загальних підходів до моделювання загроз (наприклад, STRIDE [4]) та моделей порушників (зовнішні, внутрішні[5]), модель загроз для веб-сервісу QRNG залишається недостатньо дослідженою. Водночас компрометація такого сервісу може мати катастрофічні наслідки, особливо для систем, криптографічна стійкість яких залежить від справжньої випадковості.

Метою статті є розробка моделі загроз та моделі порушника для веб-сервісу QRNG. У роботі досліджено типові архітектури таких сервісів, визначені потенційні вектори атак та профіль порушника, обґрунтовано та надано рекомендації щодо посилення інформаційної безпеки даного класу систем.

1. Методологія моделювання

Моделювання загроз і моделювання порушника є фундаментальними етапами при розробці системи захисту для будь-якої інформаційної системи, зокрема для веб-сервісу QRNG. У даній роботі для побудови моделі загроз і моделі порушника використано комплексний підхід, що поєднує стандартизовані методики аналізу ризиків, адаптовані до специфіки архітектури QRNG.

Для моделювання загроз використано адаптовану версію методології STRIDE, що запропонована компанією Microsoft, яка дозволяє класифікувати загрози за шістьма категоріями: підміна особи (Spoofing), модифікація даних (Tampering), відмова від дій (Repudiation), розголошення інформації (Information Disclosure), відмова в обслуговуванні (Denial of Service) та підвищення привілеїв (Elevation of Privilege) [4]. Цей підхід є ефективним для виявлення типових атак на веб-сервіси, включно з API, каналами зв’язку та обробкою даних, що робить його релевантним для аналізу безпеки QRNG як сервісу.

У якості основи для класифікації ризиків використано підхід, рекомендований стандартом ISO/IEC 27005, який описує процес управління ризиками інформаційної безпеки: ідентифікація активів, оцінка загроз, вразливостей, наслідків і ймовірностей [5]. Також враховано національні вимоги до захисту інформації, що викладені у нормативному документі НД ТЗІ 1.4-001-2000, зокрема щодо категоризації активів, типів порушників та цілей атак [6].

Розробка моделі загроз виконувалася у кілька етапів:

1. Ідентифікація активів – визначення критичних компонентів QRNG-сервісу: фізичний генератор, API, обробник запитів, клієнтська сторона, канал зв’язку.

2. Ідентифікація загроз – аналіз потенційних загроз згідно з категоріями STRIDE, а також з урахуванням специфіки квантових пристроїв (наприклад, вплив на джерело випадковості).

3. Оцінка ризиків – визначення ймовірності реалізації загрози та можливого збитку для кожного активу.

4. Формалізація результатів – представлення моделі загроз у вигляді таблиці, що включає тип загрози, відповідний актив, можливий вплив і приклади реалізації.

Модель порушника базується на принципах, закладених у стандарті НД ТЗІ 1.1-002-99, де порушники класифікуються за такими ознаками [9]:

– перший рівень визначає найнижчий рівень можливостей проведення діалогу з КС і запуску фіксованого набору завдань (програм), що реалізують заздалегідь передбачені функції обробки інформації;

– другий рівень визначається можливістю створення і запуску власних програм з новими функціями обробки інформації;

– третій рівень визначається можливістю управління функціонуванням КС, тобто впливом на базове програмне забезпечення системи і на склад і конфігурацію її устаткування;

– четвертий рівень визначається всім обсягом можливостей осіб, що здійснюють проектування, реалізацію і ремонт апаратних компонентів КС, аж до включення до складу КС власних засобів з новими функціями обробки інформації.

У моделі враховано профілі типових порушників. Для кожного профілю визначено потенційні вектори атаки, типові загрози, які можуть бути реалізовані, та ймовірність їх успішного виконання. При формалізації архітектури системи та побудови STRIDE-матриці використовується таблиця імовірність/вплив, що наведена у розд. 4 табл.3, та діаграма потоку даних (DFD – data flow diagram), яка приведена на рис. 1. Для візуалізації взаємозв'язку між порушниками, вразливостями та наслідками атак використовуються графи атак [7]. Приклад графів атак TA01 та TA02 на QRNG веб-сервіс наведено на рис. 2.

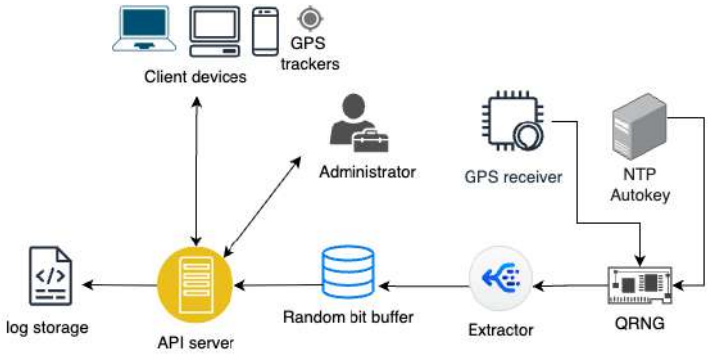

Рис. 1. Діаграма потоку даних (DFD)

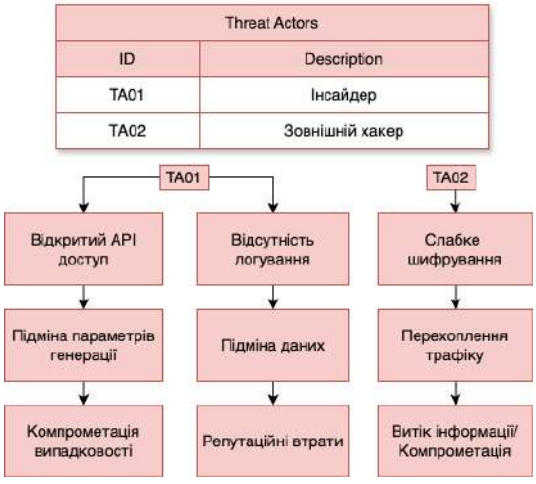

Рис. 2. Приклади графів атак на QRNG веб-сервіс

2. Розробка моделі загроз для веб-сервісу QRNG за методологією STRIDE

Модель загроз є невід'ємною складовою побудови системи захисту QRNG веб-сервісу, оскільки дозволяє ідентифікувати можливі атаки, оцінити їхній вплив та розробити відповідні контрзаходи. У контексті веб-сервісів, що забезпечують генерацію випадкових чисел, критичною є безперервність генерації, цілісність результатів та довіра до джерела випадковості [1]. Враховуючи специфіку веб-сервісу QRNG, слід звернути увагу на те, що навіть мінімальне порушення випадковості у вихідному потоці може призвести до генерації передбачуваних криптографічних ключів, що ставить під загрозу всю систему, яка базується на QRNG [3].

На основі аналізу типової архітектури QRNG-сервісу (локальний квантовий генератор, серверна частина з API, канали передачі даних, інтерфейс клієнта) було виділено такі критичні активи:

– QRNG-пристрій – джерело фізично згенерованої випадковості;
– сервер API – компонент, що обробляє запити та генерує відповіді;
– канал зв'язку (інтернет) – передача результатів до клієнта;
– буфер обробки/постобробки (екстрактор) – цифрова обробка випадкових бітів;
– логування та моніторинг – системи контролю коректності функціонування;
– інтерфейс клієнта.

Для оцінки рівня впливу загроз були використані значення, що наведені в табл. 1.

Таблиця 1

Рівень впливу загрози	Опис
1	незначний (низький)
2	нижчий за середній
3	середній
4	вищий за середній
5	значний (високий)

Із застосуванням методології STRIDE був проведений аналіз вразливості кожного активу веб-сервісу QRNG до шести класів загроз, результати аналізу наведено на рис. 3. Додатково враховано специфіку квантових пристроїв, зокрема можливість впливу на джерело генерації з боку навколишнього середовища або сторонніх сигналів.

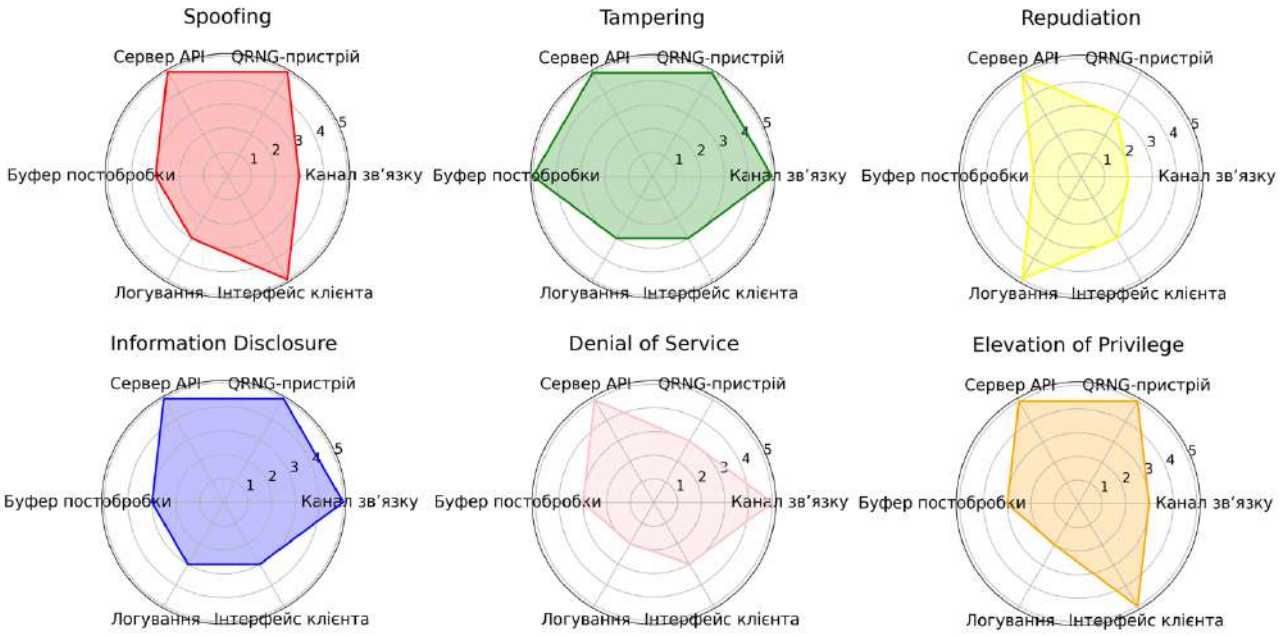

Рис. 3. Результати аналізу активів веб-сервісу QRNG згідно з методологією STRIDE

Результати аналізу показали, що найбільш вразливими елементами системи є: сервер API, QRNG пристрій та канал зв'язку, які схильні до більшої кількості загроз відносно решти активів. Для подальшої формалізації ризику застосовується матриця ймовірність/вплив, що надана у розд. 4 табл. 3.

3. Розробка моделі порушника

У процесі аналізу безпеки веб-сервісу QRNG особливу увагу слід приділити ідентифікації потенційних порушників – суб'єктів, здатних ініціювати загрози для конфіденційності, цілісності та доступності системи. Побудова моделі порушника дозволяє краще зрозуміти мотиви, можливості та технічні ресурси атакуючих сторін, що є важливим для проектування заходів захисту критичних програмних систем [8]. Модель порушника – абстрактний формалізований або неформалізований опис дій порушника, який відображає його практичні та теоретичні можливості, апріорні знання, час та місце дії. По відношенню до сервісу порушники можуть бути внутрішніми (з числа співробітників, користувачів системи) або зовнішніми (сторонні особи або будь-які особи, що знаходяться за межами контрольованої зони) [6].

Згідно з підходами, що використовуються в національному нормативному документі НД ТЗІ 1.4-001-2000 [6], модель порушника повинна визначати:

– можливу мету порушника та її градацію за ступенями небезпечності для АС;
– категорії осіб, з числа яких може бути порушник;
– припущення про кваліфікацію порушника;
– припущення про характер його дій.

Класифікація порушників виконується за наступними критеріями [6]:

– мета;
– категорія особи;
– рівень можливостей та доступу;
– рівень обізнаності про систему;
– методи та засоби.
– місце здійснення дій.

Мету порушника визначено шляхом дослідження і класифікації вразливостей, враховуючи технічні особливості веб-сервісу QRNG:

– отримання атрибутів доступу споживачів з метою перехоплення даних та їх подальшого використання або поширення;

– маніпуляція середовищем коду екстрактора з метою подальшого впливу на процес генерації випадкових чисел під час роботи QRNG;

– компрометація криптографічних бібліотек з метою підміни джерела випадкових чисел під час виконання криптографічних операцій шляхом інтеграції менш стійкого програмного генератора випадковості;

– відновлення вихідних даних QRNG з метою подальшого їх використання або поширення;

– несанкціонований доступ до системи та її програмних або апаратних елементів з метою фізичного впливу на апаратну інфраструктуру або шпигунства;

– порушення випадковості з метою компрометації ресурсу в цілому;

– блокування роботи сервісу або зупинки передачі випадкових чисел кінцевим споживачам.

За рівнем обізнаності порушника запропоновано наступну класифікацію:

– споживачі даних, які мають інформацію про можливості сервер API;

– спеціалісти, які володіють високим рівнем знань та досвідом роботи з технічними засобами системи та їхнього обслуговування;

– адміністратор системи – має доступ до системи і відповідну документацію про архітектуру системи і її роботу;

– розробник системи – має повну інформацію про програмну частину системи, її вразливі місця, рівень захищеності;

– спеціаліст по QRNG приладам – володіє високим рівнем знань у галузі квантової електроніки, особливо у фізичних приладах квантових генераторів випадкових чисел.

За використовуваними методами і способами порушників запропоновано класифікувати згідно [6] як таких, що:

– використовують виключно агентурні методи одержання відомостей;

– використовують пасивні технічні засоби перехоплення інформаційних сигналів;

– використовують виключно штатні засоби системи або недоліки проєктування КСЗІ для реалізації спроб НСД;

– використовують способи і засоби активного впливу на систему, що змінюють конфігурацію системи (підключення додаткових або модифікація штатних технічних засобів, підключення до каналів передачі даних, впровадження і використання спеціального ПЗ тощо).

За місцем здійснення дії порушників запропоновано класифікувати як:

– з одержанням доступу до QRNG;

– з одержанням доступу до засобів адміністрування;

– без одержання доступу.

На основі цих критеріїв та особливостей веб-сервісу QRNG сформовано профіль порушника, що представлений в табл. 2.

Таблиця 2

Категорія осіб	Зовнішній (З)
	Внутрішній (ВН)
Характер дій	Навмисний (Н)
	Випадковий (ВП)
Рівень можливостей та доступу	Перший рівень (1)
	Другий рівень (2)
	Третій рівень (3)
	Четвертий рівень (4)
Рівень обізнаності про систему	Споживач даних (СД)
	Спеціаліст (СП)
	Адміністратор системи (А)
	Розробник системи (Р)
	Спеціаліст по QRNG приладам (С)
Методи та засоби	Агентурні (АГ)
	Пасивні (П)
	Штатні (Ш)
	Активні (АК)
Місце здійснення дій	З одержанням доступу до QRNG (Д)
	З одержанням доступу до засобів адміністрування (ЗА)
	Без одержання доступу (БД)
Мета дій	Отримання атрибутів доступу споживачів (АС)
	Маніпуляція середовищем коду екстрактора (МС)
	Компрометація криптографічних бібліотек (КБ)
	Відновлення вихідних даних QRNG (ВД)
	Несанкціонований доступ до системи (НСД)
	Порушення випадковості (ПВ)
	Блокування роботи сервісу (БР)

4. Аналіз результатів розробки моделі загроз та моделі порушника

На основі проведеного дослідження і розроблених моделі загроз та моделі порушника для веб-сервісу QRNG побудована таблиця імовірність/вплив для кожної загрози із врахуванням категорії загрози за моделлю STRIDE (табл. 3). Значення впливу розраховано експертним методом (рис. 3). Оцінювання ризику базується на двох ключових параметрах: ймовір-

ність реалізації та ступінь впливу. Відповідно до стандарту ISO/IEC 27005 [5], ризик розраховується як

$$,\qquad (1)$$

де R – загальний ризик, P – ймовірність реалізації загрози, C – її вплив.

Таблиця 3

Загроза	Актив	STRIDE	Ймовірність (P)	Вплив (C)
АС	сервер API інтерфейс клієнта	Spoofing	Висока	5
МС	сервер API екстрактор	Repudiation	Висока	4
КБ	QRNG екстрактор	Tampering	Середня	5
ВД	QRNG	Information Disclosure	Середня	5
НСД	QRNG сервер API канал зв'язку	Elevation of privilege	Низька	5
ПВ	QRNG екстрактор	Tampering	Низька	5
БР	канал зв'язку сервер API інтерфейс клієнта	Denial of Service	Висока	4

Враховуючи виявлені загрози і профіль порушника, розробка ефективних заходів захисту веб-сервісу QRNG вимагає інтегрованого підходу, який поєднує технічні, організаційні та процедурні механізми. Випадкові числа, згенеровані QRNG, можуть використовуватися у високозахищених криптографічних контекстах (наприклад, для генерації ключів у постквантових протоколах), і навіть незначне порушення їх цілісності може мати катастрофічні наслідки [1].

Техніки пом'якшення загроз для методології STRIDE, що запропоновані організацією OWASP, наведено у табл. 4 [10]

Таблиця 4

Тип загрози	Техніки пом'якшення загроз
Spoofing Identity	1. Відповідна автентифікація 2. Захист секретних даних 3. Не зберігати секрети
Tampering with data	1. Відповідна авторизація 2. Геші 3. MAC-коди (коди автентифікації повідомлень) 4. Цифрові підписи 5. Протоколи з захистом від підробки
Repudiation	1. Цифрові підписи 2. Мітки часу 3. Журнали аудиту
Information Disclosure	1. Авторизація 2. Протоколи з підвищеним рівнем конфіденційності 3. Шифрування 4. Захист секретів 5. Не зберігати секрети
Denial of Service	1. Відповідна автентифікація 2. Відповідна авторизація 3. Фільтрація 4. Обмеження (наприклад, швидкості запитів) 5. Якість обслуговування (QoS)
Elevation of privilege	1. Використовувати принцип найменших привілеїв

Обґрунтовано та рекомендовано наступні технічні заходи безпеки для веб-сервісу QRNG:

Захист каналу передачі даних. Передача випадкових чисел від сервера до клієнта має відбуватись виключно через захищений канал з використанням протоколів TLS 1.3 або вище. Сертифікати повинні регулярно оновлюватись, а конфігурації перевірятись на відсутність слабких шифрів [11].

Автентифікація та авторизація API. Доступ до QRNG через API повинен здійснюватися за допомогою багатофакторної автентифікації (наприклад, біометрична або OAuth 2.0 з підтримкою короткоживучих токенів) та систем контролю доступу з мінімальними привілеями [12].

Постобробка вихідних даних. Для забезпечення ентропійності та стійкості до маніпуляцій рекомендується впроваджувати процедури постобробки (наприклад, Von Neumann, Trevisan extractors), верифіковані незалежним аудитом.

Моніторинг та аудит. Усі критичні компоненти повинні логуватись, з підтримкою зовнішнього збору логів та аналізу подій. Особлива увага приділяється незвичній поведінці API, зміні патернів генерації або появі повторів у потоках.

Тестування випадковості. Регулярне застосування стандартних тестів на випадковість (наприклад, NIST SP 800-22, Dieharder) дозволяє виявити збої у роботі QRNG на ранніх етапах [13].

Обґрунтовано та рекомендовано наступні організаційні заходи безпеки для веб-сервісу QRNG:

Розмежування доступу. Адміністративний, технічний і операційний доступи до QRNG-системи повинні бути чітко розмежовані з використанням принципу найменших привілеїв.

Внутрішній контроль інсайдерів. Передбачено регулярні перевірки дій співробітників з доступом до критичної інфраструктури. Логування доступу до пристроїв і зміни конфігурацій має бути обов’язковим.

Регулярний аудит безпеки. Незалежна перевірка безпеки сервісу з боку третіх сторін не рідше одного разу на рік забезпечує відповідність актуальним вимогам кібербезпеки.

План реагування на інциденти. Має бути створено формалізований план дій у разі виявлення аномалій, включно з негайною ізоляцією сервісу, повідомленням користувачів та перезапуском QRNG з перевіркою ентропії [14].

Висновки

Проведено комплексне дослідження з метою розробки моделі загроз і моделі порушника для прототипу веб-сервісу QRNG. З огляду на критичну роль QRNG у забезпеченні криптографічної стійкості інформаційно-комунікаційних систем, захист таких сервісів має розглядатися як питання національної та корпоративної безпеки.

Проведений аналіз дозволив виявити низку специфічних загроз, характерних саме для QRNG як веб-сервісу. На відміну від традиційних PRNG (pseudorandom number generators), квантові генератори залежать від фізичних джерел ентропії, які можуть бути піддані впливу як технічного, так і середовищного характеру. Було встановлено, що навіть часткова компрометація фізичного генератора або алгоритмів обробки вихідних бітів може призвести до непередбачуваних наслідків у криптографічних протоколах, що використовують такі дані.

З використанням методології STRIDE побудовано модель загроз, яка враховує ключові активи веб-сервісу QRNG: фізичний пристрій QRNG, API, канали зв'язку, буфери обробки даних, а також логування і моніторинг. Побудовано модель порушника, яка класифікує атакуючих за рівнем доступу, обізнаністю, ресурсною базою та мотивацією.

Результати оцінки ризиків показали, що найбільшу небезпеку становлять загрози, пов’язані з перехопленням або маніпуляцією генерації випадкових чисел, а також фізичним впливом на QRNG.

Враховуючи розроблені модель порушника та модель загроз, обґрунтований та розроблений комплекс рекомендацій, що включає як технічні заходи (TLS, постобробка, аудит), так і організаційні (контроль доступу, інцидент-менеджмент, аудит безпеки) заходи безпеки.

Таким чином, розроблені модель порушника і модель загроз є уніфікованим підходом до оцінки безпеки веб-сервісу QRNG. Використання цих моделей дозволить розробникам і операторам таких сервісів ідентифікувати слабкі місця, мінімізувати ризики компрометації генерації випадкових чисел та зберегти довіру до криптографічних механізмів, що базуються на квантовій ентропії.

Список літератури:

1. M. Herrero-Collantes and J. C. Garcia-Escartin. Quantum random number generators // Rev. Mod. Phys. Marh 2017. Vol. 89, no. 1. P. 015004. DOI: 10.1103/RevModPhys.89.015004
2. T. Lunghi et al. Self-testing quantum random number generator // *Phys. Rev. Lett*. Apr. 2015. Vol. 114, no. 15. P. 150501. DOI:10.1103/PhysRevLett.114.150501
3. M. Stipčević and C. K. Koc. True random number generators // Open Problems in Mathematics and Computational Science. Springer, 2014. P. 275–315. DOI:10.1007/978-3-319-10683-0_12, link: https://cetinkayakoc.net/docs/b08.pdf
4. Microsoft Corporation. The STRIDE Threat Model // Microsoft Docs, 2005. link: https://learn.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)
5. ISO/IEC 27005:2022, Information technology – Security techniques – Information security risk management. International Organization for Standardization, 2022.
6. ДСТЗІ України НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі. Київ, 2000. link: https://tzi.com.ua/downloads/1.4-001-2000.pdf
7. B. Schneier, Attack Trees: Modeling Security Threats, Dr. Dobb's // Journal, 1999. link: https://www.schneier.com/academic/archives/1999/12/attack_trees.html
8. G. McGraw and G. Hoglund, Exploiting Software: How to Break Code, Boston, MA: Addison-Wesley, 2004. link: https://archive.org/details/Exploiting_Software_How_To_Break_Code/mode/2up
9. ДСТЗІ України НД ТЗІ 1.1-002-99. Типове положення про службу захисту інформації в автоматизованій системі. Київ, 1999. link: https://tzi.com.ua/downloads/1.1-002-99.pdf.
10. L. Conklin, V. Drake, S. Strittmatter, Z. Braiterman, A. Shostack. Threat Modeling Process // OWASP.org link: https://owasp.org/www-community/Threat_Modeling_Process#stride-threat--mitigation-techniques.
11. C. Evans, C. Palmer, and R. Sleevi. Transport Layer Security (TLS) Parameters // IETF, RFC 9325, Nov. 2022. link: https://www.rfc-editor.org/rfc/rfc9325
12. D. Hardt. The OAuth 2.0 Authorization Framework // IETF, RFC 6749, Oct. 2012. link: https://tools.ietf.org/html/rfc6749
13. L. Bassham et al. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications // NIST Special Publication 800-22, Rev. 1a, Apr. 2010. link: https://csrc.nist.gov/publications/detail/sp/800-22/rev-1a/final
14. A. Nelson, S. Rekhi, M. Souppaya, K. Scarfone et al. Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile // NIST SP 800-61 Rev. 3, Apr. 2025. link: https://csrc.nist.gov/pubs/sp/800/61/r3/final

Надійшла до редколегії 25.02.2025

Відомості про авторів:

Моргуль Дмитро Миколайович – аспірант кафедри кібербезпеки інформаційних систем, мереж і технологій, Харківський національний університет імені В. Н. Каразіна,; Україна; e-mail: dmitriymdn85@gmail.com; ORCID: https://orcid.org/0009-0007-5272-1634

Нарєжній Олексій Павлович – канд. техн. наук, Харківський національний університет імені В.Н. Каразіна, доцент кафедри кібербезпеки інформаційних систем, мереж і технологій; Україна; e-mail: o.nariezhnii@karazin.ua; ORCID: https://orcid.org/0000-0003-4321-0510

Гріненко Тетяна Олексіївна – канд. техн. наук, доцент, Харківський національний університет радіоелектроніки, доцент кафедри безпеки інформаційних технологій; Україна; e-mail: tetiana.grinenko@nure.ua; ORCID: https://orcid.org/0000-0002-8251-8991

УДК 004.056.5:004.8 **DOI:10.30837/rt.2025.2.221.05**

D.O. KOZIUBERDA, M.V. YESINA, cand. techn. sciences, Yu.L. GOLIKOV

DIGITAL IDENTITY AND ZKP: ANONYMOUS DATA AND SECURE AUTHENTICATION

Introduction

The way we verify our identity and interact in the digital environment is rapidly changing. For decades, digital identification has relied on centralized mechanisms – passwords, social logins, and centralized registries maintained by single providers or authorities. This approach creates critical vulnerabilities: from data leaks and hacks to mass surveillance and manipulation, depriving users of control over their personal information. In this model, centralized intermediaries act as controllers of personal data, which is often collected and processed without proper notification or consent, significantly limiting the individual's ability to influence how their digital identity is used.

In response to these challenges, a new model is emerging – decentralized digital identity (Decentralized Identity, DID). It is based on blockchain technologies and cryptographic primitives that allow individuals to own and store their data independently, as well as control their attestations – without intermediaries or a central authority [1].

One of the key technologies enabling this is zero-knowledge proofs (ZKP). This technology allows verifying the validity of a certain fact without revealing the information itself.

This paradigm of anonymous attestations opens the way to secure authentication that minimizes the amount of personal data transmitted or stored and eliminates the need for constant verification through centralized structures. Moreover, it creates conditions for self-sovereign identity (SSI) – the concept where the user is the sole owner of their digital persona [2].

In this article, we will examine the fundamentals of decentralized identity, the key role of ZKP in privacy protection, standardization initiatives, as well as the practical implications and prospects of combining these technologies in real-world applications.

1. Decentralized Digital Identity

Decentralized identity is an innovative approach to managing digital identity that enables individuals and organizations to independently create, own, and control their digital credentials and identifiers without relying on centralized authorities [1, 3].

Unlike traditional systems governed by governments, corporations, or third-party platforms, decentralized identity utilizes technologies such as Verifiable Credentials (VC), Digital ID Wallets, and blockchain to provide secure, verifiable, and privacy-oriented interactions in the digital space.

A key advantage is that credentials can be issued once, stored by the user in a secure digital wallet, and reused across different systems. This significantly reduces risks, eliminates the need for repeated verifications, and creates a consistent and reliable method of information verification – in finance, healthcare, education, organizational access management (IAM), or supply chains.

By placing the user at the center of the system, decentralized identity offers an effective alternative to fragmented and error-prone traditional identification models.

Key components of decentralized identity [4]:

• Verifiable Credentials (VC) are digital, cryptographically secured representations of identification information that cannot be forged or altered. They are issued by trusted organizations – government agencies, identity verification companies, banks, or other institutions. VCs guarantee the authenticity and integrity of the data, enabling the verification of a user's identity without risk of forgery or fraud. Users store these credentials (attestations) in digital wallets and can present them to verifying parties, disclosing only the necessary information.

• Digital ID Wallets are software tools designed for storing and managing verifiable credentials. They can be implemented as mobile applications or cloud-based solutions, providing conven-

ience and control over personal data. Through these wallets, users can securely share their credentials with various services while maintaining privacy and protection.

• Decentralized Identifiers (DIDs) are globally unique identifiers created and controlled by the user without involvement of a centralized authority. DIDs are typically stored on a blockchain, ensuring their immutability and security. Importantly, DIDs do not contain personal data – they point to decentralized documents that describe the identity subject and include means for authentication.

At the core of decentralized identity is a tripartite trust model that includes [4]:

1. Issuer – a trusted party that creates and signs a verifiable credential. This can be a university, government agency, financial institution, or an identity verification platform.

2. Holder – an individual or organization that receives credentials and stores them in a digital wallet. The holder independently decides how and when to share them.

3. Verifier – a party that needs to verify certain information about the holder: age, license status, education, employment, etc. The verification is performed without direct contact with the issuer, using cryptographic verification.

Fig. 1 depicts this three-party trust model, or decentralized identification system.

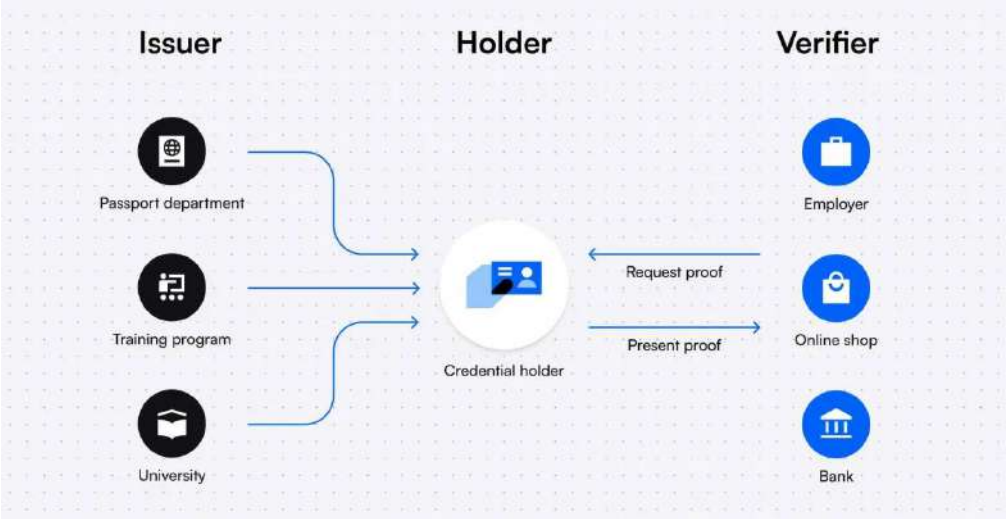

Fig. 1. Three-Party Trust Model (Decentralized Identification System)

This ecosystem enables secure and confidential data exchange between participants without the need to store or repeatedly request sensitive information.

It is also worth examining self-sovereign identity (SSI) in more detail. The terms decentralized identity (DID) and self-sovereign identity (SSI) are often used interchangeably, although there are distinctions between them.

Both concepts are based on the idea that an individual should own and control their digital identity rather than relying on centralized entities – such as governments, online platforms, or corporations – to manage identity on their behalf. However, SSI is a specific approach within the broader landscape of decentralized identity, with a particular focus on user autonomy.

Self-sovereign identity (SSI) is an identity management model in which an individual fully controls their digital attributes: how they are stored, shared, and used – without involving centralized trusted intermediaries. SSI is based on three main components: verifiable credentials, blockchain, and decentralized identifiers (DIDs).

The main difference between decentralized and self-sovereign identity:

• Decentralized identity is a broad concept that encompasses identity systems not governed by a single central authority. It includes both models where the user controls their own identity (e.g., SSI), as well as enterprise-focused models in which control is exercised collectively (e.g., federated Identity and Access Management (IAM) networks that utilize verifiable credentials).

• Self-Sovereign Identity (SSI) is a philosophy and implementation model within the broader decentralized identity paradigm that emphasizes full user control, data minimization, and the principle of privacy by design. In an SSI system, it is the user – not a company or government – who makes the final decision about which data to share, when, and with whom.

Fig. 2 illustrates the components of Self-Sovereign Identity.

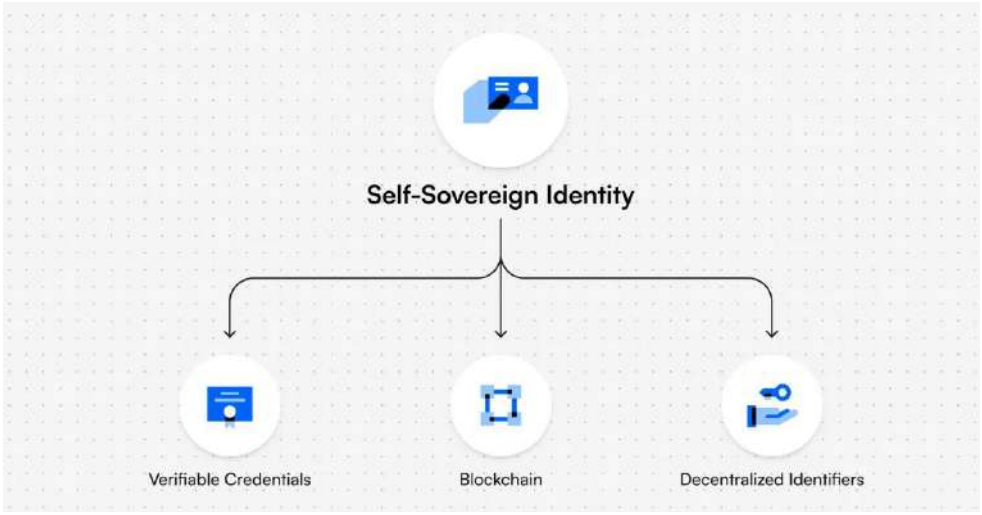

Fig. 2. Self-Sovereign Identity

2. Use of ZKP in decentralized identifiers

Zero-knowledge proof/protocol (ZKP) is an interactive cryptographic protocol that allows one party (the verifier) to be convinced of the truth of any statement (usually mathematical) without gaining any additional information from the other party (the prover).

Zero-knowledge proofs (ZKP) add a new level of privacy and control for the user in decentralized identity solutions. Here is how they enhance DID capabilities in various use cases [4, 5]:

• Selective disclosure. Users can prove specific attributes about themselves (e.g., "I am over 18 years old," "I have a valid driver's license") without revealing the underlying data. This ensures necessary verification while preserving privacy.

• Minimal data sharing. Instead of sharing entire documents or personal data, ZKPs enable precise identity verification using only the minimally required information. This reduces disclosure of sensitive data and lowers the risk of misuse.

• Enhanced trust. ZKPs guarantee the authenticity of information without requiring centralized trust in the identity data provider. They facilitate interaction between parties that otherwise would not trust each other with personal data.

• Reputation systems. ZKPs can support privacy-preserving reputation systems based on verified credentials. Users can prove they possess certain qualifications or meet requirements without fully revealing their identity.

• Decentralized access control. ZKPs can provide fine-grained access control in decentralized systems. Users can prove they have access rights to specific resources or services without disclosing unnecessary personal information.

• Correlation prevention. ZKPs can be used to create unique, unlinkable proofs each time credentials are used. This prevents tracking and the creation of detailed behavioral and identity profiles of individuals.

• Private electronic voting. Election integrity is critical, but voter anonymity is also important. Systems combining DID and ZKP enable mechanisms where a voter's identity can be verified without linking to a specific vote. ZKPs allow verification of voting eligibility and prevent double voting while preserving ballot secrecy.

• Medical data protection. Medical information is among the most sensitive data categories. ZKPs within the decentralized identity model give patients control over their medical records. Users can decide themselves who and to what extent can access their data – for example, doctors for treatment or researchers for scientific purposes – without revealing the full content of records. This opens possibilities for confidential medical research without compromising patient privacy.

There are two types of zero-knowledge proofs for identification: interactive and non-interactive.

In the interactive version, the prover must perform a series of tasks to confirm their knowledge of certain facts. For providing self-sovereign identity, this method often uses principles of mathematical probability.

The non-interactive zero-knowledge proof utilizes decentralized identity management and does not require interaction between the prover and the verifier.

Both types of zero-knowledge proofs include the following three requirements:

1. Soundness. If the prover provides incorrect or missing information, the verifier will not be convinced, since the statement cannot be falsified.

2. Completeness. If the statement is true, the verifier is confident that the prover possesses all the necessary information.

3. Zero-knowledge. The verifier gains no additional information about the prover, ensuring the anonymity of personal and sensitive data.

One of the earliest scientific works on zero-knowledge proofs, first published in 1988, presents a new identification scheme based on such proofs, which is a more efficient alternative to RSA-based schemes. In identification schemes, subject A verifies their identity to subject B using some constant value S in the form of a value or a physical card, without giving subject B the ability to later impersonate A. Traditional identification schemes use encryption and/or hashing together with credentials such as digital passwords, PIN codes, credit card chips, etc. This work proposes a practical scheme that makes it impossible even for an experienced attacker to collude with a dishonest verifier B to create forged credentials and impersonate A.

The methodology is based on interactive proofs, where a subject can confirm their identity by proving knowledge of the secret key of their credentials without revealing the secret itself. It is sufficient to provide proof of knowledge of the secret, which serves as a digital signature unique to each individual. The article describes a scheme that does not require a directory (i.e., a centralized repository of public keys or identity data). It also proposes implementing such a scheme using hypothetical "smart cards," which can act as physical credentials generating zero-knowledge proofs of identity using microprocessors – for use in everyday identity verification.

The zk-creds protocol uses zero-knowledge proofs (specifically zk-SNARKs) to transform existing identity documents into anonymous credentials, eliminating the need for issuers of such credentials to store signing keys. This system differs from traditional methods where issuers sign credentials and identity documents for verification. By integrating with existing identification infrastructures – such as government ID cards or university diplomas – zk-creds transforms these traditional credentials into a digital, anonymous, yet verifiable format [5].

3. Architecture and Standards of the Ecosystem: Trends and Innovations

Key points highlighting the importance of standardization:

• Compatibility. Common standards ensure seamless interaction between different decentralized identity solutions and platforms.

• Adoption. Standardization fosters trust and lowers barriers for businesses and users interested in decentralized identity.

• Ecosystem development. A harmonized set of standards stimulates innovation and collaboration across the decentralized identity space.

Table 1 below presents key initiatives and their role in the standardization of digital identity.

Table 1

Major frameworks and projects in digital identity standardization

Initiative	Focus	Role in Standardization
W3C Verifiable Credentials	Establishes standards for the format and structure of verifiable credentials, covering their issuance, presentation, and cryptographic signatures.	Provides a common representation of verifiable credentials, enhancing interoperability between different systems.
Decentralized Identity Foundation (DIF)	Develops open-source protocols, specifications, and tools to ensure interoperability within the decentralized identity ecosystem.	Promotes collaboration and the creation of common standards so that various decentralized identity solutions can interoperate.
Hyperledger Indy and Aries	Projects focused on developing decentralized enterprise-grade identity solutions with built-in privacy protection features, including integration of zero-knowledge proofs (ZKP).	Support standardization in enterprise environments by ensuring implementations meet scalability, security, and business process requirements.

The field of decentralized identity based on zero-knowledge proofs (ZKP) is dynamic, focused on addressing challenges and pushing the boundaries of what is possible. Let's consider several promising research directions [6]:

• Advanced ZKP schemes. Research into more efficient zero-knowledge proof systems tailored to the specific requirements of decentralized identity use cases, improving performance.

• Credential (attestation) aggregation. The ability to use ZKP to simultaneously prove compliance with multiple criteria will expand applications in complex identity-related scenarios.

• Hybrid privacy solutions. In some cases, combining ZKP with other privacy-enhancing technologies, such as secure multiparty computation, can offer the best balance between efficiency, privacy, and functionality.

• Social recovery mechanisms. Providing convenient ways for users to recover lost or compromised DIDs and related credentials in a decentralized manner is a key usability challenge.

It is also worth mentioning several leading solutions driving the development of decentralized identity based on ZKP [6, 7]:

1. zkKYC by Polygon. Polygon's solution utilizes zero-knowledge proofs to verify identity while preserving privacy, simplifying registration on decentralized finance (DeFi) platforms and other services. Built on Polygon ID, a decentralized identity platform, zkKYC enables users to prove compliance with specific criteria (e.g., being over 18 years old or residency) without revealing the exact values of those attributes.

From a technical standpoint, Polygon ID is based on the Iden3 protocol and the Circom language for constructing zk-proofs. This stack is used to create so-called zkSNARKs (Succinct Non-interactive Arguments of Knowledge) – concise cryptographic proofs that can be verified without revealing the underlying information on which they are based.

The system supports:

• Self-Sovereign Identity (SSI) – a model where identity belongs directly to the user without reliance on centralized providers.

• Selective disclosure – the ability to provide only the portion of information necessary for a specific verification.

• On-chain verification – verification performed by a smart contract directly on the blockchain, enabled by a specialized proof query language (ZK Query Language).

This solution is actively used in the context of decentralized finance (DeFi), where it is important to combine service accessibility with compliance to AML/KYC requirements (anti-fraud mechanisms). zkKYC also enables the creation of trust systems in which individuals retain full control over their credentials.

zkKYC is an example of an effective implementation of privacy, scalability, and regulatory compliance principles through the use of advanced cryptographic methods.

2. Sismo Protocol. Sismo applies ZKP to reputation systems and privacy-preserving badges within Web3 communities, allowing users to prove their contributions while controlling what information they disclose.

Its architecture is based on zero-knowledge proofs, enabling users to demonstrate their activity or status without revealing any link to specific identifiers (such as wallet addresses or social media accounts).

Sismo consists of several key components:

• Data Vault – a local storage of attributes (identifiers) fully controlled by the user. Attributes may include data from Ethereum, Twitter (X), or GitHub, for example.

• ZK Badges – unique cryptographic badges that act as soulbound tokens (tokens that cannot be transferred to others). They certify membership in a particular group or achievement without revealing the source of these achievements.

• Sismo Connect – an interface (SDK/API) that allows web applications to receive ZK proofs from users to grant access or verify certain conditions.

Unlike classical authentication systems where a user provides a login or password, Sismo allows confirming statements like "I am a member of DAO X" or "I have more than 1 ETH in my wallet" without revealing who you actually are.

This approach opens possibilities for:

• Confidential voting within DAOs;

• Reputation systems for participation in airdrops;

• Anonymous access to Web3 services based on attributes or achievements.

Sismo plays a crucial role in the development of Web3 identities by simultaneously providing privacy, verifiability, and flexibility for integration with existing decentralized services.

3. Self-Sovereign Identity (SSI) by Evernym. A comprehensive decentralized identity platform that uses standards and is oriented towards interoperability, supporting zero-knowledge proofs (ZKP) for selective disclosure of attributes.

In this model, users receive, store, and manage their verifiable credentials independently of centralized authorities.

Technological foundation of the platform:

• Hyperledger Indy – a specialized blockchain for identity, supporting decentralized registries of DIDs (Decentralized Identifiers).

• Hyperledger Aries – a set of protocols and tools for agents (software interfaces) that exchange credentials between users, organizations, and services.

• Verifiable Credentials – standardized W3C documents that can be issued, verified, and revoked.

The platform supports zero-knowledge proofs, enabling users to selectively disclose only parts of credential attributes.

Key features of Evernym:

• User control over data – all credentials are stored in a local "agent" (an app or module) that shares data only with the owner's permission.

• High integration capability – supports enterprise needs such as revocation, auditing, and credential lifecycle management.

• Participation in global standardization – Evernym has played a key role in developing W3C specifications and the Decentralized Identity Foundation.

Conclusions

The combination of Decentralized Identity (DID) and Zero-Knowledge Proofs (ZKP) represents a radical step toward a safer, more private, and user-centric internet. Such a system enables individuals to control their own data, interact in the digital space without relying on centralized intermediaries, and prove facts (e.g., age or education) without revealing unnecessary information.

Although the technology is rapidly evolving, it faces several challenges: usability complexity for ordinary users, the risk of key loss, a limited number of trusted credential issuers, and the need for interoperability at a global level. Additionally, legal recognition of digital credentials across different jurisdictions remains an open issue.

Decentralized identity based on ZKP is key to secure, private, and scalable digital interactions. It addresses fundamental problems of centralized systems such as data breaches, redundant verifications, and limited user autonomy. The combination of DID and ZKP forms a new paradigm of digital identity management focused on security, privacy, and user autonomy. DID ensures the storage and control of credentials in a personal environment, while ZKP allows attribute verification without revealing the underlying data. Despite existing technical, regulatory, and user adoption barriers, the intensive development of standards, infrastructure, and governmental initiatives indicates a transition of this model from conceptual stages to practical implementation. In the future, it has the potential to become the foundation of a secure, interoperable, and sovereign digital identity on a global scale.

Further research and development in this field will contribute to improving existing mechanisms, increasing their accessibility, and adapting them to diverse application scenarios – from the financial sector to government services and everyday digital interactions.

References:

1. Camenisch J., Drijvers M., Lehmann A. Anonymous attestation using the strong Diffie-Hellman assumption revisited. Trust and Trustworthy Computing: 9th International Conference, TRUST 2016, Vienna, 29–30 August 2016. 2016. P. 1–20.

2. Reed D., Preukschat A. Self-Sovereign Identity. 2nd ed. Shelter Island, NY : Manning, 2021. 374 p.

3. Decentralized Identifiers (DIDs) v1.0: core architecture, data model, and representations. World Wide Web Consortium (W3C). [Electronic resource]. Available at: https://www.w3.org/TR/did-1.0/.

4. A Survey on Decentralized Identifiers and Verifiable Credentials / C. Mazzocca et al. IEEE Communications Surveys & Tutorials. 2025. P. 7.

5. A Survey on the Applications of Zero-Knowledge Proofs / R. Lavin et al. arXiv preprint arXiv:2408.00243. 2024. [Electronic resource]. Available at: https://arxiv.org/abs/2408.00243.

6. Fischlin S. Formalising Zero-Knowledge Proofs in the Symbolic Model : master's thesis. Zurich, 2021. 76 p.

7. Decentralized Identity: The Ultimate Guide. dock labs. [Electronic resource]. Available at: https://www.dock.io/post/decentralized-identity.

Received 15.03.2025

Information about the authors:

Koziuberda Dmytro Olexandrovych – Cybersecurity Master, Faculty of Computer Sciences, V.N. Karazin Kharkiv National University; development employee of LLC “LADYZAIN”, Ukraine; e-mail: koziuberda.dmytro@gmail.com; ORCID: https://orcid.org/0009-0005-3088-9685

Yesina Maryna Vitaliivna – cand. techn. sciences, associate professor, acting duties of the head of the Department of Cybersecurity of Information Systems, Networks and Technologies in V.N. Karazin Kharkiv National University; Researcher and Head of the international department in JSC "IIT", Ukraine, e-mail: m.v.yesina@karazin.ua; ORCID: https://orcid.org/0000-0002-1252-7606

Golikov Yurii Leonidovych – CEO and Founder of DevBrother tech company, USA, e-mail: yuriy@devbrother.com, ORCID: https://orcid.org/0009-0008-7946-4663

УДК 004.056.5 **DOI:10.30837/rt.2025.2.221.06**

А.М. ЄВГЕНЬЄВ, З.М. СИДОРЕНКО, О.В. СЄВЄРІНОВ, канд. техн. наук

ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ ДАНИХ У СИСТЕМАХ ПРОМИСЛОВОГО ІНТЕРНЕТУ РЕЧЕЙ НА ОСНОВІ ВИКОРИСТАННЯ ЗАВАДОСТІЙКИХ КОДІВ

Вступ

Промисловий Інтернет речей (Industrial Internet of Things, IIoT) – це сучасна технологія, яка об'єднує інтелектуальні сенсори, пристрої та програмне забезпечення з метою автоматизованого контролю, збору даних і управління виробничими процесами. Попри значні переваги, впровадження IIoT несе ряд серйозних проблем безпеки, які можуть призвести до витоку конфіденційної інформації, фінансових втрат або фізичної шкоди для обладнання та персоналу. Одним із основних викликів, пов'язаних з безпекою IIoT, є забезпечення цілісності інформації, тобто збереження її точності, достовірності та незмінності протягом усього життєвого циклу – від збору до обробки й зберігання [1].

Порушення цілісності даних у IIoT-системах може спричинити збої у функціонуванні обладнання, виробничі інциденти та суттєве зниження рівня довіри до системи. В умовах промислового середовища, де активно застосовуються автоматизовані технології та велика кількість взаємодіючих пристроїв, ця проблема набуває особливої гостроти.

Мета статті – розглянути наявні підходи до забезпечення цілісності даних у IIoT та проаналізувати можливості використання завадостійких кодів, зокрема кодів Гоппи, для підвищення рівня інформаційної безпеки.

Основні проблеми безпеки IIoT

Незважаючи на такі переваги впровадження IIoT, як підвищення ефективності та зниження витрат, впровадження таких систем породжує низку викликів у сфері інформаційної безпеки.

По-перше, це застаріле або вразливе програмне забезпечення пристроїв IIoT. Через тривалий життєвий цикл промислових пристроїв оновлення програмного забезпечення може бути складним або навіть неможливим. У результаті багато елементів IIoT залишаються відкритими до атак через відомі вразливості.

По-друге, це відсутність шифрування або його недостатній рівень. У багатьох випадках дані передаються між пристроями IIoT у відкритому вигляді або з використанням застарілих методів шифрування, що дозволяє зловмисникам проводити атаки "людина посередині", перехоплювати або модифікувати інформацію.

Проблемним питанням є відсутність єдиних стандартів безпеки. Відсутність загальноприйнятих стандартів безпеки для IIoT-пристроїв призводить до хаотичного підходу до їх розробки та інтеграції. Також використання різних виробників створює труднощі у забезпеченні єдиної політики безпеки.

Крім того, багато пристроїв IIoT мають обмежені обчислювальні ресурси, що ускладнює реалізацію на них складних протоколів автентифікації. IIoT-пристрої часто використовують слабкі або стандартні паролі за замовчуванням, не мають механізмів багатофакторної автентифікації. Тому вразливості в автентифікації можуть призвести до того, що зловмисники отримають несанкціонований доступ до даних систем.

Однією з головних проблем IIoT є забезпечення цілісності даних. У промислових середовищах навіть незначне спотворення даних може мати серйозні наслідки: порушення технологічного процесу, аварії обладнання або вихід з ладу систем управління. Дані, що передаються від датчиків або приймаються автоматизованими системами, повинні залишатися незмінними під час передачі і зберігання. Проте через велику кількість вузлів і слабкий

захист деяких пристроїв ця інформація може бути перехоплена, змінена або знищена без виявлення даного факту.

Для забезпечення цілісності даних пропонується застосовувати нові підходи, що поєднують сучасні криптографічні засоби та завадостійке кодування.

Методи забезпечення цілісності даних в системах IIoT

На сьогодні для збереження цілісності в промислових мережах застосовуються такі рішення [1]:

– криптографічні геш-функції на основі алгоритмів SHA-2, SHA-3 для формування контрольної суми (гешу);

– цифрові підписи з використанням алгоритмів RSA, ECDSA, постквантових схем на решітках;

– захищені протоколи передачі даних з шифруванням (TLS, DTLS, MQTT-SN), що реалізують контроль цілісності, наприклад, через HMAC;

– апаратні модулі безпеки (TPM, HSM), які забезпечують автентифікацію пристроїв;

– зберігання інформації з пристроїв IIoT у блокчейні або розподілених реєстрах, де будь-які зміни реєструються.

Проте, попри розвиток цих технологій, вони не завжди ефективно захищають від усіх можливих загроз, зокрема через неможливість виправлення помилок, спричинених перешкодами або збоями. Крім того, більшість традиційних алгоритмів шифрування, як-от AES, RSA або ECC, не гарантують стійкості в умовах постквантового періоду.

Саме тому перспективним напрямом є інтеграція криптографії з методами завадостійкого кодування.

Тривалий час відомі кодові криптосистеми McEliece, Rao-Nam і Niederreiter – це криптографічні системи, що базуються на завданнях теорії завадостійкого кодування, зокрема, на складності декодування випадкового лінійного блочного коду – однієї з фундаментальних задач у теорії завадостійкого кодування. Кодові криптосистеми також демонструють високу продуктивність (швидкість обчислень), перевищуючи традиційні криптографічні системи, як-от RSA чи ECC. Їхня особливість – стійкість до атак квантових комп'ютерів, що робить їх перспективними для постквантової криптографії [5, 6].

Забезпечення цілісності інформації полягає у введенні в інформацію надмірності (автентифікатора), що дозволяє з заданою імовірністю встановлювати дійсність переданого повідомлення. Різниця між кодами автентифікації і завадостійкими кодами полягає в тім, що більшість завадостійких кодів мають одне правило кодування, а коди автентифікації мають багато правил кодування, з яких передавач або приймач може вибирати для використання одне ключове (секретне) правило.

Основою двоключової криптосистеми McEliece та одноключової системи Rao-Nam є коди Гоппи – один із підкласів альтернантних кодів, що мають кращі характеристики серед лінійних блокових кодів. Їх ключова перевага полягає в можливості побудови великої кількості кодів із заданими параметрами. Саме це робить коди Гоппи придатними для криптографічних цілей та відкриває можливості для одночасного досягнення високої завадостійкості та цілісності даних у IIoT, а також дозволяють перетворювати інформацію з високою швидкістю.

Аналіз можливостей кодів Гоппи щодо забезпечення цілісності та завадостійкості даних у системах IIoT

Широко застосовувані для захисту від помилок завадостійкі коди не забезпечують цілісності інформації, оскільки мають одне правило кодування, що відповідає фіксованому коду. Отже, можна припустити, що використання для підвищення достовірності даних завадостійких кодів, що мають досить багато правил кодування, дозволить забезпечити цілісність

інформації, що передається, якщо обране правило кодування тримається в таємниці від зловмисника.

Реалізація цього припущення може бути пов'язана із застосуванням кодів Гоппи, які мають найкращі характеристики класу лінійних блокових кодів. Характерною властивістю кодів Гоппи є той факт, що є велика кількість способів формування коду із заданими параметрами, що потенційно може вирішити задачу не тільки забезпечення високої стійкості до завад, але і цілісності даних в системах IIoT.

Коди Гоппи є підкласом альтернативних кодів, які у свою чергу тісно пов'язані з узагальненими кодами Ріда–Соломона (ОРС) [7 – 9]. Коди Гоппи формують широку категорію кодів, до якої належать БЧХ-коди, коди Срівестави, а також узагальнення Ченя–Чоя. Вони мають доведені характеристики на границі Варшамова–Гілберта, що робить їх ефективними для створення безпечних та надійних систем передачі даних. Крім того, завдяки наявності великої кількості багаточленів $G(x)$, які задають код з параметрами не нижчими від заданих, ці багаточлени можуть виступати в ролі криптографічного ключа.

Крім того, велика кількість багаточленів Гоппи, що визначають код з параметрами не гірше заданих, дозволяє використовувати дані коди для контролю цілісності даних, а можливість визначення всієї множини кодових слів за допомогою одного багаточлена дозволяє останній використовувати як ключ відносно невеликої довжини.

Для визначення q-ичного коду Гоппи [8, 9] довжини n використовуються два об'єкти:

– многочлен Гоппи $G(x)$ ступеня t з коефіцієнтами з поля GF(q^m);

– підмножина $L=\{\alpha_1, \alpha_2, ..., \alpha_n\}$ така, що всі елементи L різні, а α_i належить GF(q^m) і $G(\alpha_i)\neq 0$ для всіх $\alpha_i=L$.

Код Гоппи прийнято позначати Г(L,G)-код.

Коди Гоппи є одним з небагатьох класів лінійних блокових кодів, що мають велику кількість законів формування при фіксованих параметрах коду, що явно спричинило створення на їх основі систем криптозахисту. Така система вперше була запропонована Мак-Елісом як система з відкритим ключем [10]. У системі Мак-Еліса секретний ключ складається з матриці, що породжує, двійкового коду Гоппи G, невиродженої матриці S і матриці перестановок P, які її маскують. Відкритим ключем є матриця кодування $G'=S\cdot G\cdot P$ звичайного лінійного коду. При шифруванні повідомлення x множиться на відкриту матрицю кодування G' і до результату додається локально згенерований шумовий блок z. Щоб розшифрувати отриманий шифртекст v необхідно помножити його на P^{-1}, декодувати $v\cdot P^{-1}$, отримавши в результаті слово в коді Гоппи, а потім помножити це слово на S^{-1}, відновивши тим самим вихідне повідомлення x.

Іншим варіантом використання кодів Гоппи є модифікована система Рао–Нама [10], в якій матриця коду Гоппи G, що породжує, є секретним ключем. При зашифруванні повідомлення x випадково вибирається вектор помилок z і обчислюється шифртекст $v = x\cdot G + z$. Якінебудь способи розкриття такої криптосистеми поки що не відомі. Ця система не використовувалася раніше, як і система Макеліса, через велику довжину ключа, що дорівнює $k\cdot n$ символів матриці коду, що породжує, в двійковому випадку.

Пропонується для забезпечення цілісності та завадостійкості даних в якості ключа замість матриці, що породжує, вибирати примітивний багаточлен Гоппи $G(x)$ і перетворення виконувати в частотній області. В цьому випадку загальна кількість ключів системи визначається кількістю багаточленів примітивної довжини, що не приводяться, $N_q(t)$ (рис. 1).

Аналіз отриманих результатів показує, що зі збільшенням довжини n коду Гоппи при фіксованій мінімальній відстані $d=2t+1$ кількість багаточленів ступеня t, що не приводяться, росте набагато швидше, ніж при збільшенні ступеня багаточлена при фіксованій довжині коду n (чи відповідно фіксованого розміру поля q). Це означає, що довгі коди є кращими з погляду працевтрат на розкриття їхнього закону формування.

Оцінка можливості кодів Гоппи щодо забезпечення цілісності

Оцінимо можливості скорочених кодів Гоппи щодо забезпечення цілісності у випадку вибору зловмисником стратегії нав'язування помилкових даних. При випадковому виборі зловмисником *n*-послідовностей імовірність нав'язування буде розраховуватися згідно з виразом

(1)

де n – довжина коду Гоппи; k – кількість інформаційних символів коду Гоппи; t – кількість помилок, що виправляються кодом.

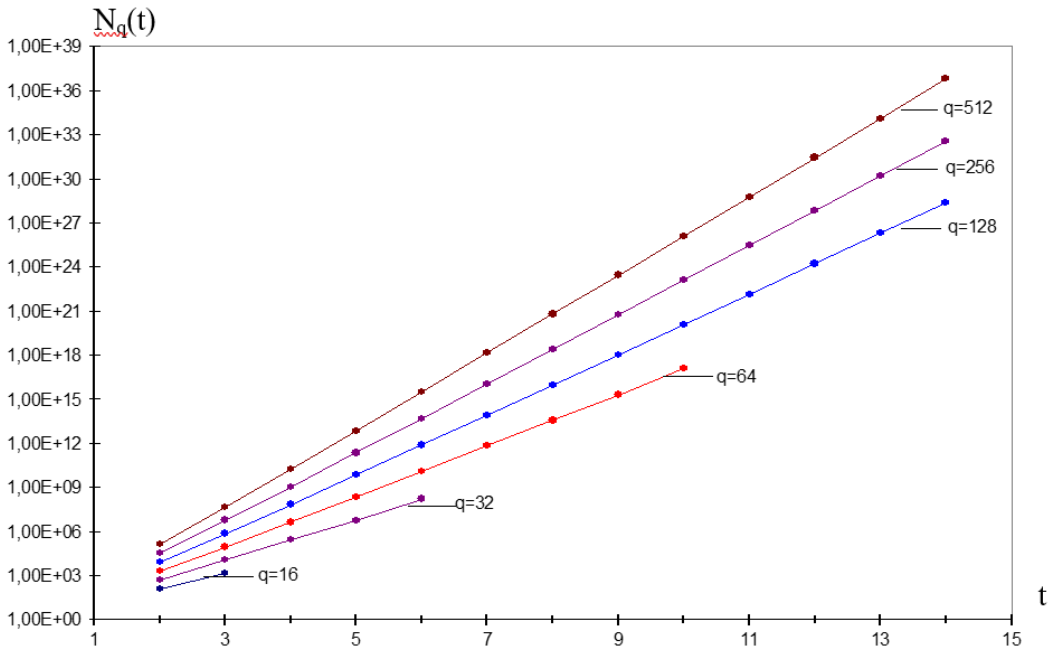

Рис. 1. Залежність кількості багаточленів Гоппи, що не приводяться, $N_q(t)$ від їх ступеня t для різних полів Галуа GF(q)

На рис. 2 представлено залежності імовірності нав'язування $P_{нав.}$ від довжини двійкових кодів Гоппи при швидкості коду R = 1/3, 1/2, 2/3.

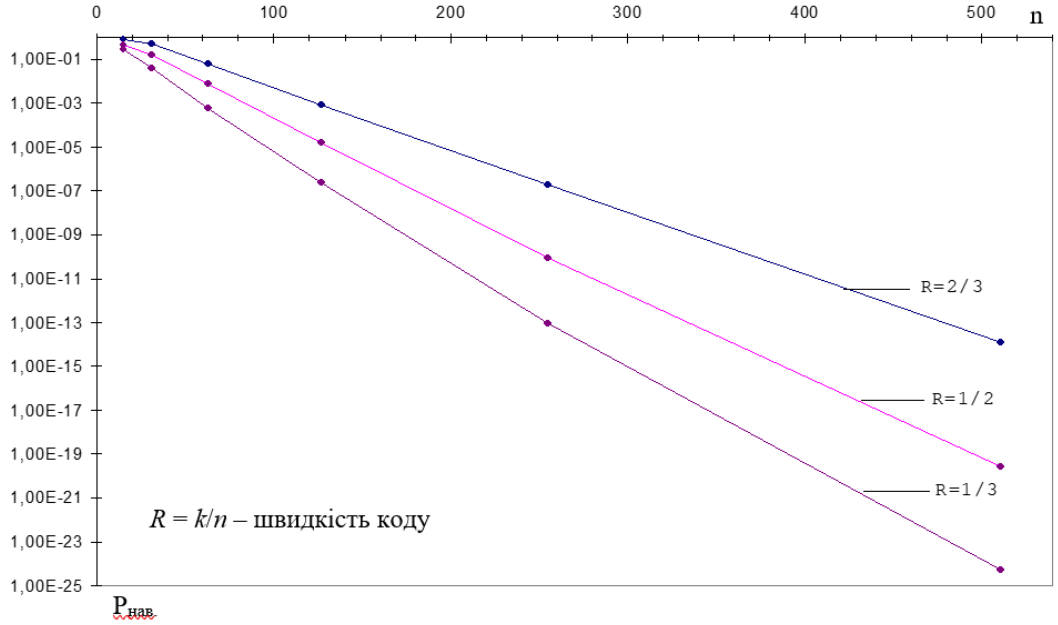

Рис. 2. Залежність імовірності нав'язування $P_{нав.}$ від довжини двійкових кодів Гоппи

Аналіз даних залежностей показує, що зменшення швидкості і збільшення довжини коду приводить до зниження імовірності нав'язування. Це пояснюється зменшенням відношення кількості кодових слів до кількості всіляких n-послідовностей з ростом довжини коду.

Отже, при використанні в системі IIoT кодів Гоппи вираз (1) дає верхню границю імовірності нав'язування.

Висновки

Аналіз класу лінійних блокових кодів – кодів Гоппи показав, що останні володіють високими потенційними можливостями для забезпечення цілісності і завадостійкості каналів передачі даних. Для даних кодів довжини порядку 256 символів загальне число правил кодування є порівнянним із загальним числом ключів існуючих криптосистем, а для кодів більшої довжини значно перевершує, що робить їх перспективними для застосування у постквантову епоху. Аналіз криптостійкості за умови, що зловмиснику невідомий закон формування коду, дозволяє зробити висновок про можливість суттєвого зниження імовірності нав'язування помилкових повідомлень на основі використання таких кодів при збереженні заданих вимог по завадостійкості. Для кодів з фіксованою швидкістю R імовірність нав'язування суттєво знижується зі збільшенням довжини коду n.

Таким чином, застосування кодів Гоппи в системах IIoT може забезпечити не лише завадостійке кодування, а й захист цілісності даних. Це робить їх перспективним рішенням у сфері побудови надійних, захищених і стійких до майбутніх викликів інформаційних систем у промисловості.

Список літератури:

1. Сирадоєв А.О., Можаєв О.О. (2024). Дослідження споживчого і промислового Інтернету речей.

2. Melenti Y. et al. Development of post-quantum cryptosystems based on the Rao-Nam scheme // Eastern-European Journal of Enterprise Technologies. 2025. 1 (9(133)). P. 35–48.

3. Керничний В., Сєвєрінов О.В. Аналіз стійкості криптосистеми McEliece // Global Cyber Security Forum: матеріали Першого міжнародного науково-практичного форуму, 14 – 16 листоп. 2019 р. Харків : ХНУРЕ, 2019. С. 55–56.

4. Шипілов Д.В., Халімов Г.З. Аналіз постквантової криптосистеми McEliece // Комп'ютерні та інформаційні системи і технології. ХНУРЕ, 2019. С. 83–84.

5. Dam D. T., Tran T. H., Hoang V. P., Pham C. K., & Hoang T. T. A survey of post-quantum cryptography: Start of a new race // Cryptography. 2023. 7(3). P 40.

6. Melenti Y., Korol O., Shulha V., Milevskyi S., Sievierinov O., Voitko O., ... & Pashayeva S. DEVELOPMENT OF POST-QUANTUM CRYPTOSYSTEMS BASED ON THE RAO-NAM SCHEME // Eastern-European Journal of Enterprise Technologies. 2025. 133(9).

7. Blahut R. E. (1983). Theory and practice of error control codes. (No Title).

8. Goppa V. D. A new class of linear error-correcting codes // Probl. Inf. Transm. 1970. № 6. P. 300–304.

9. Tsfasman M.A., Vladut S.G., Zink Th. Modular Gurves, Shimura Gurves and Goppa Codes, Bitter than Varshamov-Gilbert Bound // Math. Nachrichten. 1982. Vol. 109. P. 21–28.

10. Diffie W. (1988). The first ten years of public-key cryptography // Proceedings of the IEEE. 1988. № 76(5). P.560–577.

Надійшла до редколегії 14.03.2025

Відомості про авторів:

Євгеньєв Андрій Михайлович – Харківський національний університет радіоелектроніки, аспірант кафедри безпеки інформаційних технологій, факультет комп'ютерної інженерії та управління, Україна; e-mail: andrii.yevheniev@nure.ua; ORCID: https://orcid.org/0000-0003-4365-5675

Сидоренко Зоя Михайлівна – Харківський національний університет радіоелектроніки, аспірантка кафедри безпеки інформаційних технологій, факультет комп'ютерної інженерії та управління, Україна; e-mail: zoia.sydorenko@nure.ua; ORCID: https://orcid.org/0000-0002-0104-6807

Сєвєрінов Олександр Васильович – канд. техн. наук, доцент, Харківський національний університет радіоелектроніки, професор кафедри безпеки інформаційних технологій, факультет комп'ютерної інженерії та управління, Україна; e-mail: oleksandr.sievierinov@nure.ua; ORCID: https://orcid.org/0000-0002-6327-6405

УДК 004.056.5 **DOI:10.30837/rt.2025.2.221.07**

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

ІДЕЯ ЗЛАМУ ГЕШ-ФУНКЦІЇ НА КВАНТОВІЙ ШВИДКОСТІ

Вступ

Квантові комп'ютери доволі швидко опановують світ. Так, є припущення експертів, що квантовий комп'ютер зможе впоратися зі 2048 бітовим шифруванням вже наприкінці 2030-х років.

Критично важливі елементи структури кібербезпеки державного управління, військового та промислового комплексу залишаються незмінними протягом десятиріч з перспективою їх подальшого використання. Стають зрозумілими спроби зі сторони зловмисників заволодіти великими об'ємами зашифрованих даних з надією їх накопичити та розшифрувати у майбутньому за допомогою квантових комп'ютерів – метод HNDL (Harvest Now, Decrypt Later – «Збери зараз, розшифруй пізніше»). Інформація, яку зашифрували з використанням криптографічних стандартів, що не є квантово-безпечними, може вважатися втраченою.

Вже існують так звані квантово-центричні суперкомп'ютери. Це досить складна обчислювальна архітектура, яка використовує при обчисленнях переваги паралельних обчислень з використанням одночасно квантових та класичних обчислень. Саме такі гібридні обчислювальні системи в найближчий час можуть бути основною загрозою для більшості класичних криптоалгоритмів.

До основних методів і задач криптоаналізу, що можуть бути вирішені за допомогою квантового комп'ютера та становлять загрозу для сучасних крипто перетворень, можна віднести наступні [1 – 3]:

1) алгоритм Гровера для пошуку в несортованій базі;

2) алгоритм факторизації Шора;

3) алгоритм Шора для розв'язку дискретного логарифму в скінченному полі;

4) алгоритм Шора для розв'язку дискретного логарифму в групі точок еліптичної кривої.

Саме через загрозу з боку квантових технологій у 2016 р. NIST розпочав конкурс щодо розробки квантово-безпечних стандартів з оприлюдненням вимог до майбутніх розробок [4 – 7]. Було проведено три раунди з відбору кандидатів на стандартизацію, розроблено проєкти стандартів та продовжено дослідження в четвертому раунді.

Постквантова криптографія (PQC) є головним пріоритетом національної безпеки розвинених держав, які готуються переходити до квантово-безпечних практик.

У травні 2021 р. Президент України підписав «Про Стратегію кібербезпеки України» [8].

У січні 2024 р. було опубліковано ключові ідеї квантової стратегії НАТО. Передбачено спрямовувати співпрацю НАТО з промисловістю для розвитку трансатлантичної екосистеми квантових технологій, одночасно готуючи НАТО до захисту від зловмисного використання квантових технологій.

Квантово-безпечна криптографія вже існує. Є декілька підходів до розробки алгоритмів, що не є вразливими до атак квантовими комп'ютерами. Це криптографія заснована на: алгебраїчних решітках, геш-функціях, математичних кодах, багатовимірній криптографії та ізогеніях суперсингулярних еліптичних кривих.

Постквантова криптографія на основі геш-функцій

Злам геш-функції означатиме наступне: виходячи з відповідного гешу знайти повідомлення, з якого цей геш було сформовано зі складністю менш, ніж O(n). Якщо це неможливо зробити, функція вважається криптографічно стійкою.

Вхідний набір даних найчастіше кодується у ASCII або двійковому форматі, а вихідний – у шістнадцятковому.

Квантовий комп'ютер за допомогою відомого алгоритму Гровера здатен знайти принаймні одне повідомлення, пов'язане з даним гешем зі складністю O(n/2), що значно краще, ніж O(n) з використанням класичного комп'ютера.

Багато прикладів використання алгоритму Гровера викликають розчарування: вони починають із кодування рішення в квантову схему Oracle, а потім запускають алгоритм Гровера, щоб знайти рішення, яке ми вже знаємо.

У [9] запропоновано цікаву ідею – закодувати саму геш-функцію в Oracle, а не рішення. У даному випадку алгоритм не знає рішення: він знає лише алгоритм гешування і геш-функцію, як і будь-який потенційний супротивник.

Для отримання справжнього криптографічного гешу, наприклад для алгоритму SHA2, знадобляться десятки тисяч квантових гейтів і реєстр із 128 кубітів (не рахуючи вражаючої кількості допоміжних кубітів) квантового комп'ютеру.

Для демонстрації ідеї запропонована вигадана геш-функція **(toy)**, яка працює від вхідного набору {0,1}**6 до цільового набору {0,1}**4, що використовує лише два квантові вентилі XOR і 6 кубітів. Ця функція не володіє добрими криптографічними властивостями і призначена лише показати цей підхід без втрати загальності [10].

```
def toy(message):
    message[0] = message[4] ^ message[5]
    message[2] = message[5] ^ message[0]
    return message
```

Кодування геш-функції в AWS Braket.

Згідно з ідеями [9, 10] виконуємо чотири кроки:

- обчислюємо геш (toy) з квантовими вентилями;
- позначаємо квантові стани, що відповідають заданому значенню геш-функції;
- uncompute toy () для скидання реєстру кубітів;
- посилюємо розмітку за допомогою оператора дифузії.

1. Комп'ютерна функція toy.

У AWS Braket можна представити функцію dream наступним чином:

```
@circuit.subroutine(register=True)
def quantum_hash():
    ocirc=Circuit()
    ocirc.ccnot(4,5,0).ccnot(5,0,2)
    return ocirc
```

@circuit.subroutine(register=True) – декоратор, який реєструє функцію quantum_hash як підпрограму у квантовому контексті;

ocirc = Circuit() – створюється новий квантовий цикл;

ocirc.ccnot(4, 5, 0) – елемент CCNOT (Toffoli-гейт), що застосовується до кубітів 4 і 5 (контрольні), впливає на кубіт 0 (цільовий);

ocirc.ccnot(5, 0, 2) – ще один Toffoli-гейт, де контрольні кубіти – 5 і 0, а цільовий – 2;

return ocirc – повертає побудовану квантову схему.

Для надання всього простору повідомлень завдовжки 6 бітів вводяться 6 кубітів, що охоплюють 2^6=64 можливих повідомлення. При цьому кубіти нумеруються від 0 до 5.

Перші 4 кубіти при квантовому обчисленні дають один з 2^4=16 можливих значень геш-функції. Останні 2 кубіти є частиною обчислення, що не рахуються у результаті, тому вони ігноруються при наступних кроках.

2. Позначаємо квантові стани, що відповідають заданому значенню геш-функції.

Значення геш-функції складається з чотирьох кубітів. Використовується вентиль CCCC-NOT для позначення відповідного квантового стану. Задіяно додатковий шостий кубіт, щоб звільнити результуючий вихід вентеля, який нам не потрібен.

3. uncompute dream() для скидання реєстру кубітів.

Зворотні обчислення виконуються просто обчисленням їх у зворотному порядку. Далі представлено uncompute квантового гешу:

```
@circuit.subroutine(register=True)
def rev_quantum_hash():
    ocirc=Circuit()
    ocirc.ccnot(5,0,2).ccnot(4,5,0)
    return ocirc
```

Необчислення, як відомо, – це техніка, яка використовується в оборотних схемах для очищення тимчасових впливів на допоміжні біти, щоб їх можна було використовувати повторно [11]. Необчислення є фундаментальним кроком в алгоритмах квантового обчислення.

Ці перші три етапи складають оракул квантового пошуку (рис. 1).

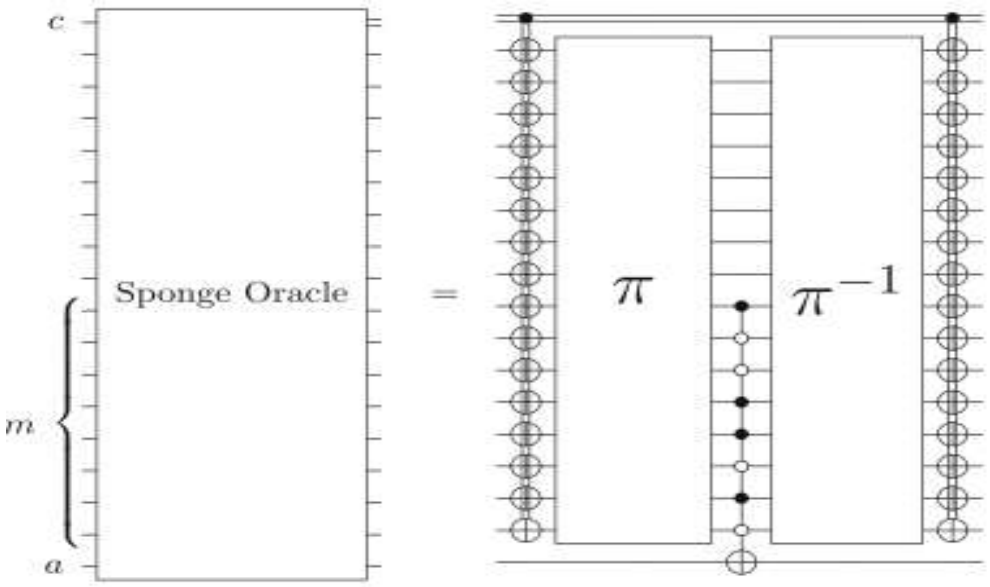

Рис. 1. Оракул квантового пошуку

У статті вони представлені наступним чином:

- "m" – можливі повідомлення в кубітах;
- "a" – це допоміжний кубіт, який використовується для вентилів CCCC-NOT;
- π – квантова геш-функція з першого кроку;
- шлюз CCCC-NOT, стиснутий між π та π^{-1}, налаштований на пошук гешу 10011010 (на рисунку у статті геш довжиною 8 біт, у нас в експерименті буде 4 біти) (крок 2);
- π^{-1} – uncompute квантова геш-функція (крок 3).

Далі регістр повертається до початкового стану і тоді сигнал готовий до посилення.

4. Посилення.

Використовується той же оператор дифузії, що запропоновано у статті (рис. 2).

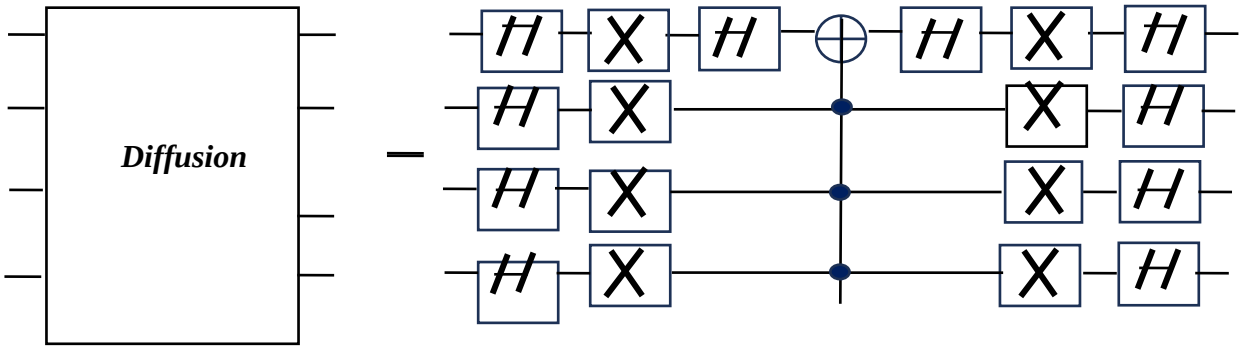

Рис. 2. Оператор дифузії

У нашому випадку потрібно лише 4 кубіти (геші мають 4 біти):

```
def diffuse(qbits=4):
    circ=Circuit()
    circ.h(np.arange(qbits))
    circ.x([0,1,2,3]).h([0]).cccnot(targets=[3,1,2,0]).h([0]).x([0,1,2,3])
    circ.h(np.arange(qbits))
    return circ
```

Це реалізація квантової дифузної операції (інверсія відносно середнього) – ключовий елемент алгоритму Гровера.

circ.h(np.arange(qbits)) застосовує Адамари до всіх кубітів (створює суперпозицію);

circ.x([...]) інвертує всі кубіти (підготовка до відображення);

circ.h([0]) → cccnot(targets=[3,1,2,0]) → circ.h([0])

реалізація мультикубітного контролюємого NOT (у даному випадку трьохконтролюємий Toffoli) з цільовим кубітом 0 – звичайно використовується як відображення відносно $|0\rangle$;

circ.x([...]) інвертування зворотно;

знову circ.h(np.arange(qbits));

завершення інверсії відносно середнього.

Ці чотири кроки ми можемо повторювати і більше одного разу. Але не занадто багато. Наша функція dream може обробляти 2^6=64 можливих повідомлення.

Якщо оцінити роботу класичного комп'ютера, то він може зламати геш-функцію після 64/2=32 спроб. Квантовий комп'ютер зробить це за $\sqrt{M}$ спроб, Тобто лише за 8 спроб, якщо M=1 і за 4 спроби, якщо M=4.

Нехай нам потрібно знайти повідомлення, що відповідає геш-функції 1111, що реалізовано як CCCC-NOT ([0,1,2,3,5]) в AWS Braket.

Коректність квантового пошуку у нашій спрощеній ситуації можна перевірити простим перерахуванням всіх повідомлень, які відповідають геш-функції 1111. Виявляється, чотири повідомлення дають геш-функцію 1111.

Це повідомлення 011110, 010110, 111110 і 110110.

Запускаємо програму AWS Braket двічі по 2 раунди кожного разу (2^2=4 спроби).

Ми повторюємо цю комбінацію 1111, щоб отримати середнє значення. Ось результати, найкращі збіги виділені жирним шрифтом:

{**'111110': 482**, **'110110': 416**, '110001': 4, '100000': 2, **'010110': 460**, '011111': 6, **'011110': 435**, '101111': 4, '111010': 7, '011101': 6, '111000': 4, '101101': 5, '101110': 4, '000000': 8, '110101': 3, '000100': 1, '100010': 5, '000110': 6, '010100': 4, '100111': 5, '010001': 3, '001100': 4, '111001': 5, '110110': 2, '101011': 3, '010000': 7, '001011': 2, '100011': 5, '011100': 2, '110000': 3, '010010': 1, '011011': 6, '111101': 5, '001110': 4, '101000': 4, '111111': 3, '011000': 3, '110011': 4, '011001': 4, '111011': 3, '110010': 7, '100110': 1, '111100': 4, '100100': 2, '110111': 3, '001000': 2, '001010': 4,

'100101': 5, '000101': 5, '100001': 3, '101100': 1, '011010': 3, '001111': 3, '000001': 2, '101001': 2, '000010': 4, '010101': 2, '010011': 3, '000111': 1, '101010': 1, '001101': 2}

Висновки за результатами експерименту.

Після чотирьох спроб ми отримуємо наступні результати:

- ймовірність знаходження квантовою схемою повідомлення 111110 становить 48,2 %;
- ймовірність знаходження квантовою схемою повідомлення 010110 становить 46 %;
- ймовірність знаходження квантовою схемою повідомлення 011110 становить 43,5 %;
- ймовірність знаходження квантовою схемою повідомлення 110110 становить 41,6 %.

Тобто, ймовірність знайти за допомогою квантового комп'ютера хоча б одне з повідомлень, якому відповідає геш-функція 1111, становить близько 90 %.

Щодо класичного комп'ютера, то ймовірність знайти одне повідомлення становить близько 5 %, знайти хоча б одне повідомлення – близько 23 %.

Тобто квантові комп'ютери значно прискорюють інверсію геш-функцій і є вагомі причини хвилюватися щодо криптографічної стійкості примітивів, що засновані на комбінаториці. А це не тільки геш-функції.

Висновки

Алгоритм Гровера теоретично знижує стійкість геш-функцій до атак на прообраз та колізій. Це означає, що для підтримки аналогічного рівня безпеки в квантову еру розмір виходу геш-функцій може знадобитися збільшити вдвічі. Існують теоретичні дослідження щодо побудови квантових схем для обчислення геш-функцій та їх обернення, але експериментальні реалізації цих схем на сьогоднішніх квантових комп'ютерах є дуже обмеженими і стосуються лише спрощених версій геш-функцій.

Розробка достатньо потужних і стабільних квантових комп'ютерів, здатних виконати такі складні обчислення, є серйозним науково-технічним викликом.

Проте, дослідження в галузі постквантової криптографії активно розвиваються, і вже існують перспективні криптографічні алгоритми, які, як вважається, будуть стійкими до атак як класичних, так і квантових комп'ютерів, включаючи геш-функції.

Список літератури:

1. Горбенко І. Д., Горбенко Ю. І. Прикладна криптологія : підручник. 2-ге вид. Харків : Форт, 2013. 878 с.

2. Горбенко Ю.І. Методи побудування та аналізу криптографічних систем : моногр. Харків : Форт, 2015. 959 с.

3. Gorbenko I.D. Methods of building general parameters and keys for NTRU Prime Ukraine of 5th–7th levels of stability. Product form / I.D. Gorbenko, O.G. Kachko, Yu.I. Gorbenko, I.V. Stelnik, S.O. Kandyi, M.V. Yesina // Telecommunications and Radio Engineering, 2019. Vol. 78. Is. 7. P. 579–594. Режим доступу: 10.1615/TelecomRadEng.v78.i7.30.

4. NIST IR 8413. Status Report on the Third Round of the NIST PostQuantum Cryptography Standardization Process. July 2022 (Updated 9/26/2022). [Електронний ресурс]. Режим доступу: 10.6028/NIST.IR.8413-upd1.

5. NIST IR 8105. Report on Post-Quantum Cryptography. April 2016. [Електронний ресурс]. Режим доступу: 10.6028/NIST.IR.8105.

6. NIST IR 8240. Status Report on the First Round of the NIST PostQuantum Cryptography Standardization Process. January 2019.[Електронний ресурс]. Режим доступу: 10.6028/NIST.IR.8240.

7. NIST IR 8309. Status Report on the Second Round of the NIST PostQuantum Cryptography Standardization Process. July 2020. [Електронний ресурс]. Режим доступу: 10.6028/NIST.IR.8309.

8. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України; Стратегія від 26.08.2021 № 447/2021. Режим доступу: https://zakon.rada.gov.ua/laws/show/447/2021#n12.

9. Quantum Search for Scaled Hash Function Preimages Sergi Ramos-Calderer12, Emanuele Bellini1, José I. Latorre123, Marc Manzano1 and Victor Mateu1 arXiv:2009.00621v1 [quant-ph] 1 Sep 2020 1 Technology Innovation Institute, United Arab Emirates.

10. Bertoni Guido, Daemen Joan, P Michaël, and VA Gilles. Cryptographic sponge functions, 2011.

11. Aaronson Scott, Grier Daniel, Schaeffer Luke (2015). The Classification of Reversible Bit Operations. arXiv:1504.05155 [quant-ph].

Надійшла до редколегії 19.02.2025

Відомості про авторів:

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

Лисицька Ірина Вікторівна – д-р техн. наук, 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 – канд. техн. наук, доцент, Харківський національний університет імені В.Н. Каразіна, старший викладач кафедри кібербезпеки інформаційних систем, мереж і технологій, навчально-науковий інститут комп'ютерних наук та штучного інтелекту; Україна; e-mail:irina.galceva@karazin.ua

УДК 004.056.5 **DOI:10.30837/rt.2025.2.221.08**

П.В. ШУЛІК, канд. техн. наук, О.І. ФЕДЮШИН, канд. техн. наук,
Д.О. В'ЮХІН, О.Ю. МОРОЗОВ

ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ВІРТУАЛІЗАЦІЇ INTEL ДЛЯ СТВОРЕННЯ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ НА БАЗІ OPEN PORTABLE TRUSTED EXECUTION ENVIRONMENT (OP-TEE)

Вступ

В сучасних операційних системах для захисту інформації існує підхід з використанням двох операційних систем, де система поділяється на два світи: звичайний (non secure world) – де працює звичайне програмне забезпечення, та захищений світ (secure world), в якому ведеться робота з конфіденційною інформацією. Звичайний світ не має доступу до захищеного світу тоді як останній може з'єднуватись при бажанні з різними пристроями. Цей підхід стосується не тільки процесора, але і пам'яті, транзакції на шинах, переривань, периферійних пристроїв в рамках системи, в тому числі, програмного забезпечення.

Як приклад програмної підтримки такого підходу можна навести опен соурс фреймфорк OP-TEE (Open Portable Trusted Execution Environment) [1]. Типова архітектура програмного забезпечення OP-TEE показана на рис. 1.

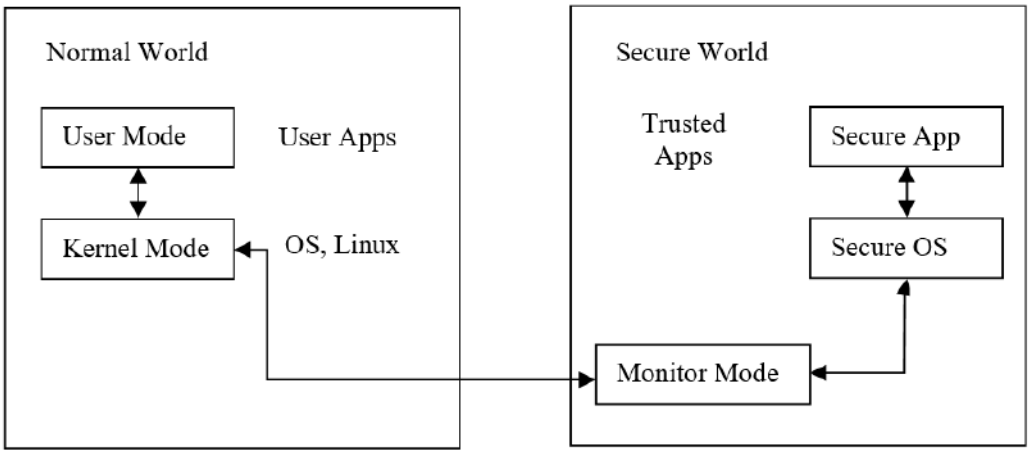

Рис. 1. Типова архітектура поділу світів OP-TEE

У звичайному світі працює основна операційна система, наприклад Linux або Android та звичайні додатки. Коли потрібно запустити якусь задачу, яка працює з конфіденційними даними, наприклад, аутентифікація, шифрування даних, банківські операції та інше, то йде запит від звичайного до сек'юрного світу. Для цього використовується API, який надається сек'юрним світом. Звернення до API виконується через Kernel module (або драйвер) та Monitor. Monitor розташований в сек'юрному світі та виступає арбітром, який обробляє запити від звичайного світу та повертає відповіді. В сек'юрному світі на рівні User space працюють додатки, які запускаються у відповідь на API запити.

Для підтримки різних світів необхідна апаратна підтримка, де периферія також поділяється на елементи для роботи з захищеною та звичайною інформацією – наприклад, розподіл оперативної пам'яті та флеш пам'яті. Така підтримка існує з боку ARM систем [2] і називається ARM TrustZone. В ARM TrustZone вводиться захищений режим роботи ARM ядра, в ньому виконується робота з секретною інформацією, яка не повинна бути доступною для основної операційної системи та її додатків. Спочатку OP-TEE була створена безпосередньо для підтримки ARM TrustZone для процесорів ARM Cortex A, де використовуються Unix-подібні операційні системи. Але OP-TEE поширюється дуже активно останні декілька років для роботи вбудованих та мобільних пристроїв і набрала популярності. Такий стан справ

викликає інтерес до використання OP-TEE з боку виробників серверних рішень, де системи в основному базуються на процесорах Intel-x86. Підтримка такого підходу з боку Intel-x86 платформ є проблематичною, тому що Intel не має подібних ARM TrustZone рішень. Але Intel-x86 має розвинену апаратну підтримку віртуалізацій, де для організації secure world може використовуватися окрема віртуальна машина.

Апаратна віртуалізація Intel-x86 – це технологія, що дозволяє запуск віртуальних машин в ізольованому режимі, де пам'ять, дисковий простір, периферія можуть бути розподілені та ізольовані між віртуальними машинами, тобто одна віртуальна машина не буде мати доступу до ресурсів іншої віртуальної машини.

Метою даного дослідження є створення системи захисту інформації на основі інтеграції OP-TEE фреймворка з Intel-X86 платформами з використанням технологій віртуалізації.

Предметом дослідження є програмні засоби інтеграції OP-TEE фреймворка з Intel-x86.

Суть інтеграції OP-TEE складається в заміщенні технології TrustZone віртуальними машинами та технологіями процесорів Intel-x86 VT-d/VT-x, де апаратні ресурси розподіляються між віртуальними операційними системами і забезпечують ізоляцію ресурсів та інформації між операційними системами [3, 4].

Інтеграції OP-TEE фреймворка з Intel-x86 платформами

У 2006 р. Intel представила VT-x – розширення для ефективної віртуалізації архітектури IA-32. Воно включає в себе набір інструкцій VMX і два нових режими роботи. Нові режими були названі root і non-root. Перший з них – для монітора віртуальних машин, другий – для гостьових оточень. За замовчуванням після включення живлення віртуалізація недоступна. Вхід в режим root відбувається після виконання нової інструкції VMXON, а наступні входи в non-root – за допомогою VMLAUNCH/VMRESUME.

Ключовий процес в будь-якій системі апаратної віртуалізації – це збереження поточного стану процесора гостя і завантаження стану монітора. Для зберігання станів як гостя, так і господаря використовується сутність під назвою VMCS (англ. Virtual Machine Control Structure). Ця структура повинна бути своя для кожного активного гостя. На рис. 2, що ілюструє переходи між режимами root і non-root, всередині VMCS використовуються дві області: стан гостя (guest-state) і стан господаря (host-state).

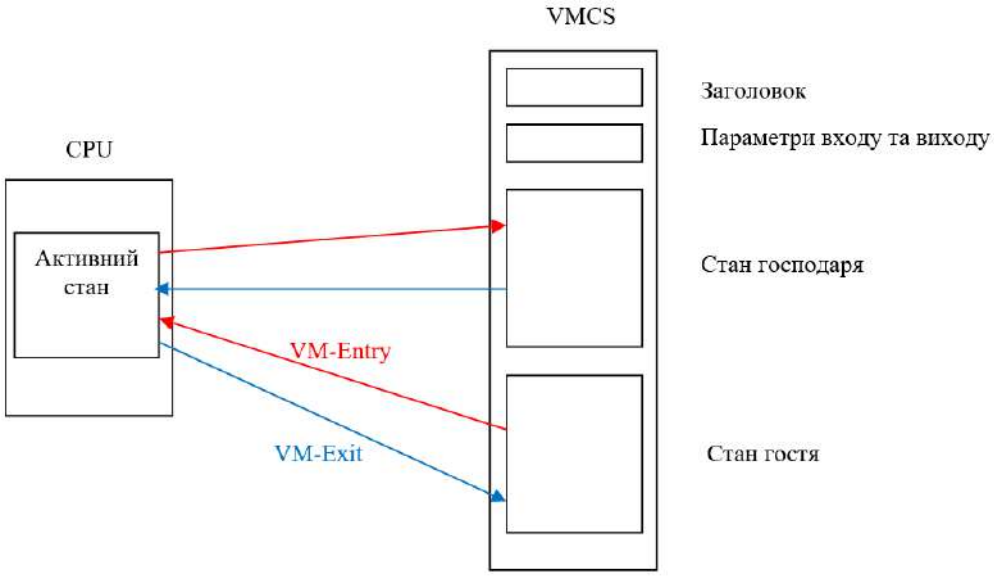

Рис. 2. VMCS та її стани

На рис. 2 подія VM-Entry – це одна з двох інструкцій: VMLAUNCH або VMRESUME, – а VM-Exit – одна з безлічі синхронних і асинхронних подій, оголошених привілейованими

в контексті VT-x non-root і тому вимагають перехоплення монітором. Деталі того, що і як завантажувати при переході з root в non-root і назад, також зберігаються в VMCS в елементах VM-entry і VM-exit controls(параметри входу і виходу). Області збереження розбиті на поля, кожне з яких зберігає в собі регістр або іншу архітектурну інформацію процесора.

У якості господаря (або арбітра), який керує перемиканням роботи процесора та доступу до ресурсів, може виступати гіпервізор першого типу або основна (хост) операційна система.

Таким чином архітектура Intel VT-x – це апаратно-програмне середовище, яке дуже схоже на ARM TrustZone з точки зору ізоляції програмного коду та ресурсів. Необхідно тільки вибрати архітектуру програмного забезпечення, тобто вирішити де буде розташований normal world та secure world.

Існує варіант інтеграції фреймворка OP-TEE на базі Intel VT-x та гіпервізора компанії Intel Kernel Guard Technology (iKGT).

iKGT – це легкий гіпервізор типу 1, з відкритим кодом Intel (https://github.com/intel/ikgt-core). Основний підхід закладений в iKGT [5] називається Intel Supervisor Mode Execution Prevention (SMEP) – запобігання виконання коду в режимі супервізора [6]. Технологія полягає в запобіганні виконання коду, розташованого на сторінці користувача (тобто звичайний світ, який не повинен мати доступу до захищеної інформації), при поточному рівні привілеїв рівному 0 (рівень доступу до захищеної інформації). Тобто до можливостей ізоляції Intel VT-x додається ще SMEP.

Використання гіпервізора потребує використання гостьової операційної системи – тобто віртуальної машини. Таким чином увесь код як звичайного, так і захищеного світу виконується всередині віртуальної машини (на рис. 3).

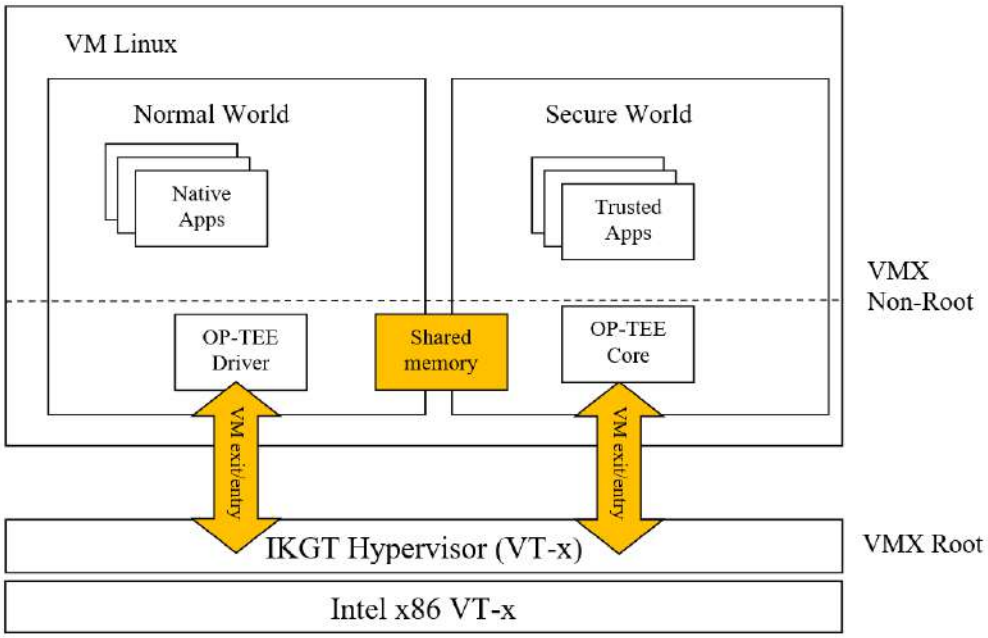

Рис. 3. Архітектура OP-TEE & IKGT

Ізоляція пам'яті досягається шляхом відповідного налаштування розширених таблиць сторінок, тому Linux не може отримати доступ до пам'яті OP-TEE. Тим не менш, є один блок спільної пам'яті, до якого може отримати доступ як Linux, так і OP-TEE для обміну параметрами та даними.

Перемикання між світами здійснюється командою «VMCALL», яка може бути викликана з Linux або з OP-TEE. Наступним кроком є виклик «VM exit» до гіпервізора iKGT, відповідального за детальне перемикання світу, таких як збереження або відновлення контексту VM, виконання «VM entry» в інший світ та інше.

В підході з використанням iKGT normal та secure world підтримують сумісність рівня API з архітектурою ARM TrustZone. Тільки драйвер Linux ядра ОС OP-TEE і OP-TEE залежать від архітектури.

Існуючий підхід має певну кількість недоліків: по-перше, normal world та secure world працюють в рамках однієї віртуальної машини, тобто в рамках однієї операційної системи. Використовуються тільки механізми перемикання між віртуальними машинами, але перемикання виконується тільки між сторінками пам’яті та використовується SMEP для обмеження доступу. Тобто, з точки зору безпеки, такий підхід дає більше можливостей для майбутніх хакерських атак. По-друге, цей підхід недостатньо модульний і потребує значних модифікацій при переході на інші платформи.

Архітектура з двома VM та використанням ACRN Hypervisor

Запропоноване в роботі рішення (див. рис. 4) базується на ізоляції secure world в окрему віртуальну машину. Апаратна підтримка теж базується на Intel x86 VT-x, але secure world існує повністю в окремій віртуальний машині. Таким чином ми маємо дві віртуальні машини – одна для normal world, де виконується основна операційна система, а друга віртуальна машина для OP-TEE. У якості гіпервізора використовуються гіпервізор ACRN [7]. ACRN – це гіпервізор першого типу з відкритим кодом, який був розроблений компанією Intel. ACRN гнучкий та легковісний, також використовується в різноманітних embedded системах, де важливі маленькі розміри гіпервізора та його гнучкість в адаптації до різноманітних систем та платформ.

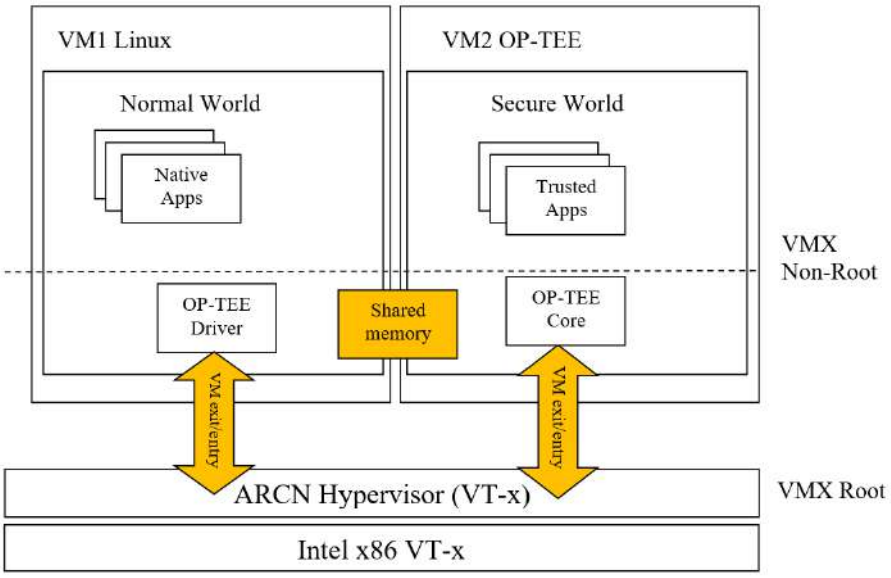

Рис. 4. Архітектура з двома VM та використанням ACRN Hypervisor

Як показано на рис. 4, ми маємо дві віртуальні машини, які працюють під керуванням ACRN гіпервізора. Перша VM1 – це звичайний світ – OS Linux, друга VM 2 – це OP-TEE.

ACRN створює ізольовану область пам'яті для TEE і шлях зв'язку для взаємодії двох віртуальних машин, але для повної підтримки поведінки ARM Trusted Firmware ACRN Hypervisor був модифікований для вирішення наступних проблем [8, 9]:

– необхідно забезпечити буфер shared memory. Тому ACRN гіпервізор був модифікований для створення такого буферу;

– організувати безпечну доставку та обробку переривань між звичайними та захищеними світами, безпечну доставку переривань та захист пам'яті на основі Intel VT-x. Ця підтримка також була додана на рівні ACRN гіпервізора.

Для підвищення безпеки як ACRN, так і OP-TEE образи були розміщені у зашифрованому регіоні жорсткого диску та ввімкнена підтримка Secure Boot.

Інтеграція як ACRN, так і OP-TEE була виконана з використанням наступних компонентів:

– Intel x86 VT-x: 9th Generation Intel® Core i7 Processors, 9850H;
– Normal World OS: Ubuntu LTS 24.04.1;
– OP-TEE 4.3.0.

Висновки

Запропонований варіант інтеграції OP-TEE на Intel x86 платформу з використанням двох віртуальних машин на базі ACRN гіпервізора.

Normal world та secure world працюють в окремих віртуальних машинах, вони повністю ізольовані на рівні операційних систем. З точки зору безпеки, така архітектура буде більш захищеною від хакерських атак в порівнянні з аналогічними рішеннями.

Побудована архітектура системи надає більше модульності та забезпечує легке перенесення на інші платформи та легке оновлення компонентів.

Список літератури:

1. GlobalPlatform, Inc.: TEE System Architecture Version 1.2 (Nov 2018), GPD SPE 009.
2. ARM Security Technology, Building a Secure System using TrustZone, ARM, Technology Copyright © 2005-2009 ARM Limited. All rights reserved. PRD29-GENC-009492C.
3. Arshad Nehal, Priyanka Ahlawat Securing IoT applications with OP-TEE from hardware level OS: 2019 3rd International conference on Electronics, Communication and Aerospace Technology (ICECA) 10.1109/ICECA.2019.8822040.
4. Kickstart Embedded. OP-TEE: What a Beginner Needs to Know. Sep. 13, 2022. [Online]. Available: https://kickstartembedded.com/2022/09/13/op-tee-part-1-what-a-beginner-needs-to-know/.
5. Intel. KGT Architecture. [Online]. Available:https://www.intel.com/content/www/us/en/developer/articles/technical/kgt-architecture.html.
6. Intel. Intel Supervisor Mode Execution Protection (SMEP) Datasheet. [Online]. Available: https://edc.intel.com/content/www/us/en/design/products/platforms/processor-and-core-i3-n-series-datasheet-volume-1-of-2/001/intel-supervisor-mode-execution-protection-smep/.
7. Intel. ACRN Hypervisor Documentation [Online]. Available: https://eci.intel.com/docs/3.0/components/acrn-hypervisor.html.
8. Шулік П. В., Федюшин О.І. Організація довіренного середовища виконання з використанням QEMU та TRUST DOMAIN EXTENSIONS від INTEL // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління : тези доп. 15-ї міжнар. наук.-техн. конф., 24–25 квітня 2025р., м. Баку, м. Харків, м. Жиліна. Т. 3. Харків : Impress, 2025. С. 97. https://doi.org/10.32620/ICT.25.t3.
9. Шулік П. В. Використання віртуальних машин для організації захисту інформації на платформах INTEL // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління : тези доп. 15-ї міжнар. наук.-техн. конф., 24–25 квітня 2025р., м. Баку, м. Харків, м. Жиліна. Т. 3. Харків : Impress, 2025. С. 98. https://doi.org/10.32620/ICT.25.t3.

Надійшла до редколегії 11.03.2025

Відомості про авторів:

Шулік Павло Вікторович – канд. техн. наук, Харківський національний університет радіоелектроніки, ст. викладач кафедри безпеки інформаційних технологій, факультет комп'ютерної інженерії та управління, Україна; e-mail: pavlo.shulik@nure.ua; ORCID: https://orcid.org/0009-0004-6200-2172

Федюшин Олександр Іванович – канд. техн. наук, доцент, Харківський національний університет радіоелектроніки, доцент кафедри безпеки інформаційних технологій, факультет комп'ютерної інженерії та управління, Україна; e-mail: oleksandr.fediushyn@nure.ua; ORCID: http://orcid.org/0000-0002-3600-405X

В'юхін Даніїл Олександрович – Харківський національний університет радіоелектроніки, ст. викладач кафедри безпеки інформаційних технологій, факультет комп'ютерної інженерії та управління, Україна; e-mail: daniil.viukhin@nure.ua; ORCID: https://orcid.org/0009-0009-8442-9587

Морозов Олексій Юрійович – Харківський національний університет радіоелектроніки, аспірант кафедри безпеки інформаційних технологій, факультет комп'ютерної інженерії та управління, Україна; e-mail: oleksii.morozov@nure.ua; ORCID: https://orcid.org/0009-0005-6482-7810

УДК 004.056.5 **DOI:10.30837/rt.2025.2.221.09**

А.А. ТЕЛЬНОВА, Д.С. БАЛАГУРА, канд. техн. наук, В.О. ФРОЛЕНКО,
В.М. СУХОТЕПЛИЙ, С.В. ФЛОРОВ, канд. техн. наук

АНАЛІЗ ВИКОРИСТАННЯ КРИПТОПРОВАЙДЕРІВ У ПРОТОКОЛІ TLS

Вступ

Щодня кожна людина надсилає десятки повідомлень і завантажує гігабайти трафіку. При цьому достатньо велика кількість даних проходить відкритими мережами. Це накладає додаткову відповідальність на end-to-end протоколи захисту даних. Одним з наймасовіших протоколів захисту даних у мережі Інтернет є протокол HTTPS (HyperText Transfer Protocol Secure). Згідно зі звітами Google Transparency Report [1], доля використання цього протоколу суттєво збільшилась: від 40 % у 2015 р., до більш ніж 90 % відсотків у 2022–2024 рр. Загальний тренд зі збільшення частки HTTPS трафіку наведено на рис. 1. Графік демонструє узагальнену інформацію щодо доступу до сайтів через протокол HTTPS у браузері Chrome, але загальна тенденція зрозуміла.

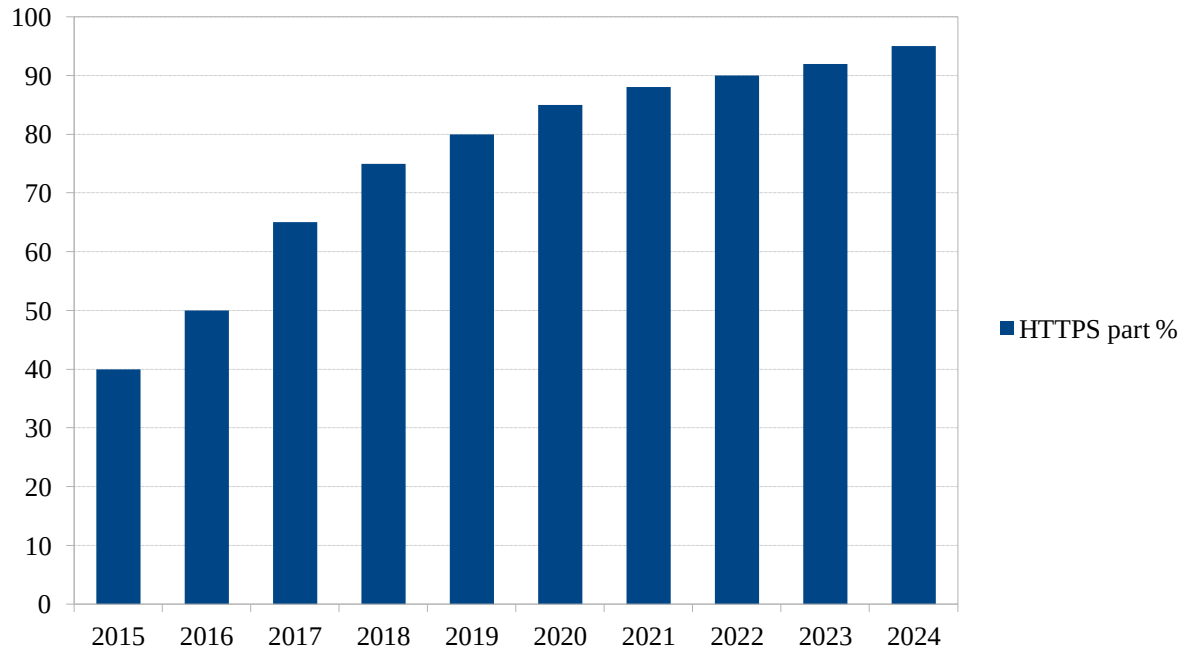

Рис. 1. Відсоток використання HTTPS протоколу

Схожа тенденція спостерігається і з шифруванням електронних повідомлень: станом на 2014 р. лише 26 – 28 % усіх вхідних і вихідних повідомлень були зашифровані відповідно. Але з того часу ситуація значно покращилася, і зараз цей показник становить майже 100 %, ми повинні постійно дбати про безпеку наших даних.

Як відомо, протокол комунікації TLS є базовим елементом протоколу HTTPS. Можна сказати, HTTPS – це HTTP over TLS. Крім того, TLS може використовуватися для забезпечення безпеки даних під час роботи й великої кількості інших протоколів, в тому числі для потреб електронної пошти, протоколів обміну файлами та інше. По суті TLS є фундаментальним елементом сучасних механізмів забезпечення безпечної передачі даних в Інтернеті.

Актуальність

Важливість TLS для захисту даних під час передачі у відкритих мережах важко переоцінити. Разом з тим, TLS, як протокол захисту даних, не може бути ефективно реалізований без криптографічних постачальників. Вони діють як основний інструмент, який забезпечує обчислювальну підтримку для всіх криптографічних операцій.

Постачальник послуг криптографії (CSP) – це незалежний модуль, який дозволяє виконувати криптографічні операції. Яскравим прикладом постачальника послуг криптографії є CryptoAPI та CNG в операційних системах Microsoft. Також існують «незалежні» CSP, які не є елементами жодної операційної системи, наприклад OpenSSL, BoringSSL. Вони можуть бути задіяні незалежно від операційної системи. Вибір, розробка та вдосконалення криптопровайдерів безпосередньо впливає на продуктивність, безпеку та поширення протоколу TLS у мережах.

TLS вимагає шифрування для захисту даних, а постачальники криптографії пропонують реалізацію таких алгоритмів:

- симетричні алгоритми шифрування (AES, ChaCha20) – для захисту основного каналу передачі даних;
- асиметричні алгоритми шифрування (RSA, ECC) – для обміну ключами між клієнтом і сервером;
- ґеш-функції (SHA-256, SHA-3) – для забезпечення цілісності даних.

Крім того, криптографічні постачальники відповідають за створення, зберігання та керування криптографічними ключами, які використовуються в протоколі TLS. Вони обробляють сертифікати X.509, які використовуються TLS для автентифікації сервера та оптимізації обчислювальних операцій для зменшення затримки, що є критично важливим для TLS.

Метою даної роботи є аналіз ефективності роботи криптопровайдерів у протоколі TLS, а також визначення особливостей криптопровайдерів, що впливають на їх вибір та використання в TLS протоколі з урахуванням різних аспектів функціонування протоколу.

Для досягнення поставленої мети висуваються такі завдання:

- аналіз архітектури протоколу TLS;
- визначення вразливостей протоколу;
- вивчення ролі криптографічних провайдерів;
- порівняння сучасних рішень;
- формулювання рекомендацій.

Проведемо аналіз наукових робіт, які також досліджували це питання.

Аналіз наукових робіт

У сучасних дослідженнях, що стосуються використання криптопровайдерів у протоколі TLS, основна увага приділяється питанням криптостійкості, продуктивності та зручності впровадження на різних платформах. Різні криптографічні бібліотеки й API, зокрема Microsoft CryptoAPI, CNG, OpenSSL і BoringSSL, аналізуються у контексті їх здатності ефективно забезпечувати захищене з’єднання.

У роботі [2] розглядається реалізація TLS через бібліотеку CNG. Детально розглянуто внутрішню побудову та ефективність використання CNG у TLS-з’єднаннях. У роботі показано, що CNG пропонує сучасний API для криптографічних операцій, однак має обмежену гнучкість порівняно з відкритими реалізаціями, а також потенційно нижчу продуктивність через сильну інтеграцію із системним сховищем ключів.

Дослідження [3] акцентує увагу на проблемах управління секретами в мобільних реалізаціях TLS. Зокрема, продемонстровано, що навіть сучасні провайдери, такі як BoringSSL, які широко використовуються в Android, можуть зберігати ключову інформацію у пам’яті

після завершення TLS-сесії. Це створює потенційну вразливість, яка може бути використана через аналіз дампів пам'яті або сайд-канальні атаки. Цей аспект підкреслює важливість не лише крипостійкості, а й коректного управління життєвим циклом ключів.

У контексті високопродуктивних обчислювальних систем заслуговує на увагу стаття [4], яка досліджує ефективність роботи бібліотек OpenSSL, BoringSSL, Libsodium і Crypto++ у середовищах із паралельними обчисленнями. Зокрема, порівнюються латентність, пропускна здатність та масштабованість TLS-сесій у середовищі MPI-комунікацій. Результати
демонструють перевагу BoringSSL у масштабованості, що робить його привабливим для серверних рішень і хмарних інфраструктур.

Окрему увагу в літературі приділено Microsoft CNG API як заміні традиційної CryptoAPI. У статті [5] надається практичний огляд можливостей нового API. CNG пропонує більш модульний і гнучкий підхід до криптографії в Windows, підтримує сучасні алгоритми, інтеграцію з апаратними модулями та централізоване управління ключами через NCrypt API. Однак, використання CNG лишається обмеженим Windows-платформою та має менше прикладів кросплатформеного впровадження у TLS.

Крім того, в роботі [6] було запропоновано реалізацію постквантового алгоритму обміну ключами на базі NTRU у TLS 1.3 з використанням OpenSSL. Результати показують, що навіть за умов додаткових обчислювальних витрат, продуктивність TLS-сесій із постквантовим обміном ключів залишалась високою, що відкриває перспективи впровадження OpenSSL у майбутні стандарти стійких до квантових атак систем.

Кожна робота висвітлює окремі питання застосування криптопровайдерів з точки зору швидкодії або безпеки використання, в тому числі у протоколі TLS. Разом з тим, ці роботи не надають загальної картини щодо використання криптопровайдерів у протоколі TLS.

Архітектура протоколу TLS

Протокол TLS є фундаментальним елементом безпечного обміну даними в Інтернеті, який забезпечує шифрування, автентифікацію та цілісність інформації. Його ефективність ґрунтується на поєднанні механізмів взаємодії та різних криптографічних механізмів, які гарантують конфіденційність та захист від несанкціонованого доступу. Серед ключових компонентів TLS – алгоритми шифрування, ґеш-функції та інфраструктура формування та підтримки сертифікатів. [1] Кожен із цих елементів та їхня роль у створенні надійного механізму безпеки розглянуті нижче.

Алгоритми шифрування. Шифрування є базовим елементом безпеки TLS, який забезпечує захист переданої інформації від перехоплення. У межах протоколу застосовуються два типи криптографічних методів:

- симетричне шифрування: використовується для захисту переданих даних після встановлення з'єднання. Обидві сторони сесії застосовують один спільний ключ, що пришвидшує обробку та зменшує навантаження на систему;

- асиметричне шифрування: застосовується на початковому етапі встановлення з'єднання для захисту обміну ключами. Цей метод базується на використанні двох ключів: відкритого (public) та закритого (private).

Ґеш-функції. Ґеш-функції відіграють важливу роль у гарантуванні цілісності переданих даних і створенні цифрових підписів у TLS. Вони використовуються для формування Message Authentication Codes (MAC), які дозволяють виявляти будь-які зміни в даних під час передачі. Основні алгоритми наведено у табл. 1.

Ключі та сертифікати. Для забезпечення автентифікації та довіри між сторонами у TLS використовується механізм цифрових сертифікатів та криптографічних ключів. Формування та життєвий цикл сертифікатів відкритих ключів забезпечується центрами сертифікації відкритих ключів. Разом з тим, безпечне зберігання особистих ключів а також зберігання

сертифікатів відкритих ключів у системах кінцевих користувачів часто покладається на функціонал криптопровайдерів.

Наявність інфраструктури відкритих ключів у TLS гарантує, що сервер або клієнт, з яким встановлюється з'єднання, дійсно є тим, за кого себе видає, що зменшує ризик атак типу «людина посередині» (man-in-the-middle, MITM) [2].

Таблиця 1

Алгоритми, що використовуються у TLS

Тип алгоритму	Назва алгоритму	Призначення/примітка	TLS-версії
Симетричне шифрування	AES-128-GCM / AES-256-GCM	Стандарти шифрування з автентифікацією	TLS 1.2, TLS 1.3
	AES-128-CBC / AES-256-CBC	Старі режими блочного шифрування (менш безпечні)	TLS 1.0 – TLS 1.2
	ChaCha20-Poly1305	Альтернатива AES для пристроїв безапаратного AES	TLS 1.2, TLS 1.3
	3DES	Застарілий алгоритм, небезпечний	TLS 1.0, TLS 1.1
Ассиметричне шифрування / обмін ключами	RSA	RSA алгоритм для обміну ключами	TLS 1.0–1.2
	DH	DH Алгоритм обміну ключами	TLS 1.0–1.2
	ECDH	Версія DH на еліптичних кривих	TLS 1.0–1.2
	DHE/ECDHE	Динамічні (ефемерні) версії DH/ECDH для forward secrecy	TLS 1.2, TLS 1.3
	Kyber	Post-quantum KEM (експериментальний, у гібридних обмінах)	TLS 1.3 (через розширення)
Геш-функції / MAC	SHA-1	Застаріла, не рекомендована до використання	TLS 1.0–1.2
	SHA-2 (SHA-256, SHA-384)	Сучасні стандарти для гешування / HMAC	TLS 1.2, TLS 1.3
	HMAC		TLS 1.2, 1.3
	BLAKE2	Не в основному стандарті, можливий через розширення	(експериментальні)
Алгоритми підпису (ЕЦП)	RSA-PSS	Рекомендований стандарт підпису у TLS 1.3	TLS 1.2, TLS 1.3
	ECDSA	Підписи на еліптичних кривих	TLS 1.2, TLS 1.3
	EdDSA (Ed25519, Ed448)	Сучасні, компактні та швидкі ЕЦП	TLS 1.3 (через розширення)
	Dilithium, Falcon	Post-quantum підписи (у режимі тестування / PQC експерименти)	TLS 1.3 (через розширення)

Етапи TLS-протоколу. Протокол TLS як правило визначається трьома етапами: TLS-Handshake, data transfer і connection termination [1], кожен з яких використовує окремі сімейства алгоритмів, що дає можливість у клієнтських застосунках використовувати криптопровайдери з обмеженими наборами алгоритмів. Але на практиці набори криптографічних алгоритмів не обмежуються.

Вразливості протоколу TLS

Попри широке впровадження, TLS не позбавлений вразливостей, які можуть виникати як через недоліки в дизайні протоколу, так і через помилки в реалізації алгоритмів

конкретними криптографічними бібліотеками. Ці вразливості можуть бути експлуатовані зловмисниками для проведення атак, що ставить під загрозу безпеку переданих даних. Попри постійні оновлення версій протоколу, які усувають ці вразливості, стверджувати про відсутність вразливостей у протоколі неможливо – деякі вразливості просто можливо просто ще не були виявлені. Наведемо найбільш відомі й критичні вразливості, що були виявлені в TLS.

Однією з ключових проблем ранніх версій TLS (1.0 та 1.1) була вразливість до атак типу BEAST (Browser Exploit Against SSL/TLS) [9], яка використовувала недоліки в реалізації режиму шифрування CBC для отримання доступу до зашифрованих даних. Ця атака стала можливою через передбачуваність ініціалізаційного вектора (IV) в цих версіях протоколу.

Також достатньо цікавою вразливістю є можливість виконання атаки типу POODLE (Padding Oracle On Downgraded Legacy Encryption) [10], яка використовує можливість за певних обставин знизити версію протоколу до SSL 3.0. Відповідно така маніпуляція дозволяє зловмиснику атаки, що були можливі для версії SSL 3.0, і тому числі padding oracle атаки. Це стало можливим через підтримку зворотної сумісності в TLS, що дозволяє зловмиснику нав'язати використання застарілих і менш безпечних версій протоколу.

Прикладом критичної помилки в реалізації OpenSSL, яка дозволяла зчитувати до 64 кілобайтів пам'яті сервера, включаючи конфіденційні дані, такі як приватні ключі та паролі, є вразливість Heartbleed (CVE-2014-0160) [11]. Ця помилка виникла через неправильну обробку запитів heartbeat, що дозволяло зловмиснику отримувати доступ до пам'яті сервера без
авторизації. Після цього, у 2013 р., атака Lucky13 (CVE-2013-0169) продемонструвала, як навіть незначні відмінності в часі обробки повідомлень можуть бути використані для витоку інформації [12]. Ця атака експлуатує час обробки padding в режимі CBC, що дозволяє зловмиснику поступово відновлювати зашифровані дані.

З-поміж іншого, Bleichenbacher атаки, вперше описані в 1998 р., залишаються актуальними й сьогодні. Вони експлуатують помилки в обробці помилок при дешифруванні RSA, що дозволяє зловмиснику отримати доступ до зашифрованих даних без знання приватного ключа [13]. Незважаючи на численні оновлення протоколу, деякі реалізації TLS залишаються вразливими до цих атак.

Безпека протоколу TLS залежить не лише від його специфікації, але й від реалізації конкретними криптографічними провайдерами. Вибір бібліотеки повинен враховувати не лише продуктивність, але й рівень безпеки, підтримку сучасних алгоритмів і швидкість реагування на виявлені вразливості. Регулярне оновлення бібліотек, відмова від застарілих алгоритмів і впровадження сучасних практик безпеки є ключовими факторами для забезпечення надійного захисту даних в мережевих комунікаціях [2].

Вплив криптографічних провайдерів на роботу протоколу TLS

Криптографічний провайдер (Cryptographic Service Provider, CSP) – це програмний або апаратний модуль, який реалізує криптографічні операції, необхідні для забезпечення безпеки в протоколі TLS. Він виступає як посередник між застосунками, що потребують шифрування, та криптографічними алгоритмами, які забезпечують захист даних.

Основні функції криптографічного провайдера:

- реалізація алгоритмів симетричного та асиметричного шифрування;
- створення, збереження та управління криптографічними ключами;
- генерація та перевірка цифрових підписів;
- виконання операцій ґешування та автентифікації.

Використання CSP дозволяє застосовувати TLS без необхідності глибокого розуміння складних криптографічних процесів з боку розробників. Замість цього вони можуть звертатися до стандартних бібліотек або API, які забезпечують високий рівень безпеки та продуктивності.

Різні операційні системи та програмні середовища мають власні криптографічні провайдери, які відповідають за безпеку TLS-з'єднань. Серед найвідоміших рішень виділяють
наступні:

1. *OpenSSL* – один із найпопулярніших криптографічних провайдерів з відкритим кодом. Він використовується у вебсерверах (наприклад, Apache, Nginx), поштових серверах, VPN-системах та інших мережевих додатках. OpenSSL підтримує широкий набір криптографічних алгоритмів, зокрема AES, ChaCha20, RSA, ECC, та SHA-256 [14].

До головних переваг OpenSSL можна віднести підтримку сучасних стандартів шифрування, постійний перегляд кодової бази та оновлення, які реагують на нові загрози. Крім
того, для OpenSSL існує можливість використання в різних операційних системах.

2. *BoringSSL* – це варіація OpenSSL, що була розроблена корпорацією Google для використання у власних продуктах, таких як Chrome та Android. Він оптимізований для швидкості та безпеки, а також спрощений для усунення потенційних вразливостей [15].

Особливості BoringSSL полягають у зменшеному розмірі коду та відсутності застарілих функцій, регулярних оновленнях безпеки, а також кращій інтеграції з мобільними платформами.

3. *Криптопровайдери від Microsoft, а саме сімейство CryptoAPI - CNG* – це криптографічна платформа у операційній системі Windows (починаючи з відносно застарілих версій). Вона забезпечує доступ до шифрувальних операцій через API. Крім того, вона використовується у Windows для автентифікації, підпису цифрових документів та шифрування TLS-з'єднань.

Серед основних характеристик CryptoAPI вбудована підтримка TLS у Windows, можливість роботи з сертифікатами X.509 й інтеграція з апаратними модулями безпеки (HSM, TPM).

Крім цих провайдерів, існують й інші криптографічні бібліотеки, такі як, наприклад, LibreSSL (форк OpenSSL, що зосереджується на безпеці) та WolfSSL (легковаговий криптографічний провайдер, орієнтований на IoT-пристрої).

Хоча всі криптографічні провайдери реалізують схожі алгоритми, їхня продуктивність, безпека та оптимізація суттєво відрізняються залежно від імплементації.

Безпека TLS-протоколу в криптопримітивах

Реалізація TLS значною мірою залежить від криптографічних бібліотек, які використовуються для його впровадження. Різні бібліотеки мають свої особливості, які можуть як підвищувати, так і погіршувати безпеку протоколу.

OpenSSL є однією з найпоширеніших криптографічних бібліотек, яка підтримує широкий спектр алгоритмів і протоколів. Однак її складність і підтримка застарілих алгоритмів можуть призводити до вразливостей, якщо не вжити належних заходів безпеки. Наприклад, підтримка слабких cipher suites, таких як RC4 або 3DES, може бути використана зловмисниками для проведення атак.

BoringSSL, розроблена Google, є форком OpenSSL з акцентом на безпеку і спрощення. Вона виключає підтримку застарілих і небезпечних алгоритмів, що зменшує поверхню атаки. Однак така стратегія може обмежувати гнучкість у деяких випадках, коли потрібна підтримка специфічних алгоритмів або протоколів.

CryptoAPI від Microsoft забезпечує інтеграцію TLS в операційну систему Windows. Хоча цей криптопровайдер гарантує стабільність і підтримку з боку виробника, обмеження в налаштуваннях і повільне впровадження оновлень можуть призводити до затримок у виправленні відомих вразливостей. Крім того, обмежена підтримка сучасних алгоритмів, таких як Curve25519 або SHA-3, може знижувати загальний рівень безпеки.

Аналіз імплементації основних компонентів TLS різними криптопровайдерами

Розглянемо можливості імплементації основних компонентів TLS різними криптопровайдерами.

У контексті сучасних підходів до реалізації TLS, одним із ключових критеріїв залишається продуктивність – зокрема, наскільки ефективно провайдер використовує апаратні
ресурси, оптимізацію під конкретні архітектури процесорів та підтримку новітніх криптографічних стандартів.

Можливості імплементації симетричного шифрування (AES, ChaCha20). У випадку симетричного шифрування, OpenSSL завдяки модульній структурі забезпечує максимально ефективне використання AES-NI на процесорах Intel і AMD, що підтверджено численними бенчмарками (наприклад, openssl speed-evp aes-256-gcm). Наприклад, при використанні AES-256-GCM з підтримкою AES-NI, продуктивність досягає приблизно 2251 МБ/с на блоках розміром 8192 байти. [14] Реалізація ChaCha20, починаючи з версії 1.1.0, була значно оптимізована для мобільних ARM-архітектур, що особливо помітно у середовищах без AES-NI [15].

BoringSSL, який є форком OpenSSL, активно видаляє зайвий функціонал на користь оптимізації. Реалізація ChaCha20-Poly1305 у BoringSSL є однією з найшвидших на ARM-архітектурах, забезпечуючи перевагу над AES за відсутності апаратного прискорення. Швидкість роботи алгоритму для блоків розміром 8192 байти складає до 1707.5 MB/c [16], у той час, як за використання OpenSSL – лише до 719 MB/c [14].

Натомість CryptoAPI часто працює через абстрактний інтерфейс, який обмежує прямий контроль над апаратною оптимізацією. Вимірювання продуктивності з використанням BCryptEncrypt та BCryptOpenAlgorithmProvider показують значно більше навантаження в порівнянні з OpenSSL або BoringSSL, особливо при великій кількості одночасних з’єднань. Варто зазначити, що до значних переваг CryptoAPI слід віднести реалізацію AES, яка повністю сумісна з сертифікатами Windows, однак може мати нижчу продуктивність через обмеження API.

Асиметричне шифрування (RSA, ECC, ECDHE). У контексті асиметричного шифрування, OpenSSL демонструє стабільну продуктивність із підтримкою апаратного прискорення для великих RSA-ключів через Intel QuickAssist та інші HSM. Наприклад, при використанні ключів RSA-2048 швидкість підпису становить приблизно 100 операцій в секунду, а перевірки — 22000 операцій в секунду [17]. Після версії 3.0 було покращено підтримку криптографії на кривих Brainpool та Curve25519, що важливо для сучасного TLS 1.3.

BoringSSL навмисне виключив підтримку деяких функцій, як-от CMS і повну підтримку PKCS#11, але натомість сконцентрувався на високоефективній реалізації X25519 та ECDHE, що робить його першочерговим вибором для клієнтських застосунків, таких як Android Chrome. Ці оптимізації зменшують затримку під час встановлення TLS-з’єднання, що критично важливо для користувацького досвіду в мобільному середовищі. Згідно з результатами дослідження [18] швидкість підпису з використанням X25519 складає 56680 операцій за
секунду, перевірки – 18020 операцій в секунду [18].

CryptoAPI, попри підтримку сучасних кривих через CNG, на практиці може бути обмеженим через відсутність можливості тонкого налаштування протоколу — зокрема, неможливість вибору кривих, не схвалених Microsoft, без використання сторонніх бібліотек або CAPI wrapper'ів. Наприклад, Curve25519 не входить до переліку підтримуваних алгоритмів CryptoAPI без використання сторонніх бібліотек, однак у Windows 10 вже підтримується з CNG[19].

Геш-функції (SHA-256, SHA-3). Для геш-функцій, OpenSSL продовжує демонструвати високу швидкодію завдяки SIMD-оптимізованим реалізаціям. Підтримка SHA-3 була додана у версіях після 1.1.1 і є цілком придатною для масштабних сценаріїв. У певних бенчмарках [20] видно, що SHA-2 і SHA-3 реалізовані з урахуванням паралельності обробки, що знижує

латентність при обробці великих об’ємів трафіку. При цьому реалізації ґешування в OpenSSL дозволяє обробляти до 696 МБ/с, залежно від вибраного алгоритму [20].

BoringSSL, хоч і менш гнучкий щодо вибору ґеш-функцій, у межах TLS 1.3 суворо дотримується використання SHA-256 або SHA-384, що спрощує і прискорює обчислення, одночасно мінімізуючи ризики неправильного конфігурування. Властиво, що реалізація ґешування в BoringSSL демонструє кращі результати за OpenSSL, обробляючи до 873 МБ/с [16].

У випадку CryptoAPI, незважаючи на додавання SHA-3 у нові версії Windows 10/11 (через BCryptCreateHash), підтримка обмежена до певних конфігурацій, а продуктивність суттєво нижча. CryptoAPI демонструє нижчі швидкості – до 320 МБ/с для SHA3-256, через менш ефективну реалізацію та обмеження в API [21]. Це робить CryptoAPI менш привабливим у високонавантажених TLS-серверах.

У підсумку, хоча всі три криптопровайдери підтримують основні алгоритми, OpenSSL та BoringSSL мають значну перевагу у швидкодії та адаптивності до сучасних криптографічних вимог. OpenSSL, як більш універсальний та широко підтримуваний інструмент, залишається стандартом де-факто у серверних реалізаціях TLS, тоді як BoringSSL, орієнтований на клієнтські мобільні платформи, забезпечує найкращу продуктивність у цих умовах. CryptoAPI, натомість, має більшу інтеграцію з екосистемою Windows, але поступається у гнучкості та швидкості.

Таким чином, криптографічні провайдери значною мірою впливають на продуктивність та безпеку реалізації TLS, забезпечуючи різні рівні оптимізації, підтримку апаратного прискорення та інтеграцію з операційними системами. Розуміння особливостей імплементації
алгоритмів у криптографічних провайдерах дозволяє ефективно обирати рішення залежно від вимог до продуктивності, безпеки та сумісності.

Проілюструємо результати досліджень у вигляді табл. 2.

Таблиця 2

Порівняльний аналіз ефективності криптопровайдерів щодо реалізації протоколу TLS

Критерій порівняння	Криптопровайдери		
	OpenSSL	BoringSSL	Crypto API
Загальні характеристики	Потужна, кросплатформена бібліотека з відкритим кодом, яка підтримує більшість сучасних криптографічних алгоритмів. Активно розвивається, широко використовується у серверних продуктах.	Форк OpenSSL, розроблений Google з акцентом на безпеку, спрощення коду та видалення застарілих або ризикованих функцій. Найчастіше застосовується в мобільних і браузерних клієнтах.	Вбудований компонент Windows, інтегрований у системні служби. Забезпечує базовий набір криптоопераций із пріоритетом сумісності, стабільності та сертифікації (наприклад, FIPS).
Реалізація симетричного шифрування (AES, ChaCha20)	Забезпечує високопродуктивне симетричне шифрування через апаратне прискорення (AES-NI). Реалізація ChaCha20 оптимізована під ARM-процесори, що забезпечує ефективність на мобільних пристроях.	Висока швидкодія реалізації ChaCha20-Poly1305, оптимізована для мобільних платформ. Код суттєво спрощений, що мінімізує ймовірність вразливостей у реалізації симетричних алгоритмів.	Працює через абстрактні інтерфейси (наприклад, BCryptEncrypt), що знижує продуктивність. Підтримує AES, але реалізація менш ефективна, особливо у сценаріях з великою кількістю одночасних потоків.
Реалізація асиметричного шифрування (RSA, ECDSA, ECC)	Повна підтримка RSA, ECDSA, X25519, з можливістю апаратного прискорення (наприклад, через Intel QAT). Після версії 3.0 — підтримка нових кривих, включно з Brainpool.	Орієнтація на сучасні криві (X25519, P-256) із видаленням застарілих та малозатребуваних алгоритмів. Забезпечує швидке встановлення TLS-з’єднань, особливо в мобільних браузерах.	Підтримує сучасні еліптичні криві через інтерфейс CNG, однак гнучкість налаштувань обмежена. Деякі криві недоступні без сторонніх обгорток або налаштування реєстру.
Реалізація ґеш-функцій (SHA-1,	Реалізація з SIMD-оптимізацією дозволяє	Використовуються лише SHA-256 та SHA-384 у межах	Підтримка SHA-2 стабільна, SHA-3 реалізовано лише в

SHA-2, SHA-3)	досягати високої швидкодії при обробці великих обсягів даних. Повна підтримка SHA-2 та SHA-3, можливість паралельної обробки.	TLS 1.3. Така обмеженість зменшує ймовірність помилок, водночас забезпечуючи стабільну і швидку роботу.	нових версіях Windows 10/11. Продуктивність нижча в порівнянні з OpenSSL, особливо в контексті TLS-серверів
Безпека використання	Висока, за умови правильної конфігурації: бібліотека містить підтримку сучасних алгоритмів, але залишає можливість використання застарілих та слабких cipher suites (наприклад, RC4, 3DES), якщо явно не вимкнути.	Висока за рахунок видалення слабких або deprecated алгоритмів, відсутня підтримка RC4, SSLv3 тощо. Знижений ризик помилок конфігурації.	Стабільна, але залежна від політики оновлень Windows. Підтримка обмежена лише сертифікованими примітивами. Застарілі алгоритми можуть залишатися доступними в системі за замовчуванням.

Під час аналізу сучасних криптографічних провайдерів виявлено, що рішення з відкритим кодом, такі як OpenSSL та BoringSSL, демонструють високу продуктивність, адаптивність до новітніх криптографічних стандартів і швидку реакцію на виявлені вразливості. Особливу увагу заслуговує BoringSSL, оптимізований для мобільних платформ, де критично важливими є затримки з'єднання та ефективне використання ресурсів. Водночас реалізації від Microsoft, як-от CryptoAPI, забезпечують глибоку інтеграцію в екосистему Windows, проте мають обмеження в налаштуваннях і підтримці сучасних криптографічних примітивів, що знижує їхню придатність у високонавантажених сценаріях.

Загальний рівень безпеки протоколу TLS залежить не лише від його формальної специфікації, але й від правильності та актуальності реалізації з боку постачальників криптографічних функцій. Наявність вразливостей, таких як Heartbleed, POODLE, Lucky13 або BEAST, свідчить про необхідність постійного оновлення бібліотек, відмови від застарілих версій TLS і шифрувальних наборів, а також впровадження сучасних захистів, зокрема механізмів forward secrecy та strict certificate validation.

Висновки

У результаті дослідження встановлено, що протокол TLS є фундаментальним елементом захисту інформації під час її передавання в мережевих середовищах. Його надійність забезпечується за рахунок поєднання симетричних і асиметричних алгоритмів шифрування, а також криптографічних ґеш-функцій, що разом створюють багаторівневу архітектуру безпеки. Ефективність і стійкість TLS значною мірою залежить від якості реалізації криптографічних провайдерів, які виконують обчислювальні операції, керують криптографічними ключами, а також забезпечують обробку цифрових сертифікатів.

У реалізаціях криптографічного забезпечення доцільно орієнтуватися на OpenSSL або BoringSSL як найбільш актуальні, продуктивні та гнучкі рішення з широкою підтримкою сучасних криптографічних стандартів. Для підвищення безпеки мережевої інфраструктури важливо забезпечити регулярне оновлення криптографічних бібліотек, контроль за налаштуванням TLS-з'єднань, перевірку сертифікатів та обмеження підтримки слабких алгоритмів. Необхідно також досліджувати можливості апаратного прискорення криптографічних операцій для забезпечення масштабованості та високої ефективності систем захисту.

З огляду на динамічний розвиток інформаційних технологій, особливу актуальність набуває адаптація TLS до умов постквантової криптографії. Зважаючи на загрозу, яку становлять квантові обчислення для сучасних криптосистем, провайдери криптографічних послуг та криптобібліотеки мають інтегрувати квантово-стійкі алгоритми в архітектуру TLS та
забезпечити їхню ефективну підтримку.

У перспективі доцільним є розвиток інструментів моніторингу безпеки TLS, аналізу роботи криптопровайдерів у реальному часі, а також підготовка до поступового переходу на

квантово-стійкі криптографічні протоколи як запоруки збереження конфіденційності та цілісності даних у майбутніх поколіннях мережевих технологій.

Список літератури:

1. Dierks T., and Rescorla E. The Transport Layer Security (TLS) Protocol Version 1.2 (RFC 5246) // Internet Engineering Task Force (IETF). 2008 https://doi.org/10.17487/RFC5246
2. Lee Jae-Ho. Analysis of SSL Communication Process in CNG Crypto Library // The Journal of Korean Institute of Communications and Information Sciences. 2017. Vol. 42, no. 5. P. 1027–1037. https://doi.org/10.7840/kics.2017.42.5.1027
3. Lee Jaeho, and Wallach Dan S. Removing Secrets from Android's TLS // Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security (AsiaCCS '19), ACM, 2019. https://doi.org/10.1145/3321705.3329810
4. Naser Abu, et al. Performance Evaluation and Modeling of Cryptographic Libraries for MPI Communications // Proceedings of the 2022 IEEE International Parallel and Distributed Processing Symposium (IPDPS). 2022. P. 1192–1201. https://doi.org/10.1109/IPDPS53621.2022.00104
5. Howard Bryan. Applying Cryptography Using the CNG API in Windows Vista // MSDN Magazine, July 2007. https://learn.microsoft.com/en-us/archive/msdn-magazine/2007/july/applying-cryptography-using-the-cng-api-in-windows-vista
6. Bernstein, Daniel J., et al. OpenSSLNTRU: Faster post-quantum TLS key exchange // 31st USENIX Security Symposium (USENIX Security 22). 2022. P. 359–376. https://www.usenix.org/conference/usenixsecurity22/presentation/bernstein
7. Schneier, B. Applied Cryptography: Protocols, Algorithms, and Source Code in C (20th Anniversary ed.). Wiley, 2015
8. Rescorla, E. The Transport Layer Security (TLS) Protocol Version 1.3 (RFC 8446) // Internet Engineering Task Force (IETF). 2018. https://doi.org/10.17487/RFC8446
9. Rizzo J., and Duong T. BEAST: Surprising crypto attack against HTTPS // Presented at Ekoparty Security Conference. 2011. https://hal.science/hal-01154820/document
10. Moeller B. This POODLE Bites: Exploiting The SSL 3.0 Fallback // Google Security Blog. 2014. https://security.googleblog.com/2014/10/this-poodle-bites-exploiting-ssl-30.html
11. Durumeric Z., Kasten J., Adrian D., Halderman J. A., Bailey M., Li F., ... and Ensafi R. The Matter of Heartbleed // Proceedings of the 2014 Conference on Internet Measurement Conference. 2014. P. 475–488. https://doi.org/10.1145/2663716.2663755
12. AlFardan N. J., and Paterson K. G. Lucky Thirteen: Breaking the TLS and DTLS Record Protocols // 2013 IEEE Symposium on Security and Privacy. 2013. P. 526–540. https://doi.org/10.1109/SP.2013.13
13. Bleichenbacher D. Chosen Ciphertext Attacks Against Protocols Based on the RSA Encryption Standard // Advances in Cryptology – CRYPTO '98. 1998. P. 1–12. Springer. https://doi.org/10.1007/BFb0055716
14. Calomel.org. AES-NI SSL Performance Benchmarks, 2022 https://calomel.org/aesni_ssl_performance.html
15. OpenSSL Software Foundation. OpenSSL: Cryptography and SSL/TLS Toolkit. https://www.openssl.org
16. GitHub. Performance degradation in the FIPS-BoringSSL version being used by Envoy, 2021. https://github.com/envoyproxy/envoy/issues/19037
17. OpenSSL Cookbook 3rd Edition - 1.4 Performance. Feisty Duck | SSL/TLS and PKI training and books, 2020. https://www.feistyduck.com/library/openssl-cookbook/online/openssl-command-line/performance.html
18. BoringSSL Gerrit. Use packed representation for large Curve25519 table, 2023. https://boringssl-review.googlesource.com/c/boringssl/+/60107
19. Microsoft Docs. ECC Curve Support in CNG. Microsoft, 2023. https://learn.microsoft.com/en-us/windows/win32/seccng/cng-named-elliptic-curves
20. Security and So Many Things. Hashing Methods Benchmark, 2021. https://asecuritysite.com/openssl/openssl_full2b
21. GitHub. BenchmarkDotNet Crypto Hash Test, 2023. https://github.com/dotnet/BenchmarkDotNet

Надійшла до редколегії 10.02.2025

Відомості про авторів:

Тельнова Аліна Анатоліївна – Харківський національний університет радіоелектроніки, бакалавр кафедри безпеки інформаційних технологій факультет комп'ютерної інженерії та управління; Україна; e-mail alina.telnova@nure.ua; ORCID: https://orcid.org/0009-0001-3574-7425

Балагура Дмитро Сергійович – канд. техн. наук, доцент, Харківський національний університет радіоелектроніки, доцент кафедри безпеки інформаційних технологій, факультет комп'ютерної інженерії та управління, Україна; e-mail: dmytro.balahura@nure.ua; ORCID: https://orcid.org/0009-0006-9839-3317

Фроленко Владислав Олегович – Харківський національний університет радіоелектроніки, аспірант кафедри безпеки інформаційних технологій факультет комп'ютерної інженерії та управління, Україна; e-mail: vladyslav.frolenko@nure.ua; ORCID: https://orcid.org/0009-0004-3730-3432

Сухотеплий Владислав Миколайович – Харківський національний університет Повітряних Сил імені Івана Кожедуба, старший викладач кафедри радіоелектронних систем пунктів управління Повітряних Сил, Україна; e-mail: vladislav181168@gmail.com; ORCID: https://orcid.org/0000-0002-2566-4167

Флоров Сергій Володимирович – канд. техн. наук, Університет митної справи та фінансів, доцент кафедри кібербезпеки та інформаційних технологій, факультет інноваційних технологій, Україна; e-mail: pre.pod@hotmai.com; ORCID: https://orcid.org/0000-0002-4682-7666

УДК 004.056.55 **DOI:10.30837/rt.2025.2.221.10**

Є.В. КОТУХ, канд. техн. наук, Г.З. ХАЛІМОВ, д-р техн. наук, І.Є. ДЖУРА

КРИПТОГРАФІЧНА КОНКУРЕНТОСПРОМОЖНІСТЬ КРИПТОСИСТЕМ НА ОСНОВІ НЕКОМУТАТИВНИХ ГРУП

Вступ

Сучасна криптографія стоїть на порозі фундаментальних змін, зумовлених стрімким розвитком квантових обчислень. Побудова повномасштабного квантового комп'ютера несе пряму загрозу для більшості криптографічних систем, що використовуються сьогодні. Алгоритм Шора, запропонований у 1994 р., дозволяє розв'язувати задачі факторизації цілих чисел та дискретного логарифмування за поліноміальний час [1]. Саме на складності цих задач базується безпека таких поширених систем, як RSA, DSA та криптографія на еліптичних кривих (ECC).

Поточний стан розробки квантових комп'ютерів демонструє неухильний прогрес. Компанії IBM, Google, IonQ та інші досягли значних успіхів у створенні квантових процесорів з десятками та сотнями кубітів. Експертні оцінки щодо появи криптографічно релевантного квантового комп'ютера (CRQC) – системи, здатної зламати сучасні криптографічні стандарти, – варіюються від 10 до 30 років [2]. Однак принцип "збирай сьогодні, розшифровуй завтра" змушує вже зараз переходити до постквантової криптографії, оскільки конфіденційні дані, зашифровані сьогодні, можуть зберігати свою цінність протягом десятиліть.

Усвідомлення цієї загрози стимулювало глобальний рух до розробки та стандартизації постквантових криптосистем (Post-Quantum Cryptography, PQC) – алгоритмів, стійких до атак як з боку класичних, так і квантових комп'ютерів. Національний інститут стандартів і технологій США (NIST) з 2016 р. проводить міжнародний конкурс з відбору стандартів PQC [3]. У 2022 р. було завершено перший раунд стандартизації, в результаті якого було обрано чотири алгоритми: CRYSTALS-Kyber (інкапсуляція ключів), CRYSTALS-Dilithium та FALCON (цифрові підписи), а також SPHINCS+ (резервний алгоритм підписів). Усі ці рішення базуються на решітчастій криптографії та криптографії геш-функцій.

Серед основних напрямів досліджень у галузі PQC виділяють криптографію на основі кодів, що виправляють помилки (code-based), геш-функцій (hash-based), решіток (lattice-based), багатовимірних поліномів (multivariate) та некомутативних груп (non-commutative group-based) [4]. Примітно, що алгоритми на основі некомутативних груп не увійшли до першого набору стандартів NIST, що частково пояснюється їх відносною новизною та складністю аналізу безпеки. Однак четвертий раунд конкурсу NIST, який триває, розглядає альтернативні підходи, включаючи системи на некомутативних групах [5].

Криптосистеми на основі некомутативних груп представляють особливий інтерес завдяки унікальним властивостям некомутативних алгебраїчних структур. Некомутативність – властивість, за якої результат операції залежить від порядку операндів – забезпечує природний захист від квантових алгоритмів, які ефективно працюють з комутативними структурами. Основними представниками цього напряму є групи кіс (braid groups), матричні групи над кінцевими кільцями, групи автоморфізмів та поліциклічні групи. Ці системи демонструють привабливі характеристики: компактність ключів, високу швидкість криптографічних операцій та потенційну стійкість до як класичних, так і квантових атак.

Однак розробка практичних криптосистем на некомутативних групах стикається з низкою викликів. По-перше, це складність ретельного аналізу криптографічної стійкості через нестандартні математичні основи порівняно з класичними підходами. По-друге, необхідність забезпечення балансу між безпекою, продуктивністю та розміром ключів/підписів відповідно до сучасних практичних вимог. По-третє, важливість забезпечення сумісності з існуючою інфраструктурою та підтримки криптографічної гнучкості (crypto-agility) – здатності швидко переходити між різними алгоритмами у разі виявлення вразливостей [6].

Актуальність дослідження криптосистем на некомутативних групах зумовлена кількома факторами. Насамперед, принцип диверсифікації криптографічних підходів вимагає розробки альтернативних рішень, заснованих на різних математичних засадах. Монокультура в постквантовій криптографії, коли усі системи базуються на решітчастих задачах, створює ризик одночасного компрометування всіх алгоритмів у випадку прориву в методах їх аналізу. Некомутативні групи можуть слугувати як резервне або доповнююче рішення, забезпечуючи криптографічну стійкість навіть у разі компрометування основних постквантових стандартів.

Метою даного дослідження є комплексний аналіз криптографічної конкурентоспроможності систем на основі некомутативних груп, оцінка їх переваг і недоліків порівняно з існуючими постквантовими рішеннями, а також визначення перспектив їх практичного застосування в умовах квантової загрози.

Групова криптографія на основі некомутативних груп

Криптографія на основі некомутативних груп є одним з найстаріших і водночас найменш досліджених напрямів PQC. Її привабливість полягає у використанні математичних структур, де задачі, аналогічні задачі дискретного логарифма, вважаються обчислювально складними навіть для квантових комп'ютерів. Прикладами таких задач є задача пошуку спряженого елемента (Conjugacy Search Problem, CSP), задача розкладу елемента за множиною твірних (Decomposition Problem, DP) або проблеми слова (Word Problem, WP) [6].

Безпека криптосистем на некомутативних групах базується на уявній складності цих специфічних задач, на основі яких було розроблено низку протоколів обміну ключами. Відомим прикладом є протокол Аншеля–Аншеля–Гольдфельда (AAG). Це один з перших протоколів, що базується на складності одночасного розв'язання задачі CSP. Два користувачі, Аліса та Боб, обирають секретні елементи з певних комутуючих підгруп і обмінюються публічними ключами, які є результатом спряження. Спільний секретний ключ обчислюється як результат послідовного застосування секретних елементів. Безпека протоколу критично залежить від вибору платформної групи [7]. Протокол Ко–Лі використовує властивості комутаторів. Аліса обирає секретний елемент a, а Боб – b. Вони обмінюються спряженими елементами, і спільний ключ обчислюється як комутатор $[a,b]=aba^{-1}b^{-1}$. Цей протокол також виявився вразливим у багатьох групах [8].

Вибір «правильної» платформної групи є центральною проблемою в некомутативній груповій криптографії. Ідеальна група повинна поєднувати високу складність обчислювальних задач з ефективністю групових операцій та стійкістю до відомих атак [9].

Історично групи кіс (Braid Groups) були першими і найпопулярнішими кандидатами на роль платформних груп. Вони мають інтуїтивну геометричну інтерпретацію, а групова операція (композиція кіс) є відносно простою. Протоколи AAG та Ко–Лі початково пропонувалися саме для груп кіс. Однак з часом було знайдено низку ефективних атак. Атака лінійного розкладу (Linearization attacks) використовує гомоморфні відображення групи кіс в матричні групи, де задача CSP стає значно простішою. Атака на основі довжини (Length-based attacks)

використовує специфічні метрики та властивості нормальних форм (наприклад, нормальна форма Гарсайда) для отримання інформації про секретний ключ. Через ці атаки більшість криптосистем на групах кіс сьогодні вважаються зламаними або небезпечними [10].

Поліциклічні групи (Polycyclic Groups) мають перевагу в ефективному представленні елементів та швидких групових обчисленнях. Це дозволило розробити практичні криптосистеми. Проте, структура цих груп виявилася занадто "регулярною". Атака Усова (Usov's attack) продемонструвала, як можна ефективно лінеаризувати задачу CSP у поліциклічних групах, що робить їх непридатними для криптографії, що використовує проблему CSP [11].

Група Томпсона F (Thompson's Group F) має низку унікальних властивостей, зокрема, вона є нескінченною, скінченно породженою та не містить вільних підгруп. Були спроби побудувати на ній криптосистеми, але задача CSP в цій групі виявилася тривіальною [12]. Дослідження продовжуються, але наразі Група Томпсона F не вважається надійним кандидатом для «платформної» групи.

Групи матриць, такі як $GL(n,q)$, були запропоновані як платформи для протоколів, що базуються на задачі розкладу (DP). Перевагою є швидкі матричні операції. Однак багато таких схем вразливі до атак, що використовують методи лінійної алгебри, наприклад обчислення власних векторів та значень. Протокол MOR виявився вразливим саме через такі методи [13].

Дослідження, результати якого представлено в даній роботі, дало новий імпульс використанню кінцевих простих груп та груп автоморфізмів, що пов'язані з максимальними кривими Деліня–Люстига (Ерміта, Сузукі, Рі) [14 – 23].

Незважаючи на теоретичну привабливість, некомутативна групова криптографія поки не досягла значного успіху в процесі стандартизації PQC NIST. Подані пропозиції не дійшли до фінальних раундів конкурсу NIST PQC. Так, схема цифрового підпису WalnutDSA була однією з найвідоміших кандидатів у першому раунді NIST PQC. Однак схему WalnutDSA, що базується на групах кіс та використовує нову обчислювальну задачу E-Multiplication, було незабаром зламано за допомогою атаки лінійного розкладу [24]. Інші пропозиції на основі груп також були атаковані або не змогли продемонструвати достатню ефективність порівняно з кандидатами на основі решіток чи кодів. Проаналізуємо основні причини, що гальмують стандартизацію криптопримитивів на основі групової криптографії. По-перше, це проблеми з доведенням безпеки, бо формально складно довести складність базових задач для конкретних груп в поєднанні до складної проблеми, що застосовується як «платформне» рішення. По-друге, швидкі реалізації атак на початкові пропозиці підірвали довіру до напряму в цілому. По-третє, багато з опублікованих групових протоколів мають великий розмір ключів та/або повільні операції порівняно з лідерами PQC, такими як Kyber та Dilithium. І хоча, на думку автора, великий розмір ключів в постквантову еру не є фактором, що міг би заблокувати рішення від подальшого розгляду в поєднанні з висвітленими проблемами, це визивало скепсіс у експертів NIST.

Сучасний стан криптографії на основі некомутативних груп можна охарактеризувати як період обережного оптимізму та інтенсивного пошуку. Після хвилі успішних атак на перше покоління протоколів спільнота усвідомила, що вибір платформної групи та дизайну протоколу є надзвичайно складним завданням. Проаналізуємо основні виклики для створення успішного PQC кандидата на основі групової некомутативної криптографії. По-перше, зрозуміло, що основним викликом є пошук надійних платформ – груп, що не допускають «простих» гомоморфізмів у лінійні групи та є стійкими до атак на основі структурних властивостей. По-друге, формальний аналіз безпеки та доведення складності обчислювальних задач

для кандидатних груп має бути наведено з урахуванням сучасного уявлення про побудову та реалізацію атак з використанням квантового компьютера. По-трете, проблема підвищення ефективності, а саме зменшення розміру ключів або реалізація прискоренних обчислень, мала б на меті демонстрацію криптографічної конкурентоспроможності з іншими PQC-напрямами.

Одним із підходів у цьому напряму є використання криптосистем на основі логарифмічних підписів (Logarithmic Signatures, LS), зокрема сімейства MST [25 – 29]. Історично реалізації, такі як криптосистема MST3, використовували для криптографічних перетворень, переважно центр скінченної некомутативної групи (наприклад, групи Сузукі). Такий підхід має суттєвий недолік: потужність (порядок) центру групи значно менша за потужність самої групи. Це обмежує як розмір простору повідомлень, так і варіативність криптографічних перетворень, що потенційно звужує простір ключів та може створювати вразливості.

Дане дослідження узагальнює результати розробки та аналізу нового підходу до побудови криптосистем на некомутативних групах. В якості математичної платформи було обрано групи автоморфізмів функціональних полів, асоційованих з максимальними кривими Деліня–Люстига, а саме кривими Ерміта, Сузукі та Рі. Ці групи є багатопараметричними, мають надзвичайно великий порядок та складну внутрішню структуру, що робить їх привабливими кандидатами для побудови стійких постквантових криптосистем.

Метою статті є представлення узагальненої моделі для класу криптосистем на основі логарифмічних підписів, проведення порівняльного аналізу різних платформних груп (Сузукі, Ерміта, Рі) та оцінка їхньої криптографічної конкурентоспроможності з погляду безпеки та затрат на реалізацію.

Результати дослідження криптосистем на основі груп з використанням логарифмічних підписів

В основі дослідження груп лежить теорія алгебраїчних кривих над скінченними полями. Важливим класом максимальних кривих є так звані криві Деліня–Люстига, що виникають у теорії представлень скінченних груп типу Лі [30]. У дослідженні було розглянуто три родини таких кривих – Ерміта, Сузукі та Рі. Ці групи автоморфізмів є скінченними простими або майже простими групами типу Лі. Вони мають великий порядок та неабелеву структуру, що робить їх ідеальними кандидатами для побудови криптосистем. На відміну від груп кіс, ці групи є 3-х або 4-параметричними, що ускладнює їх аналіз та потенційно робить обчислювальні задачі складнішими. Порядок цих груп зростає поліноміально з високим степенем від розміру поля, що створює великий простір для ключів. Замість класичних протоколів AAG/Ко–Лі для цих груп було розроблено метод направленого шифрування на основі логарифмічних підписів. Концепція логарифмічного підпису є центральною для криптосистем сімейства MST. На практиці він реалізується у вигляді представлення, де кожному елементарному блоку повідомлення ставиться у відповідність певний елемент групи. У класичній криптосистемі MST3 повідомлення відображалося в центр групи $Z(G)$, що обмежувало як простір повідомлень, так і варіативність перетворень.

Ключова ідея дослідження полягає у відмові від обмеження центром групи та використанні для шифрування значно більших її підструктур – ядра гомоморфізму або повної групи. Запропонований метод направленого шифрування дозволяє подолати головний недолік старих систем MST – обмеженість центром групи. Таким чином, вдалося значно збільшити розмір повідомлення та потенційну криптостійкість.

Загальний алгоритм можна представити у вигляді блок-схеми:

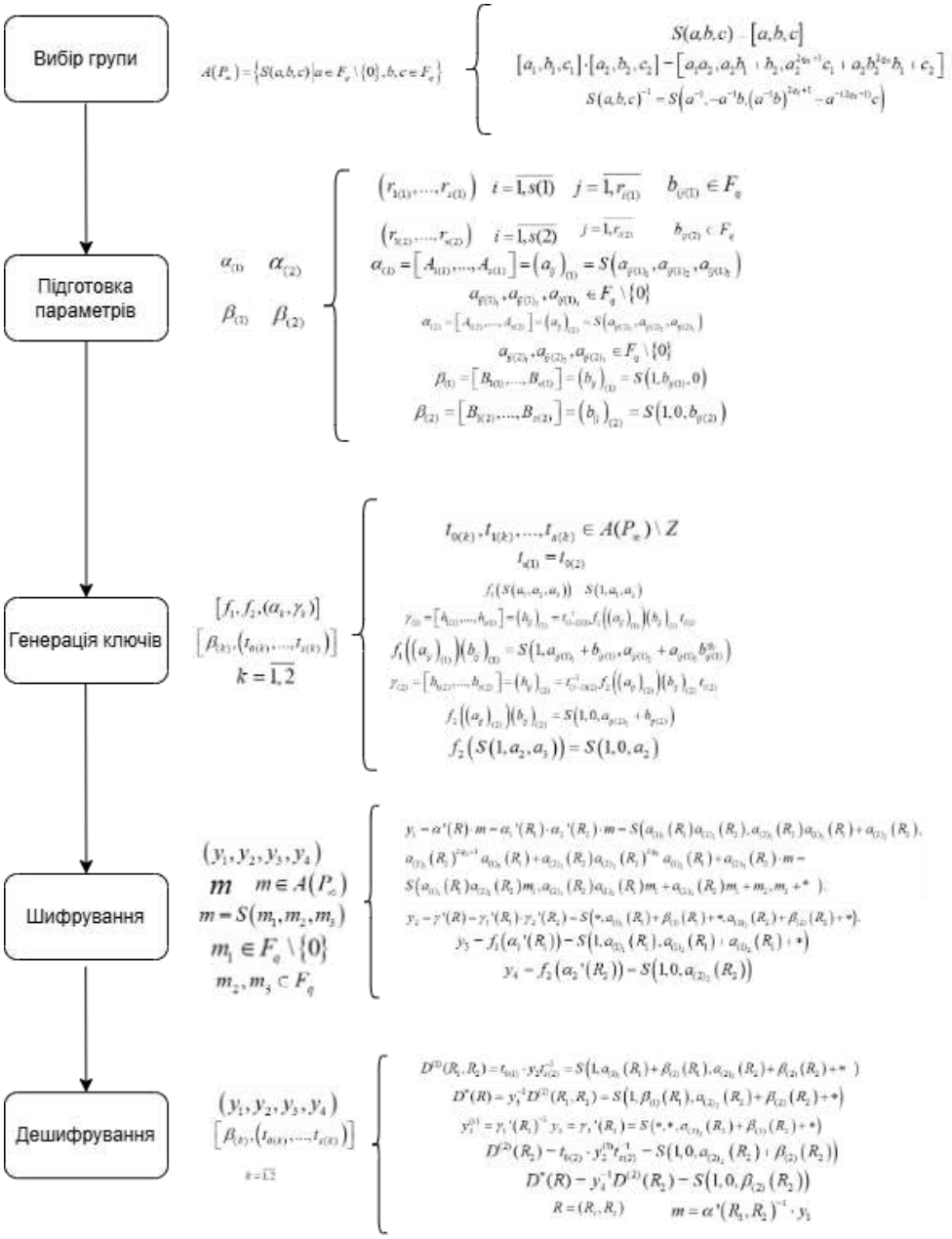

Рис. 1. Блок-схема загального алгоритму направленого шифрування на максимальних групах Деліня–Люстига

В якості математичної платформи було обрано групи автоморфізмів функціональних полів, асоційованих з максимальними кривими Деліня–Люстига: кривими Ерміта, Сузукі та Рі. Ці групи є скінченними простими або майже простими групами типу Лі. Вони мають великий порядок та складну неабелеву структуру, що робить їх ідеальними кандидатами для побудови стійких криптосистем. На відміну від груп кіс, ці групи є 3-х або 4-параметричними, що ускладнює їх аналіз та потенційно робить обчислювальні задачі складнішими.

ISSN 0485-8972 Radiotekhnika No. 221 (2025)
eISSN 2786-5525

Таблиця 1

Порівняльні характеристики платформних груп

Артефакти	**Автоморфізми функціонального поля групи Сузукі**	**Автоморфізми функціонального поля групи Ерміта**	**Автоморфізми функціонального поля групи Рі**
Група	$A(P_\infty)=\{S(a,b,c)\mid a\in F_q\setminus\{0\}, b,c\in F_q\}$	$A(P_\infty)=\{S(a,b,c)\mid a\in F_q\setminus\{0\}, b,c\in F_q\}$	$A(P_\infty)=\{a(x),\beta(x),y(x),h(\lambda),I^{-}\mid x\in F_q,\lambda\in F_q^{x}\}$
Порядок	$OrdA(P_\infty)=q^2$	$OrdA(P_\infty)=q^3(q^2-1)$	$OrdA(P_\infty)=q^3$
Кількість параметрів	3-параметрична	3-параметрична	4-параметрична
Скінченне поле	F_q	F_q	F_q
Структура центра			
Елемент групи	$S(a,b,c)=[a,b,c]$	$S(a_1,b_1,c_1)\cdot S(a_2,b_2,c_2)=S(a_1a_2,a_2b_1+b_2,a_2^{q+1}c_1+a_2b_2^qb_1+c_2)$	$S(a,b,c)=a(a)\beta(b)\gamma(c)$
Зворотній елемент групи	$S(a,b,c)^{-1}=S(a^{-1},-a^{-1}b,(a^{-1}b)^{2q_0+1}-a^{-(2q_0+1)}c)$	$S(a,b,c)^{-1}=S(a^{-1},-a^{-1}b,-a^{-(g+1)}c+a^{-(g+1)}b^{q+1})$	$S(a,b,c)^{-1}=S(-a,-b-a^{3t+1},-c-ab+a^{3t+2})$
Гомоморфізми	$f_1(S(a_1,a_2,a_3))=S(1,a_1,a_2)$ $f_2(S(1,a_2,a_3))=S(1,0,a_2)$	$f_1(S(a_1,a_2,a_2^{q+1}/2))=S(1,a_2,a_2^{q+1}/2)$ $f_2(S(a_1,a_2,a_2^{q+1}/2))=S(1,0,a_2)$	$f((a_{ij})_{(1)})(b_{ij})_{(1)}=S(0,a_{ij(1)_1},a_{ij(1)_2})S(0,b_{ij(1)},0)=S(0,a_{ij(1)_1}+b_{ij(1)},a_{ij(1)_2})$, $f((a_{ij})_{(2)})(b_{ij})_{(2)}=S(0,0,a_{ij(2)_2})S(0,0,b_{ij(2)})=S(0,0,a_{ij(2)_2}+b_{ij(2)})$
Розмір логарифмічного підпису	<256 записів по 128 біт	<256 записів по 128 біт	256 записів по 64 біти
Особливості	Просте представлення при непарній характеристиці	Ефективні обчислення в полях характеристики 2	Найбільший порядок та кількість параметрів серед груп на кривих Деліня–Люстіга
Атака грубою силою на зашифрований текст	$O(q^2)$, визначається повним порядком групи	$O(q^3)$, визначається вичерпним пошуком по всій групі	$O(q^2)$, визначається повним порядком групи
Атака грубою силою на $R=(R_1,R_2)$.	$O(q)$, забезпечується зв'язуванням ключів	$O(q^l)$, забезпечується зв'язуванням ключів та гомоморфним шифруванням	$O(q^2)$, забезпечується зв'язуванням ключів та гомоморфним шифруванням
Атака грубою силою на $(t_{0(k)},\dots,t_{s(k)})$.	$O(q)$	$O(q^5)$	$O(q^3)$
Атака на алгоритм	$O(q^2)$	$O(q^5)$	$O(q^2)$
Оцінка PQC стійкості	Висока, оскільки для задачі WP невідомі ефективні квантові алгоритми	Висока, оскільки невідомі ефективні квантові алгоритми	Найвища з розглянутих, зважаючи на максимальний порядок та складність структури

У класичній криптосистемі MST3 повідомлення відображається в центр групи Z(G), який є абелевою підгрупою. Це дозволяє легко виконувати обчислення, але обмежує простір зашифрованих значень. Гіпотеза дослідження полягала в тому що використання логарифмічних підписів з відображенням на всю групу, а не тільки в центр групи як в базовій конструкції MST3 не в центр, дозволяє суттєво збільшити довжину повідомлення, яке можна зашифрувати за одну ітерацію та розширити простір ключів та підвищити загальну криптографічну стійкість системи за рахунок використання складнішої структури всієї групи. Практичні результати, що викладені в табл. 1, підтверджують гипотезу.

Використовуючи всю групу для шифрування, вдалося значно збільшити розмір повідомлення та потенційну криптостійкість. Як показано у дослідженні, початкові версії направленого шифрування були вразливі до атак послідовного відновлення. Цю проблему було вирішено шляхом зв'язування ключів та застосування гомоморфного шифрування до випадкових покриттів, що є важливим кроком до створення практично безпечної системи.

Використання багатопараметричних груп дозволяє досягати високого рівня безпеки при відносно менших розмірах скінченного поля. Це прямо впливає на затрати на ключі та загальні параметри. Застосування розроблених контрзаходів дозволяє довести складність атаки на криптосистему до повного перебору по всій групі. Продемонструємо отримані в роботах [14 – 23] результати.

Результати дослідження платформних груп

Дослідження дозволило отримати низку вагомих наукових та практичних результатів, що підсумовано нижче.

Привабливими групами є групи з центром, який визначається елементарною 2 абелевою групою, що досягається на скінченних полях характеристики 2. Застосування логарифмічних підписів та випадкових покриттів призводить до низьких витрат на загальні параметри криптосистеми.

Таким класом груп, з накриттям Галуа ступеня *m* та з характеристикою 2, є узагальнені 2-групи Сузукі. Узагальнені 2-групи Сузукі є багатопараметричними групами і можуть мати довільний великий порядок. Криптосистеми MST на основі узагальненої 2-групи Сузукі потенційно мають перевагу над іншими реалізаціями схем у секретності та реалізації. Використання багатопараметричних груп потенційно забезпечує кращі характеристики в реалізації за рахунок оптимізації обчислення по параметрах групи та розміру скінченного поля. Максимальна підгрупа повної групи автоморфізмів $A(P_\infty)$ ототожнюється з трійкою $A(P_\infty)=\left\{[a,b,c]\,|\,a,b,c\in K, a\neq 0,\ ma\ c^{q_0}+c=b^{q_0+1}\right\}$, має порядок більший ніж порядок групи Сузукі, що дорівнює $ordH(P_\infty)=q^3\left(q^2-1\right)$. Для непарної характеристики поля F_{q^2} група автоморфізмів $A(P_\infty)$ визначається як $A(P_\infty)\left\{\left[a,b,\frac{b^{q+1}}{2}+c\right]\middle| a\in F_{q^2}^*, b\in F_{q^2}\ \ and\ \ c^q+c=0\right\}$. Для непарного характеристичного поля група автоморфізмів $A(P_\infty)$ функціонального поля Ерміта має просте представлення. Обчислювальні вектори з використанням матриць логарифмічних підписів і випадкових покриттів легко транскодуються в координати підгрупи $A(P_\infty)$.

Вперше запропонований метод направленого шифрування по групі автоморфізмів функціонального поля функцій Сузукі має переваги у високій секретності схеми шифрування на основі групи автоморфізмів $A(P_\infty)$ функціонального поля Сузукі над F_q, що дорівнює q^2. При цьому довжина зашифрованого тексту визначається значенням $3\log q$ для обчислення в скінченному полі над F_q, довжина логарифмічного масиву підпису визначається кінцевим полем понад F_q і значно менше порівняно з криптосистемою MST3, а обчислення в кінцевому полі простіші, в порівнянні з криптосистемою MST3 по групі Сузукі, за рахунок обчислення оберненого елемента в кінцевому полі розмірності, яка в два рази більша.

Вперше запропоновано метод направленого шифрування на групах автоморфізмів функціонального поля Ерміта. Було розроблено та обгрунтовано нове рішення, яке полягає в тому, щоб побудувати логарифмічний підпис поза центром групи для реалізації шифрування по всім координатам групи. Таке рішення дало можливість зменшити розмір кінцевого поля F_{q^2}, складність обчислення при фіксованій секретності криптосистеми. Практично це реалізується за рахунок обчислень в квадратичному полі непарної характеристики. Для перекодування значень обчислювальних векторів в координати групи Ерміта вимагається вирішення рівняння $c^q + c = 0$. Для непарної характеристики квадратичного поля такі рішення знаходяться за виразом $c_i = \gamma^{(q+1)/2+i(q+1)}$, $i = 0,1,...q-1$. Функціональне поле Ерміта є розширенням Галуа над $\mathrm{F}_{q^2}(x)$ з великою групою автоморфізмів, фіксовані поля підгруп групи автоморфізмів надають багате джерело максимальних функціональних полів. Для функціонального поля Ерміта існує кілька сімейств підгруп $A(P_\infty)$.

Метод направленого шифрування на групах функціонального поля Ерміта було вдосконалено використанням гомоморфного перетворення. Складність атаки відновлення ключа в такій криптосистемі визначається вичерпним пошуком по всій групі. У запропонованій криптосистемі з гомоморфним шифруванням випадкові покриття є секретом для криптоаналітика. У цьому випадку відомі атаки на основі слабкості логарифмічних підписів неможливі. Криптосистема MST3, що заснована на групі автоморфізму функціонального поля Ерміта, має перевагу над реалізаціями по групі Сузукі в секретності та реалізації.

Вперше побудовано метод направленого шифрування по малій групі Рі, який, на відміну від MST3 по групі Сузукі, використовує шифрування по ядру групи, що дозволило збільшити розмір повідомлення для зашифрування до значення $|m| = q^2$. Розроблено удосконалення методу направленого шифрування по малій групі Рі на основі шифрування по повній групі $U(q) = \left\{ S(a,b,c) \middle| a,b,c \in F_q \right\}$ зі зв'язаними ключами $R = (R_1, R_2, R_3)$, що дозволило захиститися від атаки послідовного відновлення та забезпечити складність атаки грубої сили q^3.

Криві Рі є максимальними кривими найбільшого роду і мають найбільші групи, що породжуються кривою. Група автоморфізмів по кривій Рі є 4-параметричною групою над полем F_q. Це найбільша група по максимальним кривим Деліня–Люстіга.

Вперше побудовано метод направленого шифрування по групі автоморфізмів функціонального поля Рі, який, на відміну від MST3 по групі Сузукі, використовує шифрування по ядру групи, що дозволило збільшити розмір повідомлення для зашифрування до значення $|m| = q^4$. Розроблено удосконалення методу направленого шифрування по групі автоморфізмів функціонального поля Рі на основі шифрування на повній групі зі зв'язаними ключами, що дозволило захиститися від атаки послідовного відновлення на основі зв'язування ключів логарифмічних підписів та забезпечити складність атаки грубої сили q^4. Група автоморфізмів по кривій Рі $A(P_\infty)$ з $\left|A(P_\infty)\right| = q^3(q-1)$ є максимальною підгрупою і це більше в q рази потужності групи автоморфізмів по кривій Сузукі, та в $q^{3/2}$ рази більше в порівнянні з групою автоморфізмів по кривим Ерміта. Побудова криптосистем на малих групах Рі та автоморфізмах групи Рі має кращі характеристики по секретності та реалізації.

Запропоновано удосконалення методу направленого шифрування по групі автоморфізмів функціонального поля Рі на основі секретного гомоморфного перетворення для випадкових покриттів, що забезпечує захист від послідовних атак відновлення та атак з вибраним текстом, і складність атаки відновлення ключа буде визначатися вичерпним перебором по всій групі автоморфізмів. Реалізація криптосистеми на групі автоморфізмів $A(P_\infty)$ функціонального поля Рі вимагає побудови логарифмічного підпису β на векторах 2^h, де h визначається розміром типу $r_i = 2^h$. Всі блоки B_i є підгрупами $U(q) = \left\{ S(1,b,c) \middle| b,c \in F_q \right\}$. Розмір

масивів β і α визначається типом $(r_1,...,r_s)_b$ і $(r_1,...,r_s)_c$ по координатам b,c для підгруп $U(q)$. Для 128-бітної криптографії, яка еквівалентна обчисленням над полем, $q=2^{64}$, якщо r_i тип $r_i=2^2$, $s=32$, для криптографії в групі потрібні лише 256 записів по 64 біти. У порівнянні з MST3 у Сузукі 2-групі матиме 256 записів по 128 біт для $r_i=2^2$, $s=64$ і 512 записів для $r_i=4^2$, $s=32$. Таким чином, побудова криптосистем на логарифмічних підписах по багатопараметричним групам потенційно забезпечує кращі характеристики в реалізації за рахунок оптимізації обчислення по параметрах групи та розміру скінченного поля.

Висновки

Фактично розроблено новий клас криптосистем. Створено та формалізовано метод «направленого шифрування», який ефективно використовує всю структуру великих некомутативних груп, долаючи обмеження класичних підходів, що базувалися на центрі групи. Проведено порівняльний аналіз платформ. Дослідження підтвердило, що збільшення кількості параметрів групи та її порядку напряму впливає на потенційну секретність та ефективність криптосистеми. Група Рі, як чотирипараметрична група найбільшого порядку, виявилася найбільш потужною та перспективною платформою. Досягнуто високого рівня безпеки. Запропоновані удосконалення (зв'язування ключів та гомоморфне шифрування покриттів) ефективно нейтралізують відомі атаки. Складність атаки методом грубої сили на посилені системи оцінюється повним порядком відповідної групи (наприклад, O(q8) для групи Рі), що за умови правильного вибору параметра q забезпечує надійний захист, в тому числі в постквантовій ері. Оптимізовано практичну реалізацію. Використання багатопараметричних груп дозволяє досягати високого рівня безпеки при відносно менших розмірах скінченного поля. Як зазначено в аналізі, для 128-бітного рівня безпеки система на групі автоморфізмів Сузукі вимагає ключів меншого розміру порівняно з класичною MST3, що знижує вимоги до пам'яті та обчислювальних ресурсів. Створено фундамент для постквантової криптографії. Розроблені криптосистеми базуються на задачі WP у групах автоморфізмів, для яких невідомі ефективні квантові алгоритми. Це, в поєднанні з доведеною стійкістю до класичних атак, робить їх надійними кандидатами для подальших досліджень та можливої стандартизації у якості PQC-протоколів.

Запропонований у дослідженні підхід до розробки схем направленого шифрування на групах автоморфізмів функціональних полів максимальних кривих відкриває новий шлях у розвитку криптографії на основі некомутативних груп. Виходом за межі обчислень у центрі групи вдалося не лише значно збільшити пропускну здатність шифрування, але й, після низки удосконалень, побудувати криптосистеми з високим рівнем безпеки, стійкі до відомих атак. Ключовими досягненнями є розробка методів зв'язування ключів та застосування гомоморфного шифрування, що робить запропоновані схеми надійними кандидатами для епохи постквантової криптографії. Найбільш перспективною платформою виявилися групи Рі завдяки їхній чотирипараметричній структурі та значно більшому, у порівнянні з класичними групами, порядку.

Напрямом подальших досліджень може стати аналіз інших родин некомутативних груп, зокрема узагальнених 2-груп Сузукі, які також є багатопараметричними і можуть мати довільно великий порядок, що потенційно відкриває нові можливості для побудови ще більш ефективних та безпечних криптосистем. Інтерес представляють також дослідження інших груп, таких як групи Григорчука, та інші, які можуть відповідати більшим вимогам з огляду на криптографічну стійкість. Цікавим напрямом є розробка нових задач, які не зводяться до CSP або DP і можуть бути стійкішими до відомих атак. Відкритим залишається питання напрямів удосконалення протоколів та розвиток підходів, що максимально використовують складність усієї групи, а не її окремих частин. В дослідженні представлено нові методи, зокрема зв'язування ключів та гомоморфне перетворення, які є важливим кроком у пошуку перспективних напрямів удосконалення. Іноваційним підходом може бути створення гібрід-

них схем за рахунок комбінування властивостей групової криптографії з іншими постквантовими підходами для створення систем, безпека яких базується на складності задач різної природи.

Криптографія на основі некомутативних груп залишається багатою та глибокою галуззю, що пропонує унікальний підхід до побудови безпечних систем в епоху квантових комп'ютерів. Хоча шлях до практичного застосування та стандартизації виявився складнішим, ніж очікувалося, проведене дослідження демонструє невичерпний потенціал групової криптографії з використанням логарифмічних підписів.

Список літератури:

1. Shor P. W. Algorithms for quantum computation: Discrete logarithms and factoring // Proceedings 35th Annual Symposium on Foundations of Computer Science. 1994. P. 124–134 // IEEE Computer Society Press. https://doi.org/10.1109/SFCS.1994.365700
2. Mosca M., & Piani M. Quantum threat timeline report 2024. Global Risk Institute in Financial Services & evolutionQ. https://globalriskinstitute.org/publication/2024-quantum-threat-timeline-report/
3. National Institute of Standards and Technology. (2016, December). Post-quantum cryptography standardization: Call for proposals / U.S. Department of Commerce. https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/call-for-proposals
4. Khalimov G., Kotukh Y., Kolisnyk M., Khalimova S., & Sievierinov O. LINE: Cryptosystem based on linear equations for logarithmic signatures // Cryptology ePrint Archive. 2024. P. 2024/697. https://eprint.iacr.org/2024/697
5. Kotukh Y., Severinov E., Vlasov O., Tenytska A., & Zarudna E. Some results of development of cryptographic transformations schemes using non-abelian groups // Radiotekhnika. 2021. No 204. P. 66–72.
6. Kotukh Y., & Khalimov G. Hard Problems for Non-abelian Group Cryptography // Fifth International Scientific and Technical Conference" Computer and Information systems and technologies". 2021. https://doi.org/10.30837/csitic52021232176.
7. Anshel I., Anshel M., & Goldfeld D. An algebraic method for public-key cryptography // Mathematical Research Letters. 1999. No 6(3-4). P. 287–291.
8. Myasnikov A. G., & Ushakov A. Random subgroups and analysis of the length-based and quotient attacks // Journal of Mathematical Cryptology. 2008. No 2(1). P. 29–61. https://doi.org/10.1515/JMC.2008.003
9. Kotukh Y., & Khalimov G. Towards practical cryptoanalysis of systems based on word problems and logarithmic signatures // Information security: problems and prospects. 2022. P. 55.
10. Hofheinz D., & Steinwandt R. A practical attack on some braid group based cryptographic primitives // Public Key Cryptography – PKC 2003. P. 187–198. Springer. https://doi.org/10.1007/3-540-36288-6_14
11. Kotov M., & Ushakov A. Analysis of a certain polycyclic-group-based cryptosystem // Journal of Mathematical Cryptology. 2015. No 9(3). P. 161–167. https://doi.org/10.1515/jmc-2015-0013
12. Ruinskiy D., Shamir A., & Tsaban B. Cryptanalysis of group-based key agreement protocols using subgroup distance functions // Public Key Cryptography – PKC 2007. P. 61–75. Springer. https://doi.org/10.1007/978-3-540-71677-8_5
13. Monico C. Cryptanalysis of a matrix-based MOR system // Communications in Algebra. 2016. No 44(1). P. 348–363. https://doi.org/10.1080/00927872.2014.974254
14. Khalimov G., & Kotukh Y. (2025). Cryptographic strengthening of MST3 cryptosystem via automorphism group of Suzuki function fields [2504.07318] Cryptographic Strengthening of MST3 cryptosystem via Automorphism Group of Suzuki Function Fields // arXiv preprint arXiv:2504.07318. https://arxiv.org/abs/2504.07318
15. Khalimov G., & Kotukh Y. (2025). MST3 encryption improvement with three-parameter group of Hermitian function field [2504.15391] MST3 Encryption improvement with three-parameter group of Hermitian function field // arXiv preprint arXiv:2504.15391. https://arxiv.org/abs/2504.15391
16. Khalimov G., & Kotukh Y. (2025). Advanced MST3 encryption scheme based on generalized Suzuki 2-groups [2504.11804] Advanced MST3 Encryption scheme based on generalized Suzuki 2-groups // arXiv preprint arXiv:2504.11804. https://arxiv.org/abs/2504.11804
17. Khalimov G., & Kotukh Y. (2025). Improved MST3 encryption scheme based on small Ree groups [2504.10947] Improved MST3 Encryption scheme based on small Ree groups // arXiv preprint arXiv:2504.10947. https://arxiv.org/abs/2504.10947
18. Khalimov G., Kotukh Y., & Khalimova S. Encryption scheme based on the automorphism group of the Ree function field // IEEE 7th International Conference on Internet of Things: Systems, Management and Security (IOTSMS). 2020. P. 1–8.
19. Khalimov G., Didmanidze I., Sievierinov O., Kotukh Y., & Shonia O. Encryption scheme based on the automorphism group of the Suzuki function field // IEEE International Conference on problems of infocommunications. Science and technology PIC ST2020. 2020. P. 383–387.
20. Khalimov G., Kotukh Y., & Khalimova S. Improved encryption scheme based on the automorphism group of the Ree function field // IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS). 2021.

21.Khalimov G., Kotukh Y., & Khalimova S. MST3 cryptosystem based on the automorphism group of the Hermitian function field // IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T). 2019. P. 865–868.

22.Khalimov G., Kotukh Y., Didmanidze I., Sievierinov O., Khalimova S., & Vlasov A. Towards three-parameter group encryption scheme for MST3 cryptosystem improvement // IEEE Fifth World Conference on Smart Trends in Systems Security and Sustainability (WorldS4). 2021. P. 204–211.

23.Khalimov G., Kotukh Y., Didmanidze I., & Khalimova S. Encryption scheme based on small Ree groups // Proceedings of the 2021 7th International Conference on Computer Technology Applications (ICCTA '21). 2021. P. 33–37.

24.Hart D., Kim D., Micheli G., Pascual-Perez G., Petit C., & Quek Y. A practical cryptanalysis of WalnutDSA™ // Public-Key Cryptography – PKC 2018. P. 381–406. Springer. https://doi.org/10.1007/978-3-319-76578-5_13

25.Котух Є. В., Охріменко Т. О., Дяченко О. Ф., Ротаньова Н. Ю., Козіна Л. С., Зеленський Д. В. Криптоаналіз систем на основі проблеми слова з використанням логарифмічних підписів // Радіотехніка. 2021. Вип. 206. С. 106–114. Режим доступу: http://nbuv.gov.ua/UJRN/rvmnts_2021_206_11

26.Котух Є. В., Сєвєрінов О. В., Власов А. В., Козіна Л. С., Теницька А. О., Зарудна Е. О. Методи побудови та властивості логарифмічних підписів // Радіотехніка. 2021. Вип. 205. С. 94–99. Режим доступу: http://nbuv.gov.ua/UJRN/rvmnts_2021_205_11

27.Kotukh Y., & Khalimov H. Advantages of logarithmic signatures in the implementation of crypto primitives // Challenges and Issues of Modern Science. 2024. №2. P. 296–299.

28.Kotukh E., Severinov O., Vlasov A., Kozina L., Tenytska A., & Zarudna E. Methods of construction and properties of logariphmic signatures // Radiotekhnika. 2021. No 205. P. 94–99.

29.Котух Є., Халімов Г. Оцінки секретності та витрат на реалізацію криптосистеми на основі лінійних рівнянь з використанням логарифмічних підписів // Theoretical and applied cybersecurity. 2024. P. 149.

30.Deligne P., & Lusztig G. Representations of reductive groups over finite fields // Annals of Mathematics. 1976. No 103(1). P. 103–161. https://doi.org/10.2307/1971021

Надійшла до редколегії 26.04.2025

Відомості про авторів:

Котух Євген Володимирович – канд. техн. наук, доцент, професор кафедри кібербезпеки; Національний технічний університет «Дніпровська політехніка»; Дніпро, Україна; e-mail: yevgenkotukh@gmail.com; ORCID: https://orcid.org/0000-0003-4997-620X

Халімов Геннадій Зайдулович – д-р техн. наук, професор, завідувач кафедри безпеки інформаційних технологій; Харківський національний університет радіоелектроніки; Харків, Україна; e-mail: hennadii.khalimov@nure.ua; ORCID: https://orcid.org/0000-0002-2054-9186

Джура Ілля Євгенович – студент 4-го курсу, Національний Авіаційний Університет; Київ, Україна; e-mail: illya773823@gmail.com; ORCID: https://orcid.org/0009-0002-5470-4479

INFORMATION TECHNOLOGY
ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

УДК 621.372(075) **DOI:10.30837/rt.2025.2.221.11**

Ю.В. САМОХІН, О.Г АВРУНІН, д-р техн. наук

ІНТЕГРАЦІЯ ХМАРНИХ СЕРВІСІВ ДЛЯ ЗБЕРІГАННЯ ТА ОБРОБКИ КРІОМІКРОСКОПІЧНИХ ЗОБРАЖЕНЬ: ПРАКТИЧНИЙ ДОСВІД ВИКОРИСТАННЯ MINIO ТА CVAT

Вступ

Кріомікроскопічні зображення є важливим ресурсом для сучасних наукових досліджень у галузі біомедицини, клітинної біології та аграрних технологій. Завдяки високій роздільній здатності такі зображення дозволяють детально вивчати морфологію клітин, відстежувати внутрішньоклітинні процеси та виявляти патологічні зміни з високою точністю [1, 2]. Проте обробка подібних даних супроводжується низкою серйозних викликів – від зберігання великих обсягів зображень до забезпечення зручного доступу, організації та підготовки даних до машинного аналізу.

У традиційному підході дослідники змушені витрачати значну кількість часу на ручне сортування та анотування зображень, що може знижувати ефективність наукової роботи та підвищувати ймовірність помилок [3, 4]. Крім того, стандартні файлові сховища погано масштабуються при роботі з тисячами зображень великого розміру, що є особливо актуальним для завдань, пов’язаних з кріомікроскопією.

Інтеграція сучасних цифрових інструментів, таких як хмарне об’єктне сховище MinIO та система анотування зображень CVAT, відкриває нові можливості для побудови зручного, масштабованого й автоматизованого пайплайна обробки кріомікроскопічних зображень [5]. MinIO забезпечує надійне та швидке зберігання даних із можливістю гнучкої організації доступу, тоді як CVAT дозволяє точно розмічати зображення, створюючи навчальні вибірки для нейромережевих моделей і систем комп’ютерного зору.

Практичне об’єднання цих інструментів у межах єдиного робочого процесу дозволяє оптимізувати всі етапи – від зберігання до анотування — що сприяє прискоренню досліджень, покращенню якості розмітки та спрощенню подальшої автоматизованої обробки даних [6]. Такий підхід є особливо актуальним в умовах постійного зростання обсягів візуальної інформації та необхідності швидкої підготовки даних для аналізу з використанням штучного інтелекту.

Архітектура інтеграції MinIO та CVAT для обробки кріомікроскопічних зображень

Розробка ефективної системи обробки та зберігання кріомікроскопічних зображень потребує врахування величезних обсягів даних та високих вимог до швидкості їх обробки. Традиційні підходи до зберігання та обробки зображень часто не відповідають вимогам масштабних проектів, де важливо забезпечити швидкий доступ до даних та точне анотування [7].

Для вирішення цих проблем ми пропонуємо інтеграцію двох ключових інструментів: хмарного сховища MinIO та платформи для анотування CVAT. MinIO забезпечує високу швидкість доступу до даних у хмарі, що дозволяє ефективно масштабувати систему зберігання для великих обсягів зображень [8]. Водночас CVAT є потужним інструментом для створення точних та якісних розміток зображень, що є необхідним для створення навчальних вибірок для нейромереж.

Запропонована модель передбачає використання MinIO для надійного зберігання кріомікроскопічних зображень з можливістю гнучкого доступу для користувачів. CVAT, в свою чергу, дозволяє автоматизувати процес анотації, що є важливим кроком у створенні навчаль-

них даних для подальшого використання в алгоритмах машинного навчання. Це дозволяє значно пришвидшити підготовку даних до аналізу.

Для покращення процесу обробки та зменшення потреби в ручній праці, система також включає інструменти автоматизації анотації. Така організація процесу дозволяє значно скоротити час на підготовку зображень та забезпечити високу точність при розпізнаванні клітинних структур. Завдяки інтеграції обох інструментів, стає можливим створення ефективного і масштабованого рішення для обробки та аналізу зображень.

Таким чином, запропонована інтеграція MinIO і CVAT створює умови для високопродуктивної роботи з великими обсягами кріомікроскопічних зображень. Це рішення не тільки покращує точність обробки, але й значно спрощує процеси анотування та підготовки даних, що в свою чергу, прискорює наукові дослідження в різних галузях [9].

Принципи роботи MinIO та CVAT в інтегрованому рішенні для обробки кріомікроскопічних зображень

MinIO та CVAT – це дві ключові технології, кожна з яких виконує свою роль у створенні ефективної системи для роботи з великими обсягами даних, таких як кріомікроскопічні зображення. Їхнє поєднання дозволяє значно покращити якість і продуктивність обробки зображень, хоча ці інструменти мають різні підходи до зберігання та анотування даних.

MinIO є системою об’єктного зберігання, оптимізованою для роботи з великими даними. Цей інструмент забезпечує надійне та швидке зберігання кріомікроскопічних зображень, що є критично важливим для наукових досліджень, де дані можуть бути об’ємними та високоякісними [10]. Алгоритм роботи MinIO орієнтований на управління об’єктами даних, що дає можливість масштабувати сховище та забезпечувати доступ до даних з різних платформ та пристроїв, що особливо важливо при роботі з великими зображеннями, які потребують постійного доступу і оновлень.

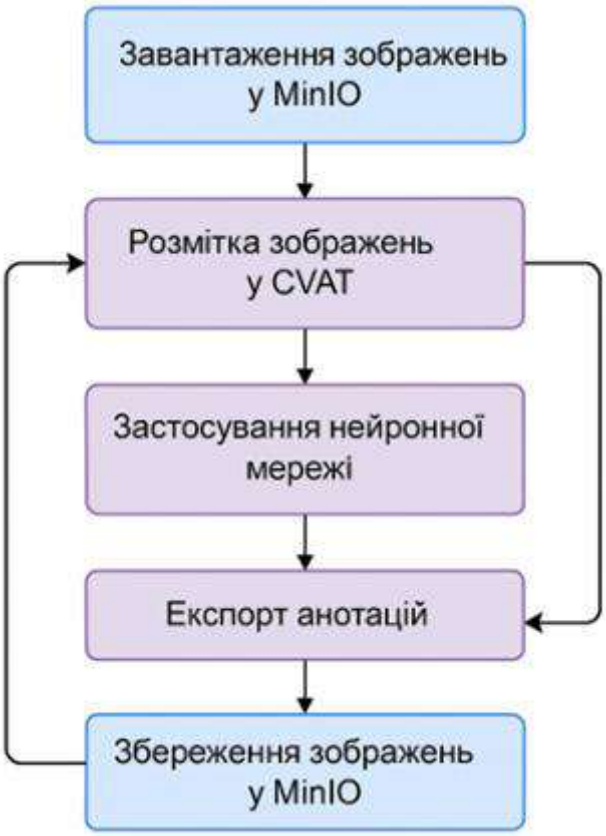

Рис. 1. Етапи роботи системи

Основний етап роботи з MinIO – це завантаження зображень у хмарне сховище, де вони потім стають доступними для обробки. Різноманітність функцій, таких як управління версія-

ми і швидкий доступ до даних, дозволяє інтегрувати MinIO з іншими системами, створюючи гнучке і масштабоване рішення для аналізу зображень.

CVAT, у свою чергу, є платформою для анотування даних, що забезпечує високу точність розмітки зображень[11]. У контексті роботи з кріомікроскопічними зображеннями важливим аспектом є використання автоматичних методів анотації за допомогою нейронних мереж, що пришвидшує процес і підвищує точність розмітки.

Процес роботи з CVAT включає: завантаження зображень, анотування ключових об'єктів на зображенні і використання нейросетевих алгоритмів для автоматизації розмітки. Після анотації дані можна експортувати для подальшого аналізу чи навчання машинних моделей.

Процес анотації в CVAT складається з таких основних етапів:

1. Завантаження зображень у систему.

2. Розмітка та виділення ключових об'єктів на зображенні.

3. Автоматизація розмітки за допомогою нейронних мереж для підвищення швидкості та точності.

4. Збереження та експорт анотованих даних для подальшого використання.

Разом MinIO та CVAT створюють потужну та ефективну систему для обробки кріомікроскопічних зображень. У цьому інтегрованому рішенні MinIO забезпечує високошвидкісне та надійне зберігання даних, тоді як CVAT допомагає швидко та точно анотрувати зображення, що значно пришвидшує підготовку даних для подальшого аналізу.

Таким чином, використання MinIO та CVAT в одній системі дає можливість не лише ефективно керувати даними, а й суттєво підвищити продуктивність та точність обробки кріомікроскопічних зображень, що є важливим кроком у прискоренні наукових досліджень.

Алгоритм виділення клітин на зображеннях за допомогою CVAT

Для виділення клітин на кріомікроскопічних зображеннях у межах даного дослідження використовується інструмент анотування CVAT (Computer Vision Annotation Tool), який забезпечує зручну платформу для ручної та напівавтоматичної розмітки зображень. Метою анотування є створення набору даних, що містить точні контури клітин, які згодом будуть використані для навчання та валідації моделей машинного навчання.

Етапи алгоритму виділення клітин.

Попередня обробка зображень Зображення попередньо нормалізуються та масштабуються до заданого розміру:

$$I_{norm}(x,y) = \frac{I(x,y) - \mu}{\sigma}, \quad (1)$$

де $I\ (x,y)$ – вихідне зображення; μ– середнє значення інтенсивності пікселів; σ– стандартне відхилення.

Далі зображення завантажуються в проєкт CVAT, де створюється задача анотування. Користувач може обрати один із форматів розмітки: полігон, bounding box, точка або трасування контуру.

Для анотування використовується режим полігональної розмітки, за якого користувач вручну окреслює межу кожної клітини на зображенні. Результатом є набір координат вершин полігона:

$$P = \{ (x_1, y_1), (x_2, y_2), \dots, (x_n, y_n)\}, \quad (2)$$

де P – контур однієї клітини; n – кількість точок, що визначають межу.

Отримані полігони перетворюються на бінарні маски:

$$M(x,y) = \begin{cases} 1, \text{якщо } (x,y) \in P \\ 0, \quad \text{інакше} \end{cases}, \quad (3)$$

де $M(x,y)$ – бінарна маска відповідної клітини.

CVAT підтримує експорт анотацій у різних форматах, зокрема COCO, Pascal VOC, YOLO тощо. Для задач сегментації та навчання нейронних мереж найзручнішим є формат COCO, оскільки він містить як координати контурів, так і відповідні категорії.

Обчислення площі клітин Для аналізу анотованих клітин може бути корисним обчислення їхньої площі:

$$A = \frac{1}{2}\left|\sum_{i=1}^{n}(x_i y_{i+1} - x_{i+1} y_i)\right|, \quad (4)$$

де координати $M(x, y)$. Формула базується на методі Гаусса для обчислення площі багатокутника.

Переваги використання CVAT:

- підтримка напівавтоматичного анотування на основі попередньо навчених моделей;
- можливість багатокористувацької роботи та розподілу задач;
- гнучкий експорт та інтеграція з пайплайнами глибокого навчання [12].

Візуалізація та аналіз отриманих даних

У цьому дослідженні реалізовано процес зберігання та анотування кріомікроскопічних зображень із використанням хмарного сховища MinIO та інструменту CVAT для аннотацій. Після завантаження зображень в хмару та їх анотації за допомогою CVAT, дані обробляються для візуалізації анотацій та подальшого аналізу. Це включає такі основні етапи: відображення анотацій на зображеннях, інтеграція з MinIO для зручного централізованого зберігання даних і проведення оцінки якості анотацій.

Після того як зображення анотовано, вони експортуються та обробляються для нанесення контурів клітин. Це дає можливість наочно оцінити точність розмітки, що є важливим, оскільки саме від якості анотацій залежить ефективність подальших кроків, зокрема навчання моделей для сегментації клітин рис. 2.

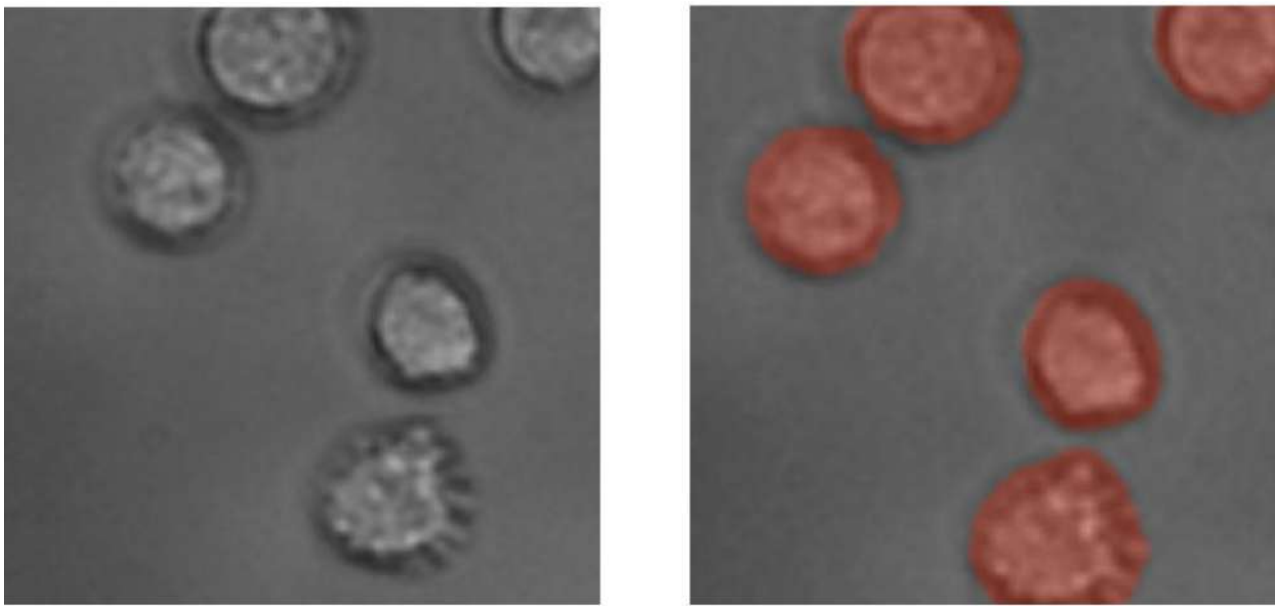

Рис. 2. Приклади нанесення контурів клітин

Всі зображення та їх анотації зберігаються в хмарному сховищі MinIO, яке забезпечує зручний доступ до даних, резервне копіювання, масштабованість і автоматичну синхронізацію при зміні даних. Це дозволяє зберігати всі дані в безпечному та доступному середовищі, що підвищує ефективність роботи з великими наборами зображень.

Для оцінки якості анотацій проводиться аналіз кількості анотованих клітин, щільності об'єктів та їхнього розподілу за розмірами. Такий підхід допомагає виявити можливі перекриття чи скупчення анотацій, що важливо для оптимізації розмітки і покращення якості майбутніх моделей. Під час аналізу було виявлено кілька проблем: дубльовані анотації, низький контраст зображень, що ускладнює точне визначення меж клітин, а також нерівномірний розподіл клітин по датасету. Для вирішення цих проблем пропонується кілька підходів: попередня обробка зображень (покращення контрасту), використання напівавтоматичних моделей для анотацій та введення додаткового етапу валідації даних, що забезпечить більш високу точність та якість розмітки.

У майбутньому планується автоматизація процесу аналізу анотацій шляхом додавання таких можливостей, як обчислення метрик якості розмітки (IoU, precision/recall), побудова теплових карт для візуалізації розподілу клітин і використання інтерактивних дашбордів для візуалізації статистичних даних. Це дозволить значно полегшити процес аналізу, підвищить прозорість роботи з анотаціями та забезпечить кращу відтворюваність результатів, що є важливим для роботи з кріомікроскопічними зображеннями в хмарній інфраструктурі.

Висновки

У рамках дослідження розроблено систему для зберігання та обробки кріомікроскопічних зображень за допомогою хмарного сховища MinIO та інструменту анотування CVAT. Результати роботи продемонстрували ефективність інтеграції цих технологій для вирішення завдань, пов'язаних з аналізом біомедичних зображень.

Інтеграція MinIO та CVAT забезпечила зручний доступ до даних, їх безпеку та масштабованість. Хмарне сховище дозволяє ефективно управляти великими обсягами даних і забезпечує їх доступність для подальшої обробки. Процес анотації за допомогою CVAT показав високу точність у визначенні контурів клітин, що є важливим для створення якісних навчальних даних для моделей сегментації.

Аналіз анотацій виявив кілька проблем, таких як дублювання або низький контраст зображень, але також було запропоновано методи для їх вирішення, зокрема попередню обробку зображень та використання напівавтоматичних методів для підвищення точності. У подальшому планується автоматизація аналізу з додаванням метрик якості анотацій і створення інтерактивних інструментів для візуалізації статистики, що допоможе прискорити процес та підвищити його точність.

Таким чином, розроблена система є ефективним інструментом для обробки кріомікроскопічних зображень, забезпечуючи високу точність анотації, зручне зберігання даних і можливості для подальшого аналізу та навчання моделей машинного навчання.

Список літератури:

1. Самохін Ю. В. Алгоритми проходження контуру на кріомікроскопічних зображень // Радіоелектроніка та молодь у XXI ст. : тези доповідей 27-го Міжнар. молодіж. форуму, 10–12 травня 2023 р. Харків : ХНУРЕ, 2023. Т. 1. С. 99–100.

2. Самохін Ю. В. Алгоритми проходження контуру на кріомікроскопічних зображень // Тематична конференція «Актуальні питання біомедичної інженерії» в рамках 26-го Міжнар. молодіж. форуму «Радіоелектроніка та молодь в XXI ст.». Зб. мат. конф. Т. 1. Харків : ХНУРЕ, 2022. С. 86–87.

3. Самохін Ю. В. Аспекти сегментації кріомікроскопічних зображень // Сучасні технології біомедичної інженерії : мат. II міжнар. наук.-техн. конф. 17−19 травня 2023 р. ; за заг. ред. І. В. Прокоповича, Н. В. Манічевої ; Нац. ун-т «Одеська політехніка». Вінниця : ТОВ «Торговий дім «Альфа і Омега», 2023. С. 110–112.

4. Самохін Ю. В. Виявлення клітин на зображенні за допомогою CVAT AI // Сучасні технології біомедичної інженерії : мат. III міжнар. наук.-техн. конф., 8−10 травня 2024 р. Вінниця : ВНТУ, 2024. С. 24–26.

5. Самохін Ю. В. Знаходження зображень клітин на крімікроскопічних зображеннях за допомогою згорткових нейронних мереж // Сучасний стан та перспективи біомедичної інженерії : мат. міжнар. наук.-практ. конф., присвяченої 125-річному ювілею НТУ України «Київ. політехн. ін-т ім. Ігоря Сікорського», 13–14 грудня 2023 р. Київ : КПІ ім. Ігоря Сікорського, 2023. С. 194–195.

6. Tymkovych M., Avrunin O., Gryshkov O., Semenets V. and Glasmacher B. Ice crystals microscopic images segmentation based on active contours // IEEE 39th International Conference on Electronics and Nanotechnology (ELNANO). 2019. P. 493–496.

7. Tymkovych M., Gryshkov O., Avrunin O., Selivanova K., Nosova Y., Mutsenko V., et al. Application of SOFA framework for physics-based simulation of deformable human anatomy of nasal cavity // IFMBE Proceedings. 2021. Vol. 80. P. 112–120.

8. Tymkovych M., Gryshkov O., Avrunin O., Semenets V. and Glasmacher B. Ice crystals microscopic images segmentation based on active contours // IEEE 39th International Conference on Electronics and Nanotechnology (ELNANO). 2019. P. 493–496.

9. Samokhin Y., Avrunin O. and Yavtushenko V. Cell Detection Model on Cryomicroscopic Images Using MinIO and CVAT // IEEE 17th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET). Lviv, Ukraine. 2024. P. 514–519. doi: 10.1109/TCSET64720.2024.10755563.

10. Tymkovych M., Gryshkov O., Selivanova K., Mutsenko V., Avrunin O. and Glasmacher B. Application of artificial neural networks for analysis of ice recrystallization process for cryopreservation // 8th European Medical and Biological Engineering Conference (EMBEC 2021). Nov. 29 – Dec. 3, 2021. P. 102–111.

11. Gryshkov O. Advances in cryopreservation of alginate-encapsulated stem cells and analysis of cryopreservation outcome / O. Gryshkov, V. Mutsenko, M. Tymkovych, D. Tarusin, V.Sirotinskaya, I. Braslavsky, O. Avrunin, B. Glasmacher // Cryobiology. Vol. 85. P. 156.

12. Prykhodko M.V. Image processing for automated microscopic analysis of ice recrystallization process during isothermal annealing / M.V. Prykhodko, M.Y. Tymkovych, O.G. Avrunin, V.V. Mutsenko, O. Gryshkov, B. Glasmacher // Bioelectromagnetism. 2018. Vol. 20(1). P. 72–75.

Надійшла до редколегії 10.03.2025

Відомості про авторів:

Самохін Юрій Вікторович– Харківський національний університет радіоелектроніки, аспірант кафедри біомедичної інженерії, Україна, e-mail: yurii.samokhin@nure.ua; ORCID: https://orcid.org/0009-0009-5269-3340

Аврунін Олег Григорович – д-р техн. наук, професор, Харківський національний університет радіоелектроніки, завідувач кафедри біомедичної інженерії, Україна, e-mail: oleh.avrunin@nure.ua, ORCID: https://orcid.org/0000-0002-6312-687X

УДК 007.51 **DOI:10.30837/rt.2025.2.221.12**

В.М. КАНЦЕДАЛ, канд. техн. наук, А.А. МОГИЛА, канд. физ.-мат. наук

ОСОБЛИВОСТІ ПОБУДОВИ АЛГОРИТМУ ЦИКЛУ МІЖЕТАПНОГО СИТУАЦІЙНОГО УПРАВЛІННЯ КОНФЛІКТНОЮ ВЗАЄМОДІЄЮ НАЗЕМНОГО КОМПЛЕКСУ РЕП З МАЛИМИ (ЛЕГКИМИ) БЕЗПІЛОТНИКАМИ

Вступ

Існують значні труднощі радіоелектронної протидії на тактичному рівні загрозам розвідувально-ударних малих (легких) БПЛА типу Суперкам або Ланцет [1 – 9] при їх проникненні до важливих об'єктів інфраструктури. Це викликає необхідність підвищення результативності наземних комплексів РЕП, зокрема за рахунок вдосконалення алгоритму циклу міжетапного ситуаційного управління [10]. Головна мета такого управління – нейтралізація загроз різних типів малих (легких) БПЛА літакового виду тактичного рівня важливому об'єкту захисту в різних сценаріях конфлікту з урахуванням специфіки типів і тактик застосування БПЛА, комплексування засобів розвідки і постановки комбінацій різних видів активних завад та їх взаємодії для сигнального і прихованого інформаційного придушення БПЛА.

Аналіз останніх досліджень і публікацій

В статтях [1, 6 – 10, 14] аналізуються різні способи та засоби протидії безпілотникам, що пов’язані з необхідністю побудови спеціалізованого наземного комплексу РЕП безпілотників на тактичному рівні. При цьому враховуються: небезпека створюваних ними загроз для об'єктів інфраструктури; їх малопомітність; низькі висоти та швидкість польоту; маневреність; віддаленість від наземного пункта управління (НПУ) та малий час, відведений на надання радіоелектронної протидії на етапах розвідки БПЛА та придушення його радіоліній.

Протидія БПЛА потребує упорядкування керуючих процесів, що полягає:

- в розподілі їх за етапами розвідки та придушення при функціонуванні комплексу РЕП (види внутрішньо етапного ситуаційного управління, що розглянуті в [10, 14], з визначенням мети кожного етапу, алгоритмів його контурів керування з вибором виконавчих засобів згідно з рівнем невизначеності інформаційного опису динамічного стану конфліктної ситуації, оптимізацією режимів та комплексного їх застосування);

- координації послідовності етапів функціонування наземного комплексу РЕП (міжетапне ситуаційне управління) для: забезпечення цілісності та безперервності (динамізму) управління процесами протидії БПЛА на інтервалі робочого часу комплексу; досягнення узгодженості етапів управління комплексом шляхом встановлення раціональних зв'язків та обміну інформацією між ними для приведення їх у відповідність із Головною метою управління; інтеграції засобів розвідки та придушення всередині етапів та між ними.

В статті [11] з посиланнями на ряд інших робіт розглядається підхід до постановки задачі координації в технологічних комплексах безперервного типу (ТК), до яких відноситься наземний комплекс РЕП. Такі комплекси відрізняються з точки зору задач управління багатовимірністю, наявністю окремих етапів функціонування, ієрархією етапів та складними зв`язками між етапами. Їх тактико-технічні характеристики (ТТХ) в цілому залежать від ТТХ окремих етапів та від взаємних зв`язків між етапами. Це приводить до необхідності розробки задачі координації роботи на керованих етапах функціонування комплексу. Розв’язанням задачі координації є визначення взаємодії етапів, при яких управління, оптимальне за критеріями ефективності кожного з етапів, є також оптимальним за загальним критерієм для ТК в цілому. Для постановки та вирішення задачі координації необхідно ТК, що досліджується, представити у вигляді пов’язаних між собою окремих етапів його функціонування. Для розв’язання задачі координації складних ТК виникає задача оцінки їх стану, що викликано

неперервною зміною як зовнішнього середовища, так і параметрів об’єкта управління – ТК. Таким чином, об’єкти керування є динамічними, для опису їх стану використовуються динамічні моделі. Методи аналізу динаміки складних динамічних об’єктів включають: детерміновані, статистичні, ймовірнісні, логічні, нечіткі та нейромережеві моделі. Для розпізнавання станів складного динамічного об’єкта керування в умовах неповноти інформації, її невизначеності, нечіткості потрібне отримання та обробка зовнішніх знань з використанням комбінованих методів їх отримання від експертів, з проблемно-орієнтованих текстів природною мовою та баз даних. Основні принципи координації – це взаємозв'язок, ієрархічна підпорядкованість, узгодження, єдність команд і дій, загальна ціль.

Як було згадано вище, вирішення завдань координації часто пов'язано з неможливістю передбачення перешкод, з ризиком, невизначеністю і неточністю інформації. Відомо, що у цьому випадку для пошуку рішення доцільно використовувати нечіткі методи аналізу, які слід адаптувати до системи управління з неповною інформацією та високою складністю у вигляді побудови сучасної технології управління із застосуванням інтегрованих нечітких штучних нейронних мереж [12]. Тобто, використання систем з нечіткою логікою поряд з класичними логіко-оптимальними методами керування, що досить ефективно працюють при повністю детермінованому об'єкті управління і середовищі, потребує використання нечітких змінних.

Виділені частини вирішення загальної проблеми щодо ТК треба адаптувати до наземного комплексу РЕП з метою підвищення його результативності протидії малій безпілотній авіаційній системі (БАС) при захисті важливого інфраструктурного об'єкта.

Для побудови методики оцінки результативності такого комплексу слід враховувати [13]:

– відсутність на теперішній час визначених критеріїв для оцінки завадозахищеності ліній радіозв'язку різних типів;

– відсутність у лініях зв'язку ефективних засобів захисту від ретрансляційних завад;

– обмеження комплексу РЕП частотним ресурсом та діапазонами частот РЕП, які енергетично доступні для його сучасних засобів радіотехнічної (РТР), радіоелектронної (РЕР) розвідки та РЕП;

– відсутність у складі комплексу РЕП ефективних технічних та програмно-апаратних засобів, які вирішували б завдання своєчасного та достовірного виявлення ліній зв'язку, які подавлені завадами з визначенням їх характеру впливу та вразливості.

Аналіз відомих публікацій показав відсутність публікацій, присвячених циклу міжетапного ситуаційного управління процесами радіоелектронної протидії різним типам БПЛА тактичного рівня при зміні етапів функціонування наземного комплексу РЕП.

Мета статті: обґрунтувати і виділити особливості побудови структури алгоритму циклу міжетапного ситуаційного управління наземним комплексом РЕП при сигнальному або прихованому інформаційному придушенні структурних елементів БПЛА літакового типу тактичного рівня з маскуючим і імітуючим ефектами впливу для сценаріїв керованого або автономного польотів БПЛА в умовах дефіциту часу протидії.

Виклад основного матеріалу

Відповідно до обстановки, що змінюється, розглядається спрощена двостороння динамічна модель конфліктної взаємодії складових частин багатофункціональних структур малого БПЛА та одноцільового наземного комплексу РЕП при захисті важливого інфраструктурного об'єкта. Він базується на визначенні об’єкта управління – динамічного стану КС, заздалегідь цілеспрямованих у напрямку Головної мети управління етапів функціонування комплексу РЕП згідно зі сценаріями протидії та алгоритмом міжетапного ситуаційного управління. Опис узгоджено до уразливості БПЛА, що аналізується на інтервалі робочого часу комплексу РЕП для сценаріїв керованого або автономного польотів БПЛА в умовах дефіциту часу протидії БПЛА.

Побудова алгоритму міжетапного ситуаційного управління реалізує *принципи прогнозування взаємодій* у вигляді попередньо заданих етапів**,** *узгодження взаємодій цих етапів та оцінки їх взаємодій*, а також *інтелектуалізації* процесів аналізу стану КС та прийняття

рішень за рахунок залучення штучних інтелектуальних ресурсів. Алгоритм повинен відповідати вимогам керованості, результативності, безперервності керування та мінімізації витрат ресурсів комплексу.

Склад многофункціональної структури сучасного одноцільового наземного комплексу РЕП

Склад наземного комплексу РЕП використовує інтегровані методи і засоби виявлення та нейтралізації загроз малих безпілотників, що мають підвищені ТТХ на відповідних етапах функціонування комплексу РЕП [10]. Він включає такі системи:

- засобів розвідки, що складаються з об'єднання маловисотного широкосмугового (ШС) оглядового радіолокатора з пасивними радіочастотними розвідувальними засобами для більш достовірного виявлення малого БПЛА та точного визначення його частотно-структурних сигнатур для його фізичного сигнального або прихованого інформаційного придушення, а також контролю результата придушення;

- засобів спрямованого радіоелектронного сигнального та прихованого інформаційного придушення радіоліній зв'язку з сигналами управління БПЛА і його супутникової навігації;

- автоматизованого управління протидією БПЛА на етапах його функціонування, де приймається велика кількість різноманітних рішень стосовно видів внутрішньо- та міжетапного ситуаційного управління. Вони різняться за змістом, термінами дії та розробленням, спрямованістю впливу, інформаційною забезпеченістю, використанням ресурсів, рівнем прийняття рішень, тощо. У зв’язку з цим виникає необхідність в упорядкуванні рішень міжетапного ситуаційного управління для підвищення керованості та результатив-ності наземного комплексу РЕП при захисті важливого інфраструктурного об’єкту.

Вхідні та вихідні складові інформаційного опису динамічного стану конфліктної ситуації на етапах функціонування наземного комплексу РЕП

Динаміка конфлікту характеризується інформаційним описом змін станів конфліктної ситуації (КС) під зовнішнім впливом та ситуаційного управління на основних етапах функціонування наземного комплексу РЕП. Описи динамічного стану КС, що є узагальненим об'єктом управління в динаміці конфлікту, містять за потреби його етапів вхідні і вихідні складові КС у різні моменти часу на інтервалі робочого часу комплексу. Вони подаються як протистояння критично важливого переліку показників узагальнених ТТХ БПЛА та комплексу з урахуванням особливостей їх побудови та тактик застосування [10]. Цей перелік на окремих етапах функціонування комплексу складається з співвідношення розвідувальної захищеності сигналів радіоліній зв'язку командної радіолінії управління (КРУ) та радіоліній супутникової навігації БПЛА, їх завадо- та імітозахищеності, з одного боку, та показників результативності взаємного застосування наборів засобів розвідки та сигнального і/або прихованого інформаційного придушення, – з іншого боку. До вхідних складових опису стану КС, як інформаційних еквівалентів вразливостей та узагальнених ТТХ БПЛА, належать сигнатури малих БПЛА як об'єктів спостереження засобами РЛР, РТР та РЕР. Це – локаційна сигнатура (ЛОК) з даними його просторово-часового знаходження в зоні відповідальності комплексу РЕП та траєкторних ознак розпізнавання його типу, структурно-частотний портрет загальної електромагнітної обстановки (ЕМО) та структурно-інформаційний портрет сукупності інформаційних повідомлень та протоколів інформаційного обміну (СІППІО) різного ступеня невизначеності, створених сукупністю його ліній радіозв'язку та супутникової радіонавігації. Вихідні складові опису стану КС представлені ймовірностями успішного вирішення завдань етапів функціонування комплексу, наприклад для сценарію керованого польоту БПЛА, у вигляді P_1, P_2, P_3 , P_4 та ймовірності досягнення Головної мети управління – Р.

Оскільки з часом уточнюється знання про загрозу БПЛА та результати радіоелектронної протидії, змінюється склад і зміст стану КС в обмеженнях двосторонньої моделі динамічного конфлікту, що розглядається, то це робить необхідним синтезувати і коригувати закони циклів управління процесами вирішення функціональних завдань на етапах функціонування

комплексу РЕП та координації його дій при зміні етапів. Їх метою є адаптація контурів управління до поточної загрози БПЛА та забезпечення найкращих можливостей її нейтралізації, в тому числі нав’язування БПЛА хибних режимів польоту за допомогою імітаційних завад з вбудованими інформаційно-технологічними впливами (ІТВ).

Етапи функціонування наземного комплексу РЕП

Розглянута спрощена двостороння динамічна модель конфлікту характеризується на інтервалі робочого часу комплексу, починаючи з моменту виявлення БПЛА, застосуванням послідовності заздалегідь цілеспрямованих етапів спільного функціонування засобів розвідки та придушення певних елементів структури БПЛА, що об'єднані Головною метою управління. Виконання вибору локально-оптимальної мети управління та умов узгодження при зміні етапів у відповідності до постановки та пошуку рішення задачі координації, що формалізує процеси міжетапного ситуаційного управління. Виконання цих дій зводиться до розподілу наявних ресурсів комплексу РЕП при мінімізації їх витрат в умовах обмеження тривалості робочого часу, невизначеності та неповноти інформації, необхідної для управління.

Системно-процесний підхід до міжетапного ситуаційного управління дозволяє уявити взаємодію етапів для сценаріїв керованого з НПУ та автономного польотів малого БПЛА.

Для цих сценаріїв нижче наведено перелік можливих етапів паралельно-послідовного функціонування комплексу РЕП та їх приватні мети протидії тактичним БПЛА, що заздалегідь орієнтовані на оперативне та скоординоване досягнення Головної мети управління – нейтралізації їх загроз об’єкту захисту. У ймовірностях успішного вирішення завдань етапів та координації їх змін, що приводяться, відображено спрямованість етапів, цілі і зміст завдань координації, характер взаємозв'язків об'єктів придушення в структурі БПЛА, склад засобів їх розвідки і спрямованого за напрямком придушення комбінаціями різних видів точкових завад з наростаючими маскуючим або/та імітуючим ефектами впливу. Впливи узгоджено з вразливістю лінії зв'язку з командами управління БПЛА і його супутникової радіонавігації.

Послідовність з чотирьох основних етапів функціонування наземного комплексу РЕП включає:

етап 1 – пошук, виявлення та визначення параметрів відбитих і випромінюваних БПЛА сигналів, ситуаційного управління засобами розвідки для формування інформаційного опису ситуаційної обізнаності в зоні спостереження через інформаційний опис вхідних і вихідних складових динамічного стану КС з відображенням сукупних вразливостей окремих ліній радіозв'язку та навігації, а також формування даних, необхідних для управління засобами розвідки та придушення на етапах;

етапи ситуаційного управління фізичним сигнальним (2, 3) та прихованим інформаційним (4) видами придушення БПЛА приймачів радіоліній зв'язку управління БПЛА та його супутникової навігації. Види придушення реалізуються, відповідно, шляхом задіяння різних типів засобів розвідки для уточнення даних управління, генерації та постановки комбінацій різних видів загороджувальних за частотою і часом активних завад, імітаційних видів завад або сигналоподібних завад з вбудованими в них інформаційно-технологічними впливами (ІТВ).

Етап 1 пошуку, виявлення та визначення сигнатур малого БПЛА, формування даних, необхідних для ситуаційної обізнаності та управління засобами різних видів розвідки та придушення

Пошук та виявлення випромінювань ліній зв'язку КРУ, радіоліній супутникової навігації БПЛА та розвідка їх частотних та структурних параметрів здійснюються протягом усього інтервалу робочого часу комплексу РЕП після пошуку та виявлення БПЛА. Їх результативність визначається малопомітністю БПЛА на фоні відбитків від підстилаючої поверхні для оглядової ШС РЛС, розвідувальною захищеністю радіоліній від засобів РТР і РЕР. Аналіз цих обставин та можливостей засобів радіоелектронного придушення комплексу РЕП дозволяють зробити висновок, що ймовірність розвідки радіоліній по робочому діапазону, потужності

випромінювання та роду зв'язку буде різною - може бути отримана у різні моменти часу, на різних ступенях їх невизначеності та при різних значеннях рубіжів їх розвідки $R_{розв}$. Це призводить до побудови певної стратегії застосування розвідувальних засобів для уточнення даних розвідки та наповнення сигнатур, що використовуються для виявлення радіоліній БПЛА [10]. Крім того, мають місце вимоги до повноти, достовірності, точності і ступеня невизначеності (розкрита, частково розкрита та розкрита-відкрита – q =1,2,3), щоб обґрунтувати вибір для застосування того чи іншого виду сигнального чи прихованого інформаційного придушення цих радіоліній.

Виходячи з того, що ймовірність P_1 успішного застосування засобів оглядової ШС РЛС, РТР та РЕР на етапі 1 є величиною зворотної ефективності застосовуваних методів забезпечення розвідувальної захищеності радіоліній у структурі БПЛА, вона визначається за формулою

$$P_1(t) = [P(t_1)_{\text{ШС РЛС}-\text{ЛОК},q=3} + P(t_2)_{\text{РТР}-\text{ЕМО}-\text{пеленг},q=1,2} + \text{Р}_{\text{РТР}-\text{ЕМО},q=2} P(t_3)_{\text{РЕР}-\text{СІППІО}-\text{РЛ},q=3})](1 - \text{ПР}_{\text{пом навед засобів розвід}}) > [1- (\text{Р}_{\text{розвідзахищ від ШС РЛС}} \text{Р}_{\text{розвідзахищ від РТР}} \text{Р}_{\text{розвідзахищ від РЕР}})], \quad (1)$$

де для розвідки сигнатур ЕМО, СІППІО БПЛА використовуються, відповідно: $\text{Р}_{\text{ШС РЛС-ЛОК, q=3}}$, $\text{Р}_{\text{РТР-ЕМО, q=2}}$, $\text{Р}_{\text{РЕР-СІППІО-РЛ, q=3}}$ – ймовірності формування вхідних складових інформаційного опису КС, n =7 – кількість радіоліній, q = 1,2,3 – ступені невизначеності умов спостереження. Розвідувальна інформація з часом накопичується, уточнюється та передається на поточний етап придушення.

При цьому з деталізацією функціональних завдань засобів розвідки:

$$P_{\text{ШС РЛС}-\text{ЛОК},q=3} = [P_{\text{виявл}} P_{\text{розпізн}}(1 - P_{\text{пом супр}})(1 - P_{\text{скр}})(1 - P_{\text{а}}P_f P_t P_{\text{корр}})] \quad (2)$$

де ймовірності: $\text{Р}_{\text{виявл}}$ – виявлення БПЛА; $\text{Р}_{\text{розпізн}}$ – розпізнавання класу/типу БПЛА; $\text{Р}_{\text{пом супр}}$ – помилки супроводу ШС РЛС, $\text{Р}_{\text{скр}}$ – добуток ймовірностей енергетичної та структурної скритності зондуючого сигналу ШС РЛС; $\text{Р}_{\text{а}}$ – селекції за напрямом та поляризації, яка проводиться в антенно-фідерному пристрої (АФП) та системі управління ДНА; Р_{f} – частотної селекції у частотно-виборчих засобах приймача; Р_{t} – часової селекції (що забезпечує виділення сприятливих ділянок часу для прийому корисного сигналу, наприклад при супроводі цілі); $\text{Р}_{\text{корр}}$ – статистичної селекції у кореляційному приймачі.

$\text{Р}_{\text{РТР – ЕМО-пеленг, q=2 –}}$ ймовірність визначення пеленгу джерела випромінювання засобами РТР:

$$P_{\text{РТР}-\text{ЕМО}-\text{пеленг},q=2} = P_{\text{ЧХ}} P_{\text{структура сигн}} \left(1 - P_{\text{скр від РТР}}\right)\left(1 - P_{\text{а}}P_f P_t\right), \quad (3)$$

де ймовірності: $\text{Р}_{\text{ЧХ}}$ – виявлення та вимірювання частотних параметрів випромінювання радіолінії; $\text{Р}_{\text{структура сигн}}$ – розтину структури сигналу радіолінії; $\text{Р}_{\text{скр від РТР}}$ – скритності від засобів РТР; (1- $\text{Р}_{\text{а}}$, Р_{f}, Р_{t}) – помилок наведення засобів РТР на джерело випромінювання.

$\text{Р}_{\text{РЕР-СІППІО-РЛ, q=3 –}}$ ймовірність визначення засобами РЕР даних радіолінії для її інформаційного придушення:

$$P_{\text{РЕР}-\text{СІППІО}-\text{РЛ},q=3} = P_{\text{вмявл ІП}} P_{\text{шифр ІП}} P_{\text{ПІО}} P_{\text{шрозвізн РЛ}}, \quad (4)$$

де ймовірності: $\text{Р}_{\text{виявл ІП}}$ – виявлення шифрованого сигналу радіолінії з інформаційним повідомленням (ІП); $\text{Р}_{\text{шифр ІП}}$ – розкриття структури інформаційнмх повідомлень (ІП); $\text{Р}_{\text{ПІО}}$ – розкриття структури протоколу інформаційного обміну (ПІО); $\text{Р}_{\text{розпізнРЛ}}$ – розпізнавання належності виявленої радіолінії.

Порядок взаємодії етапу 1 із етапами придушення елементів структури БПЛА залежить від таких факторів впливу, як:

- пріоритетність розвідки тієї чи іншої радіолінії з урахуванням розміщення її приймальних та обробних пристроїв у структурі безпілотної авіаційної системи (БАС);

- можливості структури наземного комплексу РЕП для максимально комплексного застосування засобів розвідки та придушення як роздільно, так і сумісно, починаючи з радіогоризонту у міру надходження та накопичення розвідувальної інформації;

- потреби виконання завдань координації у вертикальних послідовностях етапів того або іншого об'єкта придушення та горизонтальної координації етапів придушення для різних об'єктів придушення у структурі БПЛА;

- отримання розвідданих щодо початку (їх рубіжів розвідки) і закінчення етапів придушення цих об’єктів у складі БПЛА (їх рубежів придушення) здійснюється у різні моменти часу. Це призводить до:

- динамічних умов спостереження та придушення радіоліній зв’язку КРУ з сигналом управління та супутникової навігації БПЛА, що ускладнює вирішення завдань синхронізації та горизонтальної координації процесів придушення та їх проміжних результатів на етапах. Виникає потреба оцінки рубіжів початку і закінченні етапів придушення цих об’єктів у складі БПЛА на інтервалі робочого часу комплексу, а також в використання оглядової ШС РЛС для фіксації цих моментів часу, а не тільки для контролю змін траєкторії польоту БПЛА у разі його придушення. Це зумовлено відмінностями кожної радіолінії у властивостях розвідувальної захищеності їх параметрів сигналів та/ інформаційних повідомлень, що передаються, а також їх завадо та імітозахищеностей;

- урахування специфіки побудови, ТТХ типу малого (легкого) БПЛА і тактики його застосування, геометрії конфліктної взаємодії складових частин БПЛА та комплексу РЕП, співвідношень просторових та поляризаційних характеристик ДН антен, що застосовуються, енергетичних, частотних, часових, параметрів структурно-сигнальних форм корисних сигналів ліній зв'язку КРУ, радіоліній супутникової навігації БПЛА та засобів РТР, РЕР або засобів постановки різних видів навмисних завад, що застосовуються.

Перелік формування наступних етапів придушення структурних елементів БПЛА для сценарія керованого польоту БПЛА та приклади даних для формалізації цілей їх протидії

До них відносяться етапи сигнального (2, 3) та прихованого інформаційного пригнічення (4) на рубіжах R (керований політ, лінії зв'язку КРУ та радіонавігації у складі БПЛА, завади з маскуючим та імітуючим ефектами впливу), на підставі результатів розвідки оглядової ШС РЛС, засобів РТР і РЕР – інформаційних даних про сигнали радіоліній БАС, геометрію взаємного розташування БПЛА, засобів розвідки та придушення комплексу РЕП.

На інтервалі робочого часу комплексу розглядається заздалегідь скоординована послідовність етапів, виходячи з розвідувальної захищеності радіоліній БПЛА, їх уразливості та можливостей комплексу РЕП створити у міру надходження розвідувальної інформації наростаючі за результативністю завадові впливи на них, щоб гарантовано досягти Головної мети управління. Конфліктні ситуації характеризуються ступенем визначеності вхідних складових динамічного стану КС та виразами для ймовірностей успішного придушення об'єктів придушення у структурі БПЛА змішаними варіантами прицільного за напрямом застосування наступних засобів постановки комбінацій:

видів потужних загороджувальних завад на етапі 2 при досягненні БПЛА радіогоризонту для наземних засобів їх постановки та у разі неповноті інформаційних даних для прицільного до структури сигналу придушення:

- приймачів сигналів радіоліній супутникової навігації;

- приймача радіолінії зв'язку із сигналами управління БПЛА;

$$P_{2.1\ (\text{звгородж},q=1)} = \left(P_{\text{ШС РЛС},q=3} + \text{Р}_{\text{РТР}-\text{пеленг},q=1,2}\right)\text{Р}_{\text{придуш ЕМО},q=1,\text{загородж}}$$

$$(1 - \text{ПР}_{\text{пом навед завад, m}}) = \left(P_{\text{ШС РЛС},q=3} + \text{Р}_{\text{РТР}-\text{пелен},q=1,2}\right)\text{ПР}_{\text{придуш БРЛА}-\text{ЕМО}-\text{РЛ},q=1,n=5,\text{загородж}}$$

$$(1 - \text{ПР}_{\text{пом навед завад, m}}) > [1\text{- }(\text{Р}_{\text{розвідзахищ БПЛА – ЛОК}}\ \text{Р}_{\text{розвідзахищ БПЛА – РЛ, n=5, загородж.}})] \quad (5)$$

Зазначимо, що використання гіпотетичних інформаційних даних про частотні діапазони радіоліній змушують постановку завад з розширенням смуги спектра завад і розподілом їх потужності за спектром частот і часом в широких інтервалах, що скорочує дальність дії завад та зменшує результативність використовуваних засобів пригнічення;

видів малопотужних імітаційних завад на етапі 3 одночасно з постановкою потужних видів загороджувальних завад:

- приймачам сигналів радіоліній супутникової навігації;
- приймачу радіолінії зв'язку із сигналами управління БПЛА;

$$P_{2.2} = \left(P_{\text{ШС РЛС},q=3} + \text{Р}_{\text{РТР}-\text{пеленг},q=2}\right)[(\text{Р}_{\text{придуш БПЛА}-\text{ЕМО},q=2,\text{іміт}} + \text{Р}_{\text{придуш БПЛА}-\text{ЕМО},q=1,\text{загодж}})$$
$$(1 - \text{ПР}_{\text{пом навед завад, m}})] = \left(P_{\text{ШС РЛС},q=3} + \text{Р}_{\text{РТР}-\text{пелен},q=,2}\right)[(\text{ПР}_{\text{придуш БПЛА}-\text{ЕМО}-\text{РЛ},q=2,n=5,\text{іміт}}$$
$$+ \text{ПР}_{\text{придуш БПЛА}-\text{ЕМО}-\text{РЛ},q=2,n=5,\text{загородж}})(1 - \text{П Р}_{\text{пом навед завад, m}})] >$$
$$[1- (\text{ Р}_{\text{розвідзахищ БПЛА – ЛОК}}\ \text{Р}_{\text{розвідзахищ БПЛА – РЛ, q=2, n=5, іміт.}})]. \quad (6)$$

Вплив малопотужних імітаційних видів завад призводить до зривів синхронізації приймачів сигналів, внесення неправдивої інформації та інформаційного перевантаження процедур обробки прийнятої інформації. Через те, що частотно-структурні параметри сигналів об'єктів придушення у складі БПЛА з часом стають відомими, можливо більш прицільно за частотою і часом пригнічувати радіолінії комбінаціями загороджувальних видів завад з підвищенням їх спектральної щільності потужності.

Повинна виконуватися вимога контролю результативності придушення завадозахищених радіоліній комбінаціями імітаційних і загороджувальних видів завад на етапі 3, що відображається у виразі (3) і служить початком наступного більш результативного етапу 4 функціонування засобів придушення комплексу РЕП;

видів малопотужних завад прихованого інформаційного придушення (імітаційними з вбудованими інформаційно-технологічними впливами) на етапі 4 одночасно з імітаційними та загороджувальними видами завад для:

- приймачів сигналів радіоліній супутникової навігації;
- приймача радіолінії зв'язку із сигналами управління БПЛА;

$$P_{2.3} = \left(P_{\text{ШС РЛС},q=3} + \text{Р}_{\text{РТР}-\text{ЕМО}-\text{пеленг},q=2}\ \text{Р}_{\text{РЕР}-\text{СІППІО}-\text{РЛ},q=3}\right)[(\text{Р}_{\text{придуш БПЛА}-\text{ЕМО}-\text{РЛ},q=2,\text{іміт.}}$$
$$\text{Р}_{\text{придуш БПЛА}-\text{СІППІО}-\text{РЛ},q=3,\text{інф.}} + \text{Р}_{\text{придуш БПЛА}-\text{ЕМО},q=2,\text{іміт.}} + \text{Р}_{\text{придуш БПЛА}-\text{ЕМО},q=1,\text{загородж}})$$
$$(1 - \text{ПР}_{\text{пом навед завад, m}})] = (P_{\text{ШС РЛС},q=3} + \text{Р}_{\text{РТР}-\text{ЕМО}-\text{пеленг},q=2}\ \text{Р}_{\text{РЕР}-\text{СІППІО}-\text{РЛ},q=3})$$
$$[(\text{ПР}_{\text{придуш БПЛА}-\text{ЕМО}-\text{РЛ},q=2,n=5,\text{іміт}}\text{П} + \text{ПР}_{\text{придуш БПЛА}-\text{ЕМО}-\text{РЛ},q=2,n=5,\text{іміт.}}$$
$$+ \text{ПР}_{\text{придуш БПЛА}-\text{ЕМО}-\text{РЛ},q=2,n=5,\text{загородж.}})$$
$$(1 - \text{ПР}_{\text{пом навед завад, m}})] >$$
$$[1- (\text{Р}_{\text{завадозахищ БПЛА – ЛОК}}\ \text{Р}_{\text{завадозахищ БПЛА – РЛ, q=2, n=5, іміт.}}\ \text{Р}_{\text{імітозахищ БПЛА – РЛ, q=2, n=5, інф.}})]. \quad (7)$$

Права сторона нерівностей (1) – (7) характеризує вимоги подолання ймовірнісних показників стійкості радіоліній БПЛА на етапах, що обчислюються відповідно до відомих методик їх розрахунку [13, 15].

Кожен етап з наведеної послідовності етапів може змінити за даними засобів розвідки БПЛА, що супроводжується, його траєкторію в процесі сигнального або прихованого інформаційного придушення (якщо розпізнавати і не враховувати маневр БПЛА). Відсутність даних для управління БПЛА після придушення радіоліній зв'язку та супутникової навігації може спричинити перехід БПЛА в автономний режим. І тому виконується перевірка закінчення циклу міжетапного управління при керованому польоті БПЛА з контролем оглядовою ШС РЛС зміни його траєкторії з фіксацією моменту часу придушення або переходу в автономний режим.

Перелік формування наступних етапів придушення структурних елементів БПЛА для сценарія автономного польоту БПЛА та приклади даних для формалізації цілей їх протидії

Автономний політ малого (легкого) БПЛА виконується за підтримки бортової інерціальної навігаційної системи з можливістю разових коригувань траєкторії польоту за сигналами супутникової радіонавігації для підвищення точності його наведення, а також з виконанням

певних завдань управління польотом в бортовому пристрої керування з використанням відео інформації та штучного інтелекту у вигляді нейромережі. Тобто, на етапі 5 доцільно розглядати з урахуванням етапу 1 змішаний варіант прицільного за напрямом застосування наступних засобів постановки комбінацій:

видів малопотужних завад прихованого інформаційного придушення (імітаційними з вбудованими інформаційно-технологічними впливами) одночасно з потужними загороджувальними видами завад для приймачів сигналів радіоліній супутникової навігації;

- видів протидії штучній нейромережі в бортовому пристрої керування;

$$P_{3,1} = \left(P_{\text{ШС РЛС},q=3} + \text{Р}_{\text{РТР−ЕМО−пеленг},q=2}\ \text{Р}_{\text{РЕР−СІППІО−РЛ},q=3}\right)$$

$$[(\text{Р}_{\text{придуш БПЛА−ЕМО},q=2,\text{іміт.}}\ \text{Р}_{\text{придуш БПЛА−СІППІО−РЛ},q=3,\text{інф.}} + \text{Р}_{\text{придуш БПЛА−ЕМО},q=2,\text{іміт.}} + \text{Р}_{\text{придуш БПЛА−ЕМО},q=1,\text{загородж}})(1 - \text{ПР}_{\text{пом навед завад, m}})]$$

$$=(P_{\text{ШС РЛС},q=3} + \text{Р}_{\text{РТР−ЕМО−пеленг},q=2}\ \text{Р}_{\text{РЕР−СІППІО−РЛ},q=3})$$

$$[(\text{ПР}_{\text{придуш БПЛА−ЕМО−РЛ},q=2,n=4,\text{іміт}}\text{Р}_{\text{придуш БПЛА−СІППІО−РЛ},q=3,n=5,\text{інф.}} + \text{ПР}_{\text{придуш БПЛА−ЕМО−РЛ},q=2,n=4,\text{іміт}} + \text{ПР}_{\text{придуш БПЛА−ЕМО−РЛ},q=2,n=4,\text{загородж.}})$$

$$(1 - \text{ПР}_{\text{пом навед завад, m}})] + \text{Р}_{\text{придуш БПЛА−ШІ}} > [1-$$

$$(\text{Р}_{\text{завадозахищ БПЛА – ЛОК}}\ \text{Р}_{\text{завадозахищ БПЛА – РЛ, q=2, n=4, іміт.}}\ \text{Р}_{\text{імітозахищ БПЛА – РЛ, q=2, n=4, інф.}}\ \text{Р}_{\text{стійкість ШІ}})], \quad (8)$$

де ймовірності: $\text{Р}_{\text{стікість ШИ}}$ – стійкості ШІ в бортовому пристрої керування БПЛА, $\text{Р}_{\text{придуш ШІ}}$ – придушення ШІ.

Виділення ще одного об’єкта придушення у складі БПЛА пов'язане із застосуванням в структурі БПЛА штучного інтелекту (ШІ) у вигляді машинно-навченої («натренованої») нечіткої штучної нейромережі. Ця нейромережа може гнучко та швидко адаптувати до змін обстановки, що складається, його алгоритми пошуку об’єкта захисту, виявлення і розпізнавання за відео інформацією, наведення на нього і контролю розвідки або враження.

До протидії інтелектуальним БПЛА належать:

1) засоби протидії застосування імітаційних видів точкових завад:

- шифрування навігаційних сигналів, щоб не дати комплексу РЕП увійти в «натренеровану» нейромережу з заміною сигналу управління БПЛА;

- використання додаткових засобів для розпізнавання результату впливу імітації або заміни сигналу управління;

- врахування обмежень, що вносяться впливом засобу завадозахисту радіоліній супутникової навігації типу «Комета – М» на можливість заміни даних навігації (створення хибних супутників або спуфінгу);

- ускладнення загороджувальними завадами розпізнавання об'єкта захисту за рахунок підвищенням відношення сигнал/завада;

2) введення ШІ в оману шляхом:

- заміни зображення області поверхні, що спостерігає БПЛА;

- непомітної заміни матриці терезів вже налаштованої нейромережі помилковою матрицею;

- зробити об'єкт захисту нерозпізнаним засобами маскування, наприклад використанням імітаторів об’єкта захисту або спотворенням його зображення внесенням яскравих обманок, які перехоплюють увагу та ускладнюють розпізнавання образу об’єкта захисту (підміна характерних базових компонентів образу об'єкта розпізнавання, наприклад застосуванням мультиспектральних аерозолей з високими маскувальними властивостями для придушення сигнатур зображень об’єкта захисту та місцевості його розташування);

Отримані інформаційні дані про траєкторію польоту БПЛА, що супроводжується, доцільно передавати в якості цілевказівки безпілотникам – мисливцям за малими БПЛА та зенітно-артилерійськими засобами ближньої дії.

Таким чином, показано особливості інформаційного опису динамічного стану КС та керування цим станом та послідовності етапів вирішення конфлікту на користь комплексу РЕП. Інформаційний опис складових поточного стану КС у вигляді наведених сигнатур БПЛА залежить від ступенів їх невизначеності, потреб етапів функціонування комплексу РЕП, а також від певних ймовірностей P_j етапів комплексу РЕП та їх співвідношення на окремих етапах.

Інформаційний опис та особливості алгоритму цикла міжетапного ситуаційного управління

Координація являє собою процес розподілу діяльності складових частин контуру міжетапного ситуаційного управління на інтервалі робочого часу наземного комплексу РЕП, забезпечення взаємодії різних його частин в інтересах виконання завдань, що стоять перед ним, призначення нового функціонування шляхом забезпечення умов узгодженості та інтеграції етапів функціонування комплексу, збереження при цьому результативності, підтримки стійкості та вдосконалення режимів його роботи.

Об'єктом координації можуть бути процеси і результати цих процесів. Контур міжетапного ситуаційного управління включає інформаційні, управляючі та виконавчі засоби.

Призначення алгоритму циклу міжетапного ситуаційного управління: розв'язання завдань координації цілепокладанням, ціледосягненням і контролем формування та реалізації етапів функціонування комплексу РЕП через зіставлення цілей, ресурсів засобів розвідки та придушення, способів їх застосування, взаємного їх пристосування до об'єктів придушення БПЛА для досягнення Головної мети управління комплексу РЕП. Найбільш суттєві завдання координації:

- створення умов узгодження етапів при їх зміні через оцінку результативності рішення функціональних завдань внутрішньо- та міжетапного ситуаційного управління, синхронізації процесів інтеграції та її результатів на етапах з урахуванням гнучкої та швидкої перебудови структури комплексу відповідно до керуючих рішень координації;
- комплексування та інтеграція засобів розвідки та придушення всередині етапів та між ними;
- забезпечення безперервності управління поточним контролем умов спостереження та результатів управління для коригування цілей наступної зміни етапів.

Шуканий алгоритм повинен відповідно до його призначення забезпечити рішення задач координації в сценаріях керованого або автономного польоту тактичного БПЛА в умовах кількох об'єктів розвідки та придушення у складі БПЛА, різноманіття засобів розвідки та управління, етапів функціонування комплексу, станів конфліктної ситуації на етапах, цілей, умов спостереження, придушення та прийняття керуючих рішень при зміні етапів, а також подолання труднощів через відмінності часових характеристик етапів пригнічення окремих об’єктів придушення.

Перелік цілей циклу міжетапного ситуаційного управління та порядок управління ними визначається, як показано вище, зростаючою пріоритетністю значимості взаємодії засобів розвідки та придушення у структурі етапів функціонування комплексу РЕП у міру зниження ступеня невизначеності інформаційного опису стану КС, покращення виконання умов узгодження та синхронізації зміни етапів, вибором більш ефективних засобів розвідки та постановки видів завад об'єктам придушення з потребою контролю результативності дій щодо наближення до Головної мети управління. Алгоритм базується на застосуванні сучасних знань відносно вирішення конфліктних ситуацій методами управління з інформуванням про обмеження ресурсів і орієнтовний час їх виконання та використанням можливостей інформаційних технологій.

В залежності від конфліктної ситуації, проміжних і кінцевого результатів алгоритм циклу міжетапного ситуаційного управління повинен постійно коригувати технологію застосування методів та засобів розвідки та придушення на етапах функціонування комплексу РЕП і при їх змінах. Ця робота повинна базуватись на аналізі поточної інформації, її уточненні, визначенні проблем щодо коригуючих рішень, створення інформаційної бази даних про випадки станів КС і способи їх вирішення в тому чи іншому сценарії протидії певному типу БПЛА.

Успіх алгоритму міжетапного управління у здійсненні координації взаємодії етапів функціонування наземного комплексу РЕП у конфліктних ситуаціях можна оцінити по відношенню показників прийняття і реалізації керуючих рішень на окремих етапах функціонування комплексу [10] до Головної мети алгоритму (близькості та швидкості наближення) при мінімізації ресурсних витрат та в умовах невизначеності або неповноти інформації, дефіциту часу для всебічного аналізу обстановки у зоні відповідальності комплексу РЕП.

Особливості формализации міжетапного ситуаційного управління полягають у виділенні та аналізі впливів загальних та відмінних чинників його процесів. До загальних чинників, що суттєво впливають на побудову алгоритму та його результативність, відносяться:

- склад і багатофункціональна побудова комплексу РЕП, що реалізує базові принципи вирішення проблемних завдань, які розглядаються на основних його етапах роботи, узгоджено до уразливості технічних зразків малого БПЛА;

- цикли внутрішньо етапного ситуаційного управлення [10], що є основною складовою побудови алгоритму міжетапного ситуаційного управління;

- подання конфліктних ситуацій на етапах функціонування комплексу РЕП як протидії ймовірнісних показників їх узагальнених ТТХ (ймовірностей розвідувальної захищеності, завадо- та імітозахищеності об’єктів розвідки та придушення, що має відношення до малопомітності БПЛА, сигналів його КРУ, радіонавігації та переданих інформаційних повідомлень ймовірностям їх подолання – Pj, j= 1, 2,3,…) з урахуванням впливу особливостей побудови малого (легкого) БПЛА і комплексу РЕП та тактик їх застосування;

- застосування системно-процесного, когнітивного підходу до ситуаційного управління, орієнтованого на інформаційний опис стану КС в межах двосторонньої моделі конфлікту, що розглядається, та застосування рефлексивної і адаптивної форм управління, що спирається на високий рівень професійних компетенцій та креативно-рефлексивні здібності суб'єктів управління (операторів), а також використання у структурі інформаційних та керуючих засобів контуру управління можливостей інформаційних технологій, засобів штучного інтелекту та автоматизації;

- використання методичних переваг постановки та пошуку способів вирішення завдань координації на етапах функціонування наземного комплексу РЕП із застосуванням показників критично важливого переліку узагальнених ТТХ БПЛА та комплексу РЕП в умовах невизначеності стану конфліктних ситуацій та обмежень на витрати ресурсу, а також поточного контролю порівняння фактичних результатів вирішення завдань координації із цільовими;

- вибір напряму радіоелектронної протидії (частини структури комплексу) залежно від сценарію конфлікту між БПЛА та комплексом РЕП;

- створення умов для результативного функціонування засобів розвідки, придушення та їх адаптації до зміни цих умов, координація їх взаємозв'язку.

Відмінні чинники процесів міжетапного ситуаційного паралельно-послідовного управління від локально-оптимізаційних завдань ситуаційного управління на етапах функціонування наземного комплексу РЕП [14, 17, 18] полягають:

- у кількості вертикальних послідовностей етапів (об’єктів придушення, що одночасно пригнічуються), комбінацій видів завад з імітуючим характером впливів, особливостях окремих етапів та труднощах горизонтальної координації етапів через часову розбіжність вертикальних послідовностей етапів;

- забезпеченні безперервності (динамізму) управління, яке досягається на основі поточного контролю порівняння фактичних результатів управління, умов узгодження з

цільовими та використання певної форми зворотного зв'язку для зміни етапів; застосуванні правила закінчення циклу управління при зміні етапів функціонування комплексу, вжитті заходів для усунення відхилень та запобігання їх виникненню в майбутньому; реалізації певних кроків алгоритму.

Виділено за цілепокладанням наданих завдань координації наступні кроки алгоритму, орієнтованого більш на сценарій керованого польоту БПЛА. При цьому алгоритм використовує показники, що наведені у виразах (1) – (8).

К р о к 1 . Досягнення цілепокладання на етапі пошуку, виявлення та визначення сигнатур БПЛА, формування даних, необхідних для ситуаційної обізнаності та управління засобами різних видів розвідки та придушення. Розвідувальна інформація з часом накопичується, уточнюється та передається на поточний етап придушення:

$$P_1 \to P_{1\,max}\,,\ \mathrm{R}_1 \to \min,\ \mathrm{P}_1 \to \mathrm{P}_j \text{ за умови } [(\mathrm{T}_{\text{робоче}} - (\mathrm{T}_1 + \sum \mathrm{T}_{j+1}))] \to \min,\ j=2,3 \qquad (9)$$

Особливості координації на етапі стосуються черговості розкриття структури та параметрів радіоліній в послідовності об’єктів придушення з погляду розвідзахищеності радіоліній (зв'язку – відеоінформації, ТМІ, супутникової навігації та радіолінії зв'язку з сигналами управління БПЛА), а також забезпечення вимог до повноти, достовірності, точності і ступеня невизначеності інформації (q).

К р о к 2 . Досягнення цілей перевірки умов узгодження зміни етапів.

Це вимагає когнітивного аналізу динамічного стану поточної КС і контролю його змін, відповідності стану КС потребам наступного етапу і упорядкованості етапів протидії та здатності алгоритму циклу міжетапного ситуаційного управління протидією малому БПЛА вирішити задачу координації, а також комплексування процесів управління взаємодією засобів розвідки, придушення та їх проміжних результатів.

З'ясовуються причини відхилення від очікуваних показників результативності етапів функціонування засобів розвідки та придушення. Труднощі виконання умов узгодження можуть виникнути через відмінності цілей, способів та термінів виконання видів усередині етапного управління:

- неузгодженість умов спостереження та прийняття рішень при зміні етапів (коли введені дані одного етапу у вигляді результатів засобів розвідки та придушення є виходом іншого), відмінності термінів виконання функціональних завдань усередині етапного управління ведуть до порушення цілісності процесу управління;
- виконання процедур контролю через нерівні проміжки часу може викликати проблеми синхронізації та інтеграції;
- незадовільне перетворення результатів аналізу відхилень від необхідних цілей внаслідок недостатнього рівня знань або недостатнього контролю;
- обмеженість системи управління, що викликана нестачею визначальних її ресурсів;
- урахування впливу як змін внутрішнього середовища, так і зовнішньої (що також порушує стійкість управління).

Усунення зазначених відхилень від очікуваних показників умов узгодженості зміни етапів функціонування засобів розвідки і придушення пов'язано з визначенням складу можливих додаткових дій, потрібного складу ресурсів і порядку їх виконання на етапах функціонування.

К р о к 3 . Досягнення цілей взаємного застосування засобів розвідки та придушення на етапах та при їх зміні.

Постановка завдань управління та пошук рішень здійснюється при взаємодії характеру розвідданих етапу 1 та впливів різних видів завад поточного етапу придушення за виразом

$$\mathrm{Q}_{jin}|\mathrm{S}^{M} - \mathrm{S}^{\Phi}|_{jin} \to \text{extr}, \left(\mathrm{P}_{j+1}/\mathrm{P}_j\right) > 1, P_j \to P_{j\,max}\,,\ \mathrm{j} = 2,3,\dots,\mathrm{R}_j \to \min, \mathrm{T}_j \le \mathrm{T}_{j-\text{ДОП}}$$

$$\text{Перевірка: } \left(P_{j\,max} - P_j\right) < \Delta P_{j\text{ДОП}}, \left(\mathrm{T}_{\text{робоче}} - \sum \mathrm{T}_j\right) > 0,\ j = 2,3,\dots \qquad (10)$$

та факту зміни траєкторії польоту БПЛА за даними його супроводу оглядовою ШС РЛС.

Якщо відхилення допустимі, то остання версія рішення не коригується і цикл управління продовжується.

К р о к 4 . Дія алгоритму завершується після досягнення Головної мети P, зафіксованої в циклі міжетапного управління, або значення

$$\left(P - P_j\right) < \Delta P_{j\text{ДОП}}\left(\mathrm{T}_{\text{робоче}} - \sum \mathrm{T}_j\right)) = 0, \mathrm{j} = 2,3, \ldots \quad (11)$$

а також факту зміни траєкторії польоту БПЛА за даними його супроводу ШС РЛС [18, 19].

Тут: $\Delta \mathrm{P}_{\text{доп}}$ – допустима міра зближення; $\mathrm{T}_{\text{робітне}}$ – тривалість інтервалу робітного часу комплексу; $\mathrm{T_j}$ – тривалість операцій на j-му етапі; Q_{jin} – складний критерій якості зміни цілей та умов узгодження при переході на наступний етап з урахуванням його характеристик та особливостей – вирази (5) – (8). Критерій відображає результативність як зіставлення очікуваних значень ймовірнісних показників загальних ТТХ БПЛА і комплексу РЕП, якостей переліку умов узгодження між етапами, що змінюються, та фактично отриманих; j – порядковий номер наступного етапу функціонування комплексу РЕП; i – вхідні та вихідні складові інформаційного опису стану КС і q – ступінь невизначеності умов спостереження та прийняття рішень на j-му етапі, n – той чи інший об’єкт розвідки та придушення); $|\mathrm{S}^{M} - \mathrm{S}^{\Phi}|$ – різниця між очікуваним і фактичним показниками якості інформаційного опису складових поточного стану КС, результативності задіяних засобів розвідки чи придушення на етапі та якостей умов узгодження між змінними етапами, досягнутих на даний момент часу внаслідок реалізації синтезованого закону управління перебудовою структури комплексу РЕП, а також контролю умов спостереження та результату управління із зазначенням кількісних характеристик ступеня досягнення мети управління; R_j – вектор, що характеризує види витрат ресурсів, що є у розпорядженні комплексу РЕП на даний момент часу; $\mathrm{T}_{j-\text{ДОП}}$ – допустимий час синтезу та реалізації закону управління та координації дій при зміні етапів.

Маємо відмінність постановки задач внутрішньо етапного управління [10], що полягає у підтримці динамізму управління та перевірці умов переходу на наступний етап функціонування або умов закінчення циклу управління. Вона стосується контролю на поточному j-му етапі проміжних результатів та факту досягнення Головної мети управління на інтервалі робочого часу $\mathrm{T}_{\text{робоче}}$ комплексу РЕП або вичерпання його часу.

На рис. 1 надана структурна схема міжетапного ситуаційного управління відповідно до зазначених його кроків, що здійснюється під наглядом суб’єкта управління (операторів відповідних складових систем комплексу РЕП). Структура алгоритму логічно коригується у випадках керованого або автономного польотів БПЛА.

Рішення завдань управління на кожному етапі виробляються з застосуванням у циклі міжетапного ситуаційного управління принципу спільної реалізації функцій: пізнання стану КС, сумісного керування засобами розвідки та придушення з використанням проблемно-орієнтованих сукупності знань, необхідними для досягнення Головної мети управління на етапах 2, 3, … з використанням цілей зміни етапів та умов узгодження, зокрема відповідно до виразів (5) – (11) керованого або автономного польоту БПЛА. При цьому до інформаційних та керуючих засобів контуру ситуаційного міжетапного управління пред'являються *типові вимоги* [17, 18], водночас вимоги до виконавчих засобів суттєво відрізняються. Вони залежать від урахування специфіки побудови, ТТХ типу БПЛА і тактики його застосування, геометрії конфліктної взаємодії складових частин БПЛА та комплексу РЕП, співвідношень просторових та поляризаційних характеристик ДН антен, що застосовуються, енергетичних, частотних, часових, параметрів структурно-сигнальних форм корисних сигналів ліній зв'язку КРУ, радіоліній супутникової навігації БПЛА та засобів РТР, РЕР або засобів постановки різних видів навмисних завад, що застосовуються.

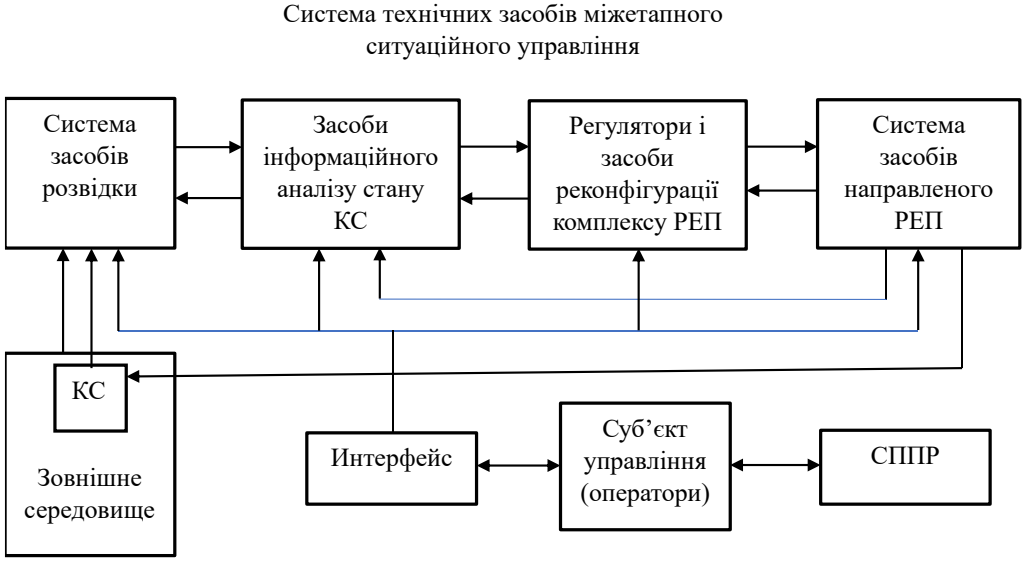

Рис. 1. Структура алгоритму міжетапного ситуаційного управління комплексом РЕП

Шукані матричні рішення керування залежать від *n*-х об'єктів розвідки та придушення, вхідних та вихідних *i*-х складових інформаційного опису стану КС, *q*-х ступенів невизначеності умов спостереження, придушення та прийняття рішень, а також наведених нижче інших вимог до побудови та реалізації алгоритму циклу міжетапного ситуаційного управління.

Керування стосується:

- складу та режимів роботи засобів радіолокаційної, радіотехнічної та радіоелектронної розвідки для виявлення БПЛА, отримання ситуаційної обізнаності, аналізу та прогнозу характеру змін результатів розвідки сигнатур БПЛА, оцінки ступеню його загрози, формування в реальному часі даних, необхідних для цілепокладання та синтезу закону координації інтегрування засобів розвідки та радіоелектронної протидії БПЛА як на етапі, так і при їх зміні;

- вибору комбінацій етапів та відповідних способів придушення, складу і режимів роботи засобів постановки різних видів завад;

- реалізації синтезованих законів координації при створенні умов спільного функціонування засобів розвідки та придушення комплексу, етапів функціонування в різні моменти часу, а також призначення комплексних режимів роботи виконавчих технічних засобів контуру управління, що відбувається за допомогою гнучкої та швидкої перебудови структури комплексу, активації призначених засобів та контролю кількісних характеристик ступеня досягнення якості умов узгодження між змінними етапами та мети управління $|\mathrm{S}^{M} - \mathrm{S}^{\Phi}|_{jin}$ відповідно до прийнятих рішень координації.

Склади комбінацій застосовуваних у різні моменти часу видів завад і рубіжі їх застосування залежать від особливостей конструктивної побудови різних типів тактичного БПЛА, наземного комплексу РЕП, сценаріїв протидії, характеру вразливості розвідувальної, завадота імітозахищеності об'єктів придушення від впливів засобів розвідки комплексу, ступеня невизначеності (q =1,2,3) вхідних і вихідних складових стану КС для комплексного керування взаємодією засобами розвідки і придушення на поточному етапі функціонування комплексу та при їх зміні, а також ступеня небезпеки завадових впливів на об'єкти придушення.

До технологічних особливостей реалізації алгоритму відноситься: застосування різних методів оптимізації; засобів штучного інтелекту у вигляді нечітких штучних нейромереж в структурі інформаційних та керуючих засобів контуру міжетапного ситуаційного управління; системи підтримки прийняття рішень для рефлексивного пізнання динамічного стану конфліктної ситуації в умовах різного ступеню невизначеності, прийняття адаптивних рішень відповідно до змін обстановки; формування баз еталонів опису динамічних станів кон-

фліктних ситуацій на етапах функціонування комплексу та для розпізнавання типів тактичних БПЛА, а також засобів автоматизації вирішення завдань координації і відповідної гнучкої та швидкої перебудови структури комплексу РЕП.

Так, у разі вирішення формалізованих завдань координації застосовуються: логіко-оптимальні; логіко-лінгвістичні, експертні методи, машинно-навчені нейро-нечіткі мережі;

У разі вирішення важко формалізованих завдань координації – інтерпретаційно-дослідний метод з урахуванням впливу фактору суб'єктності управління.

Перспективним є застосування нечітких штучних нейромереж та алгоритмів їх машинного навчання [12], що зумовлено великими обсягами інформаційних даних, що перероблюються у реальному часі, часто змінюваних наборів КС та їх динамічних станів, типів тактичних БПЛА, а також в умовах невизначеності, неповноти інформації та дефіциту часу для протидії. Штучний інтелект як сукупність сучасних інформаційних технологій, що моделюють деякі сторони розумової діяльності людини при розробці та реалізації рішень, значно посилює керованість та результативність виконання завдань координації у складних та змінних умовах, мінімізуючи ризики, що є комбінацією ймовірності певної події та можливих її наслідків. Його спрямованість пов'язана з аналізом ситуаційної обізнаності, розпізнаванням та ідентифікацією типів БПЛА за ознаками їх радіолокаційно-дальнісних, структурно-сигнальних і структурно-інформаційних портретів, підвищенням якості, швидкості вирішення завдань координації, а також адаптувати вибір засобів розвідки та придушення, видів та параметрів завад для зміни стану КС. Штучний інтелект:

- організовує розрахунок та узгодження застосування методів, засобів і часу виконання завдання за обраним варіантом (сценарієм) протидії;
- стежить за узгодженістю виконання завдань алгоритму в контурі міжетапного ситуаційного управління;
- розробляє варіанти коригувань, вибирає найкращий і координує процес виконання завдання для поточної КС та при настанні непередбачених ситуацій, що заважають виконанню завдання;
- вибирає найбільш оптимальний варіант вирішення задачі управління під наглядом суб'єкта управління.

Для зниження рівня суб'єктивності управління та залучення в процеси управління зовнішніх експертних знань і підвищення рівня професійної компетенції операторів комплексу, посилення їх креативно-рефлексивних здібностей, особливо в умовах вирішення завдань координації, що важко формалізуються, також застосовуються системи підтримки прийняття рішень (СППР). Підтримка прийняття рішень має надавати пріоритетний список загроз, який постійно оновлюється в міру зміни конфліктної ситуації, включати доступні виконавчі засоби контуру міжетапного ситуаційного управління та давати рекомендації про те, який засіб розвідки чи придушення використовувати для впливу на складові частини структури виявленого БПЛА певного типу, беручи до уваги їх вразливості та бажаний ефект впливу. Попереднє знання вразливостей типів та ефектів впливу сприяє скороченню часу ухвалення рішень. Слід також враховувати ризик, що вноситься людським фактором при застосуванні виконавчого засобу або їх комплексуванні, щоб мати можливість адаптувати ефект до загрози і поточного стану конфліктної ситуації. Повністю автономне прийняття рішень і втручання операторів можуть розглядатися, коли застосування засобу має низький ризик або рівень загрози високий. СППР повинна зіставляти наявні виконавчі засоби з цілями управління та умовами узгодженості при зміні етапів функціонування комплексу РЕП, мінімізувати ризик помилкових (пропонованих) рішень, скорочувати терміни прийняття рішень, знижувати максимально можливою мірою навантаження на операторів за допомогою засобів інтелектуалізації та автоматизації контуру управління, що розглядається.

Наділення алгоритму циклу міжетапного управління когнітивними властивостями передбачає: отримання в процесі спостереження і придушення знань про КС і результативності окремого та взаємного застосування засобів розвідки і придушення та визначення їх безпосереднього використання; залучення зовнішніх експертних знань у

вигляді експертних підсистем СППР та нечітких штучних нейронних мереж у процеси аналізу та регуляції в умовах невизначеності; можливість динамічно коригувати координацію дій комплексу Рля досягнення наперед поставлених цілей, а також навчатися на основі отриманого досвіду. Інтелектуалізація в алгоритмі процесів аналізу обстановки та вироблення керуючих рішень з необхідними характеристиками в умовах складного конфлікту вимагає розробки алгоритмів машинного навчання засобів штучного інтелекту, які можуть бути предметом подальших досліджень.

До розробки методики оцінки результативності наземного комплексу РЕП

Ефективність алгоритму, що розглядається, характеризується:

- *керованістю* змін стану КС та відповідними рішеннями координації при змінах етапів функціонування комплексу ПЕП, що дозволяють перевести КС в потрібний стан шляхом докладання цілеспрямованого впливу, що керує в мінливій обстановці загроз БПЛА процесами взаємодії складових частин комплексу РЕП і БПЛА, на ці компоненти за кінцевий інтервал часу. Вимоги до керованості алгоритму міжетапного ситуаційного управління відображені у виразах (1) – (8), які використовуються в алгоритмі як системний інструмент формалізації;

- *результативністю* – різницею очікуваного результату та фактичного $|S^{M} - S^{\Phi}|$ щодо багатофакторної зміни динамічного стану об'єкта управління – КС при зміні етапів функціонування наземного комплексу РЕП. Результативність алгоритму полягає в її приростах при кожній зміні етапів через певне поліпшення показників придушення БПЛА, тобто в тому, щоб якомога раніше отримувати локаційні дані відносно БПЛА, первинну інформацію про кожну радіолінію, що бере участь у процесі управління малим БПЛА з моменту його виявлення, і накопичувати інформацію про неї в процесі спостереження на всьому інтервалі робочого часу комплексу. Цього вимагає ситуаційна поінформованість для прийняття правильних управлінських рішень щодо вибору ефективного, динамічного та спільного застосування засобів розвідки та придушення з урахуванням геометрії взаємного розташування БПЛА та засобів розвідки і придушення комплексу поряд з іншими енергетичними, частотними, часовими факторами, характером вразливості радіоліній та нарощування зусиль протидії в різні моменти часу їх застосування залежно від своєчасності надходження та якості поточної розвідувальної інформації про об'єкти придушення в структурі БПЛА;

- *безперервністю керування*, що забезпечується на основі контролю стану КС, вирішення завдань координації при зміні етапів та перевірці умов закінчення циклу міжетапного управління;

- мінімальними *витратами ресурсу* комплексу РЕП.

Поданий опис спрощеної двосторонньої динамічної моделі конфлікту, зокрема алгоритму координації при зміні етапів функціонування комплексу, є основою побудови методики оцінки його вкладу при досягненні Головної мети управління у сценаріях керованого або автономного польоту БПЛА та в умовах дефіциту часу протидії.

Методика оцінки результативності наземного комплексу РЕП складається з набору окремих методик оцінки його результативності на інтервалі робочого часу, що підлягають розробці:

- для окремих етапів при внутрішньо етапному ситуаційному управлінні у представлених послідовностях етапів застосування засобів розвідки та придушення і для певного складу об'єктів придушення у структурі БПЛА;

- накопиченої результативності взаємодії етапів при міжетапному ситуаційному управлінні з наростаючими ефектами їх впливу внаслідок зростаючої взаємодії засобів розвідки та придушення на етапах для певного складу об'єктів придушення у структурі БПЛА. Накопичення переривається на тому чи іншому етапі послідовності досягненням позначеної в алгоритмі міжетапного ситуаційного управління Головної мети управління фактом придушення БПЛА за локаційними даними оглядової ШС РЛС або закінченням тривалості інтервалу робочого часу. При цьому кожна зміна етапів характеризується певним приростом поліпшення показників придушення БПЛА за більш короткий час функціонування і на більшій

відстані від об’єкту захисту при забезпеченні безперервності управління на етапах їх інтеграцією, взаємодією засобів розвідки і спрямованого за напрямком придушення певних структурних елементів БПЛА комбінаціями різних видів завад з наростаючим маскуючим або/та імітуючим ефектами впливу

Оцінка можливості підвищення результативності наземного комплексу РЕП при протидії БПЛА тактичного рівня вимагає комплексного підходу, методично та кількісно пов'язаного з системним та об'єктивним аналізом показників результативності алгоритму циклу міжетапного управління з урахуванням особливостей конструктивно-функціональної побудови типів БПЛА та комплексу РЕП, специфіки та тактик їх застосування для розвідки, завдання ударів по важливих об'єктах інфраструктури та розглянутих можливостей їх захисту наземним комплексом РЕП. Ця оцінка для різних сценаріїв радіоелектронної протидії безпілотникам остаточно визначає потрібну структуру комплексу РЕП з урахуванням складу об'єктів розвідки та придушення в БПЛА, інформаційних, керуючих та виконавчих засобів контуру циклу міжетапного ситуаційного управління та вимог до складу засобів гнучкої та швидкої автоматичної реконфігурації структури комплексу РЕП при реалізації керуючих рішень координації на інтервалі робітного часу комплексу.

Для досягнення потенційних можливостей придушення малих (легких) БПЛА загалом та підвищення живучості наземного комплексу РЕП слід також передбачити його комплексування за даними алгоритму із застосуванням безпілотників – мисливців за малими БПЛА та зенітно-артилерійськими засобами ближньої дії, використовуючи досвід ведення бойових дій.

Разом з тим, розглянутий наземний комплекс РЕП характеризується малою тривалістю інтервалу робочого часу, якого може не вистачити для реалізації розглянутих можливих етапів протидії при керованому польоті БПЛА. Це і залежність засобів виявлення БПЛА від рельєфу земної поверхні та дальності до радіогоризонту, не зважаючи на застосування високих щогл для підняття антен засобів розвідки та придушення, що обмежують функціональні можливості комплексу. Для реалізації потенційних можливостей протидії різним типам тактичних БПЛА при захисті важливого об'єкта інфраструктури потрібно, наприклад:

- модернізувати структуру наземного комплексу РЕП включенням до його складу прив'язного аеростату та розміщенням на його підвісній повітряній платформі певної частини з його конструктивних модулів та додаткових пристроїв для розвідки та впливу на структуру наземного пункту управління БПЛА;

- провести подальше вдосконалення алгоритмів внутрішньо та міжетапного ситуаційного управління у зв'язку з істотним збільшенням інтервалу робочого часу комплексу, розширенням складу функціональних завдань розвідки та придушення всіх структурних елементів малої безпілотної системи, що раніше були не доступні наземному комплексу РЕП.

Висновки

Надано інформаційний опис структури та особливостей побудови алгоритму циклу міжетапного ситуаційного управління наземним комплексом РЕП у рамках спрощеної двосторонньої динамічної моделі конфліктної взаємодії складових частин багатофункціональних структур малого (легкого) БПЛА тактичного рівня та одноцільового наземного комплексу РЕП при захисті важливого інфраструктурного об'єкта для сценаріїв керованого або автономного польотів БПЛА в умовах дефіциту часу протидії.

Алгоритм готує умови узгодження для ефективного вирішення функціональних завдань внутрішньо етапного ситуаційного управління з максимальними значеннями ймовірностей успішного їх вирішення P_j, j=1,2,… на послідовності етапів вирішення конфлікту на користь комплексу РЕП, а також оптимізує вирішення завдань координації взаємодії цих етапів з метою досягнення Головної мети управління – максимуму ймовірності P захисту важливого об'єкта. Це виконується при управлінні динамічним станом конфліктної ситуації на заздалегідь сформованій послідовності цілеспрямованих етапів, узгоджених за цілями, умовами

спостереження та придушення, синхронізованих у часі постановок та розв'язань завдань циклу координації взаємодії етапів функціонування комплексу РЕП при їх зміні через синергію цих процесів і їх результатів та швидку і гнучку реконфігурацію його структури. Показано специфіку критеріїв, постановки та вирішення завдань циклу координації міжетапного ситуаційного управління. Вони засновані на органічному зв'язку радіоліній зв'язку КРУ та супутникової навігації БПЛА з керованими засобами розвідки та засобами придушення їх приймальних пристроїв (об'єктів придушення), а також на залежності координуючих керувань від своєчасності надходження повної, достовірної та точної розвідувальної інформації з урахуванням уразливості об'єктів придушення та упорядкованих певним чином взаємних дій засобів розвідки та придушення при зміні етапів.

Показано особливості інформаційного опису та управління вхідними складовими поточного стану конфліктної ситуації у вигляді наведених сигнатур БПЛА, що залежать від ступенів їх невизначеності, потреб етапів функціонування комплексу РЕП, а також від складу певних ключових загальних ТТХ БПЛА і комплексу РЕП та їх співвідношення на окремих етапах.

Особливості побудови алгоритму криються також у спільному використанні на інтервалі робочого часу комплексу засобів розвідки і засобів придушення для нарощування зусиль за зміни етапів комбінаціями різних видів точкових завад для сигнального і прихованого інформаційного придушення БПЛА у міру накопичення та надходження розвідувальної інформації щодо його сигнатур, а також у технологічних особливостях його реалізації. Останні пов'язані із необхідністю застосування різних методів оптимізації в залежності від ступеня невизначеності умов спостереження та прийняття рішень, засобів штучного інтелекту та автоматизації перебудови структури комплексу РЕП відповідно до потреб координації.

Накопичувальна результативність алгоритму, що розглядається, характеризується її приростами при зміні етапів, що ведуть до певного поліпшення показників придушення БПЛА за більш короткий час функціонування і на більшій відстані від об’єкту захисту при забезпеченні безперервності керування на етапах контролем комплексування та інтеграції засобів розвідки і спрямованого за напрямком придушення певних структурних елементів БПЛА комбінаціями різних видів точкових завад з наростаючим маскуючим або/та імітуючим ефектами впливу.

Наведено обмеження, властиві наземному комплексу РЕП, розуміння яких відкриває шлях до їх подолання. Наприклад, включення до його складу прив'язного аеростату веде до досягнення потенційної результативності протидії різним типам тактичних БПЛА за рахунок суттєвого розширення функціональних можливостей комплексу, збільшення його інтервалу робочого часу, появі нових об'єктів розвідки та придушення в нових умовах протидії, де використовується вся структура малої безпілотної системи, яка раніше була недоступна наземному комплексу РЕП.

Список літератури:

1. Generation of Counter UAS Systems to Defeat of Low Slow and Small (LSS) Air Threats. https://apps.dtic.mil/sti/pdfs/AD1152139.pdf
2. Пєвцов Г.В., Олещук М.М. Аналіз спроможностей оглядових РЛС РТВ щодо виявлення, супроводження та ідентифікації безпілотних літальних апаратів // Системи озброєння і військова техніка. 2021. № 3(67). С. 24–30. https://doi.org/10.30748/soivt.2021.67.03.
3. Миценко І.М., Педенко Ю.О., Роєнко О.М. Про можливість захисту БПЛА від придушення сигналів управління // Радіотехніка. 2024. Вип. 217. С. 133–138.
4. Методичні рекомендації «Щодо радіоелектронної протидії безпілотним літальним апаратам «Ланцет» / Головне управління радіоелектронної та кіберборотьби Генерального штабу Збройних Сил України, Житомир. військ. ін-т ім. С. П. Корольова, 2023. 23 с. https://sprotyvg7.com.ua/wp-content/uploads/2023/03/
5. Sukharevsky O., Orlenko V., Vasylets V., Ryapolov I. Radar scattering char acteristics of a UAV model in X-band // IET Radar, Sonar & Navigation. 2020. Vol. 14. Iss. 4. P. 532–537.
6. Ярош С.П., Гур’єв Д.О. Впровадження специфічних способів і засобів протидії безпілотним літальним апаратам в угрупуванні зенітних ракетних військ // Наука і техніка Повітряних Сил Збройних Сил України, 2022. № 2(47). С. 47–61. DOI: 10.30748/nitps.2022.47.05

7. Лещенко С. П., Адаменко А. А., Лупандін В. А., Мегельбей Г. В. Система інформаційного забезпечення протидії безпілотним літальним апаратам противника при комплексному застосуванні засобів радіоелектронної боротьби // Зб. наук. пр. Харків. нац. ун-ту Повітряних Сил. 2022. № 3 (73). С. 31–37. https://doi.org/10.30748/zhups.2022.73.05.

8. Лупандін В. А., Сотніков О. М., Мегельбей Г. В., Танцюра О. Б. Модель захисту об'єктів і військової техніки від роїв безпілотних літальних апаратів // Системи обробки інформації. 2022. № 4 (171). С. 41–47. ttps://doi.org/10.30748/soi.2022.171.04.

9. Kaidenko M. M., Kravchuk S. O. Protection against the effect of different classes of attacks on UAV control channels // Information and telecommunication sciences. 2022. Vol. 13, №1. P. 35–43.

10. Канцедал В.М. Поліпшення рівня формалізації процесів управління на основних етапах радіоелектронної протидії малій безпілотній авіаційній системі для отримання конфліктних переваг // Радіотехніка. 2024. Вип. 219. С. 68–81. DOI:10.30837/rt.2024.4.219.08

11. Ладанюк А.П., Шумигай Д.А., Бойко Р.О. Системна задача координації в технологічних комплексах неперервного типу. Київ : НУХТ. https://dspace.nuft.edu.ua/server/api/core/bitstreams/3191308c-9d12-4a63-82fe-008604669899/content

12.Сахно Е.В., Мороз Н.В., Пономаренко С.І. Пономаренко. Використання теорії нечіткої логіки при управлінні проєктами // Наук. вісник Полісся. 2021. № 3(15). С. 119–126. https://doi.org/10.25140/2410-9576-2018-3(15)-119-126

13. Заславець В.П., Долина М.П., Чечуй О.В. Особливості розрахунку завадозахищеності ліній радіозв'язку в умовах радіоподавлення (радіоелектронного конфлікту) // Системи озброєння і військова техніка. 2020. № 1(61). С. 7–12. https://doi.org/10.30748/soivt.2020.61.01.

14. Kantsedal V. Features of the formalization of situation management cycles of the ground specialized complex of radio electronic countermeasures for small drones // Book of proceedings of the XX InternationaI Scintific Conference on Electronics and Applied Physics (APHYS 2024). 22–25 October 2024. Kuiv, Ukraine, Taras Shevchenko National University of Kyiv Faculty of Radio Physics, Electronics and Computer Systems. P. 220–221.

15. Канцедал В.М., Могила А.А. Особливості управління завадо захищеністю оглядової РЛС при її придушенні активними завадами та інформаційними впливами, що заважають // Радіотехніка. 2021. Вип. 207. С. 89–101.

16. Kantsedal V., Mogyla A. System advantages and features of the use of stochastic periodic complex pulse radio signals in the sensing modes of a surveillance radar // Book of proceedings of the 19th International Scientific Conference on Electronics and Applied Physics (APHYS 2023). 17–21 October 2023. Kuiv, Ukraine, Taras Shevchenko National University of Kyiv Faculty of Radio Physics, Electronics and Computer Systems. P. 89 –90.

17. Kantsedal V., Mogyla A. A Multifactorial Approach to Building a System for Automated Control of Radar Information Stability // IEEE Ukrainian Microwave Week (MRRS) Kharkov, Ukraine, September 21 – 25, 2020. Vol. 2. P. 373–378. https://drive.google.com/file/d/1rnRSc1SV_I6hJ--uhjkQPhxZ6FDzlLY8/view?usp=sharing (Пароль для распаковки zip-файла сборника трудов совпадает с именем файла – «UkrMW-2020».)

18. Kantsedal V. Rationale for construction of the structure of the system for cognitive control of types of signal resource surveillance radar // Book of proceedings of the 19th International Scientific Conference on Electronics and Applied Physics (APHYS 2023). 17–21 October 2023. Kuiv, Ukraine, Taras Shevchenko National University of Kyiv Faculty of Radio Physics, Electronics and Computer Systems. P. 91–92.

Надійшла до редколегії 11.03.2025

Відомості про авторів:

Канцедал Валерій Михайлович – канд. техн. наук, Інститут радіофізики та електроніки ім. О.Я. Усікова НАН України, старший науковий співробітник; Україна; e-mail: kantsedalvaleri@gmail.com, ORCID: http://orcid.org/0000-0003-4008-917X.

Могила Анатолій Андрійович – канд. фіз.-мат. наук, Інститут радіофізики та електроніки ім. О.Я. Усікова НАН України, завідувач відділу; Україна; e-mail: moganat1196@gmail.com. ORCID: http://orcid.org/0000-0002-1726-6265.

УДК 621.383.5 **DOI:10.30837/rt.2025.2.221.13**

О.Д. МЕНЯЙЛО, канд. техн. наук, О.В. ГРИГОР'ЄВА, В.Г. МАХОНІН

РОЗРОБКА ТА АНАЛІЗ МАТЕМАТИЧНИХ МОДЕЛЕЙ ФОТОЕЛЕКТРИЧНИХ ПЕРЕТВОРЮВАЧІВ СОНЯЧНИХ БАТАРЕЙ СИСТЕМ АВІОНІКИ

Вступ

Одним з основних методів перетворення сонячної енергії в електричну є використання напівпровідникових фотоелектричних перетворювачів. Більшість сучасних модулів сонячних батарей має ефективність менше 20 %, хоча в умовах космічного простору їх ефективність може сягати 80 %. Незважаючи на відносно низьку їх ефективність, в світі спостерігається значний ріст сонячної енергетики.

Для виготовлення наземних фотоелектричних перетворювачів найбільш придатними вважаються напівпровідники Si, GaAs, CdTe. Серед них найбільш розповсюдженим є кремній, що, в основному, обумовлено його низькою вартістю.

Одне з найпростіших конструктивних рішень фотоелектричного перетворювача показано на рис. 1.

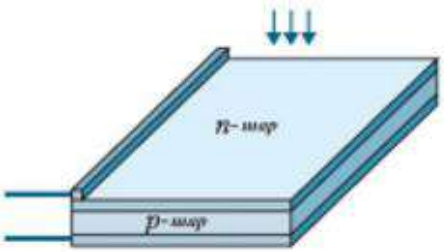

Рис. 1. Спрощена конструкція фотоелектричного перетворювача

Величина електрорушійної сили при освітлені напівпровідникового переходу випромінюванням постійної інтенсивності описується рівнянням вольтамперної характеристики перетворювача:

$$U = \frac{A \cdot k \cdot T}{e} \cdot \ln \frac{I + I_0}{I_0} + I \cdot R_n , \qquad (1)$$

де I – загальний струм; I_0 – фотострум; k – стала Больцмана; T – абсолютна температура; q– заряд електрона.

На рис. 2 показано приклад вольтамперної характеристики типового фотоелемента.

На цьому рисунку: $I_{лз}$ – струм короткого замикання, U_{xx} – напруга холостого ходу, P_{max} точка оптимальної потужності, I_{mp} – струм в точці оптимальної потужності, U_{mp} – напруга в точці оптимальної потужності.

Для визначення точки оптимальної потужності, а значить і оптимального режиму роботи фотоелектричного перетворювача, необхідно знати вольтамперну характеристику. А це, зокрема, можливо шляхом моделювання такої характеристики на основі як певних експериментальних даних, так і аналітичних співвідношень з використанням схеми заміщення фотоелектричного перетворювача.

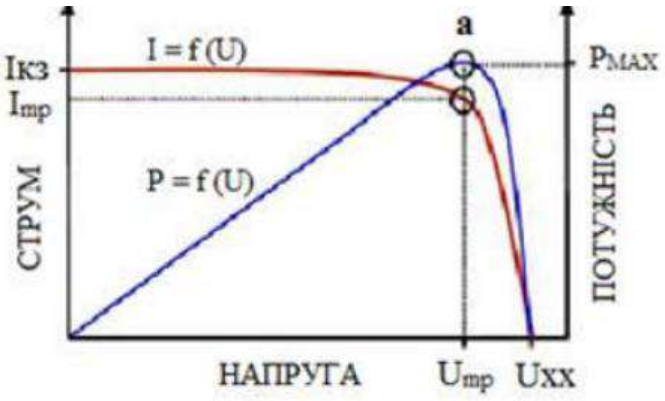

Рис. 2. Вольтамперна характеристика фотоелемента

1. Математичні моделі характеристик та методи визначення параметрів моделей фотоелектричних перетворювачів

У наукових публікаціях [3, 5] в якості основної характеристики фотоелектричних перетворювачів використовується вираз для вольтамперної характеристики, що був отриманий на базі їх схеми заміщення із зосередженими параметрами:

$$I_н = I_ф - I_0 \cdot \left\{ \exp\left[\frac{q \cdot U_н + I_н \cdot R_п}{A \cdot k \cdot T} \right] - 1 \right\} - \frac{U_н + I_н \cdot R_п}{R_ш} . \quad (2)$$

В свою чергу, параметри такої моделі можуть бути представлені функціональними залежностями від основних параметрів, що впливають на роботу перетворювачів, а саме, освітленості E і температури T, які аналітично мають вигляд:

$$\begin{cases} I_н = N_{пит} \cdot S \cdot E \cdot a_1 \cdot \left(1 + a_2 \cdot T\right); \\ I_0 = \exp\left(a_3 \cdot T + a_4\right); \\ R_п = a_5 \cdot \exp\left(a_6 \cdot T\right), \end{cases} \quad (3)$$

де $N_{пит}$ – питома енерговіддача фотоелектричного перетворювача при освітленості E = 1360 Вт / м^2 і температурі T = 40 °C; a_1, a_2, a_3, a_4, a_5, a_6 – емпіричні коефіцієнти; S – площа прийомної поверхні перетворювача.

Параметр A такої моделі, зазвичай, є певною константою, хоча в деяких окремих випадках він може також вважатися залежним від температури. Для інженерної практики модель вольтамперної характеристики доцільно представляти за трьома характерними точками, що можуть буди досить просто знайдені за допомогою нескладних вимірювань. Такими точками є: струм короткого замикання; напруга холостого ходу; струм та напруга в оптимальній точці.

Одною з можливих математичних моделей характеристик перетворювачів може бути модель у вигляді залежності

$$I_н = I_{кз} \cdot \left[1 - \exp\left(f\left(U_н\right)\right)\right], \quad (4)$$

де

$$f\left(U_н\right) = U_н - U_{xx} \cdot \frac{\ln\left(1 - i\right)}{U_{xx}\left(j - 1\right)} . \quad (5)$$

Змінні i та j в цьому виразі визначають відносне положення точки максимальної потужності, а саме:

$$\begin{cases} i = I_{\text{опт}} \big/ I_{\text{кз}}; \\ j = U_{\text{опт}} \big/ U_{\text{хх}}. \end{cases} \tag{6}$$

Подібною аналітичною моделлю може бути, наприклад, співвідношення

$$I_{\text{н}} = I_{\text{кз}} \cdot \left[1 - \frac{U_{\text{н}}}{U_{\text{хх}}} \cdot \exp\left[\frac{U_{\text{н}} - U_{\text{хх}} \cdot j \cdot ln\ 1\text{-}i}{U_{\text{опт}} - U_{\text{хх}}} \right] \right] \tag{7}$$

або аналогічна залежність

$$I_{\text{н}} = I_{\text{кз}} \cdot \left[1 - C_1 \cdot \left[\exp\left(\frac{U_{\text{н}}}{C_2 \cdot U_{\text{хх}}} \right) - 1 \right] \right], \tag{8}$$

де

$$\begin{cases} C_1 = 1 - i \cdot \exp\left[\dfrac{-j}{C_2} \right]; \\ C_2 = \left[\dfrac{j-1}{ln\ 1-i} \right]. \end{cases} \tag{9}$$

Основною проблемою використання моделей (4) – (9) є те, що вони потребують визначення залежностей виду $I_{кз}$, $I_{опт}$, $U_{хх}$, $U_{опт}$ від освітленості та температури.

Для визначення параметрів моделі, тобто відповідних коефіцієнтів, рекомендується наступна послідовність операцій:

l) визначають коефіцієнти a_1 та a_2 за умови

$$I_{\text{ф}} = \eta \cdot S \cdot E \cdot a_1 \cdot \ 1 + a_2 \cdot T \ \approx I_{\text{кз}} \ \ E, T \ . \tag{10}$$

Таке допущення справедливе тому, що в діапазоні температур від 0 до 60 °С і освітленості від 600 до 1500 Вт/м^2 з достатньою для інженерної практики точністю можна вважати, що струм короткого замикання є еквівалентним фотоструму;

2) визначають коефіцієнт A за результатами вимірювання $I_{кз}$ та $U_{хх}$ при постійній температурі і змінних значеннях освітленості, використовуючи рівняння

$$\frac{A \cdot k \cdot T}{q} = \frac{dU_{\text{хх}}}{d\ \ln\ I_{\text{ф}}} \approx \frac{\Delta U_{\text{хх}}}{\Delta\ \ln\ I_{\text{ф}}}, \tag{11}$$

3) проводять оцінку залежності струму насичення, тобто коефіцієнтів a_3 та a_4 у виразі (3), від температури за умови

$$\ln\ I_0 \ = \ln\ I_{\text{ф}} \ - \frac{U_{\text{хх}} \cdot q}{A \cdot k \cdot T}. \tag{12}$$

При визначенні коефіцієнтів A, a_1, a_2, a_3, a_4, доцільно використовувати метод найменших квадратів та експериментальні залежності струму короткого замикання і напруги холостого ходу від освітленості та температури;

4) оцінюють значення параметра схеми заміщення R_n. Відомо кілька варіантів такого визначення. Наприклад, за умови проходження характеристики перетворювача через оптимальну точку його опір можно визначити з наступного співвідношення:

$$R = \frac{U_{\text{опт}} - \frac{A \cdot k \cdot T}{q} \cdot ln\left(\frac{I_{\text{кз}} - I_{\text{опт}}}{I_0} + 1\right)}{I_{\text{опт}}} = \frac{N_{\max}}{I_{\text{опт}}^2} - \frac{U_{\text{хх}}}{ln\ I_{\text{опт}}/I_0} \cdot \frac{ln\left(\frac{I_{\text{кз}} - I_{\text{опт}}}{I_0} + 1\right)}{I_{\text{опт}}} . \quad (13)$$

Для фотоелектричних приладів на основі кристалічного кремнію визначення R_n може базуватисяся на вимірюванні двох вольтамперних характеристик при однаковій температурі, але різних значеннях освітленості та подальшому розрахунку відношення різниць напруг і струмів в області оптимальної точки:

$$R_{\text{п}} = \frac{U\ \ E_2, I_2\ \ - U_{\text{опт}}\ \ E_1}{I_{\text{кз}}\ \ E_1\ \ - I_{\text{кз}}\ \ E_2} . \quad (14)$$

Слід враховувати, що ця формула є справедливою, якщо виконуються наступні умови: величина E_1 є більшою за E_2, а, також, якщо струм в точці $U(E_2, I_2)$ експериментальної характеристики перетворювача

$$I_2 = I_{\text{опт}_{E1}} - \ I_{\text{кз}_{E1}} - I_{\text{кз}_{E2}} . \quad (15)$$

Дійсно, якщо при зміні освітленості змінюється тільки фотострум, а інші параметри схеми заміщення залишаються незмінними, то можна зробити певний висновок про залежність напруги на виході перетворювача від значення величини струму з урахуванням послідовного опору.

2. Результати експериментальних досліджень фотоелектричних перетворювачів сонячних батарей

З практичної точки зору представляє певний сенс питання адекватності математичних моделей експериментальним результатам. Для відповідних досліджень були відібрані фотоелектричні перетворювачі розробника НДТІП (науково-дослідний технологічний інститут приладобудування), місто Харків, та ФП наземного застосування дослідного виробництва ПО «Прапор», місто Полтава.

Про основні властивості застосованих моделей можна судити за наведеними на рис. 3 залежностями, які відображають поведінку моделей з усередненими коефіцієнтами для перетворювачів, виготовлених ПО «Прапор».

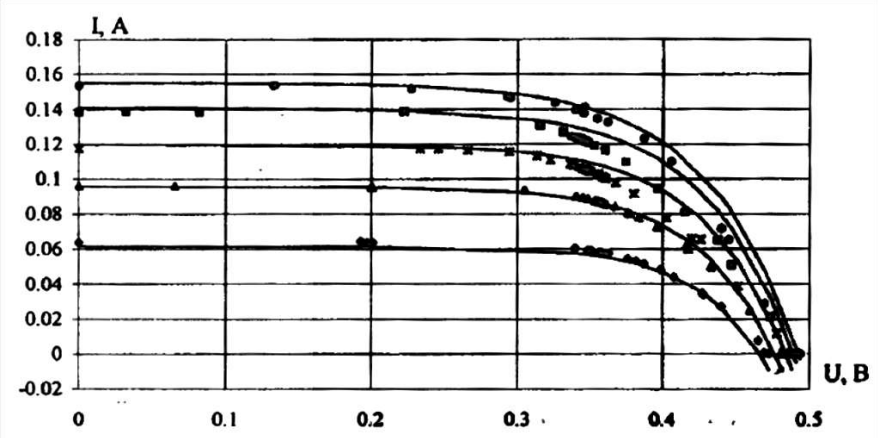

Рис. 3. Експериментальна та розрахункова ВАХ при температурі +60 °С та рівнях освітленості E=1500 Вт / м^2; E=1360 Вт / м^2; E=1160 Вт / м^2; E=925 Вт / м^2; E=600 Вт /м^2

Залежність напруги холостого ходу моделей від температури (рис. 4) добре відповідає експериментальним даним в широкому діапазоні температур від –40 °С до +60 °С.

Подальше зменшення величини U_{xx} зі зниженням температури пов'язане з тим, що в моделі відсутня залежність коефіцієнта A від температури, що зі зниженням температури починає різко зростати.

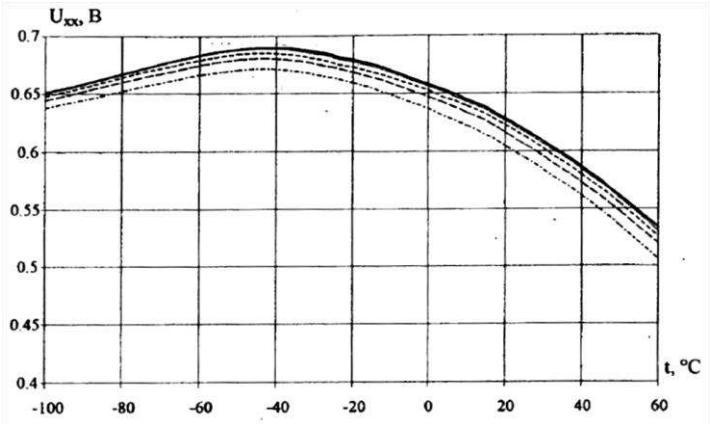

Рис. 4. Залежність напруги холостого ходу перетворювачів від температури

Характер кривих $I_{кз}(T)$ та $R_n(T)$, наведених на рис. 5, 6, дозволяє зробити висновок, що їх залежність від температури з достатньою для практичного застосування точністю відповідає теоретичним даним.

Функціональний зв'язок параметрів i та j від температури не суперечить експериментальним даним аж до –100 °С. Однак їх точність поблизу лівої межі діапазону суттєво зменшується.

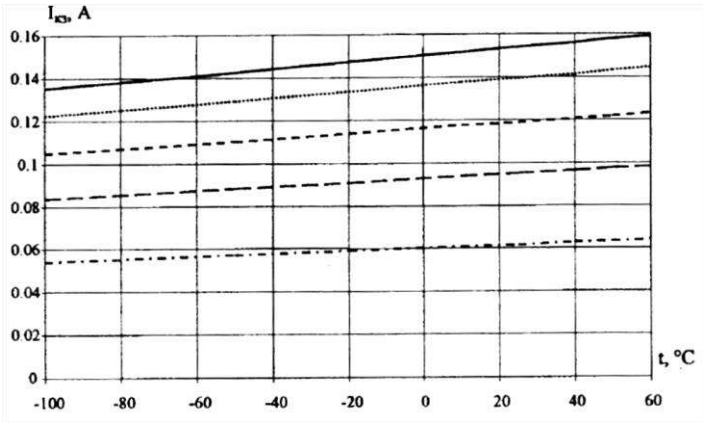

Рис. 5. Залежність $I_{кз}$ від освітленості та температури

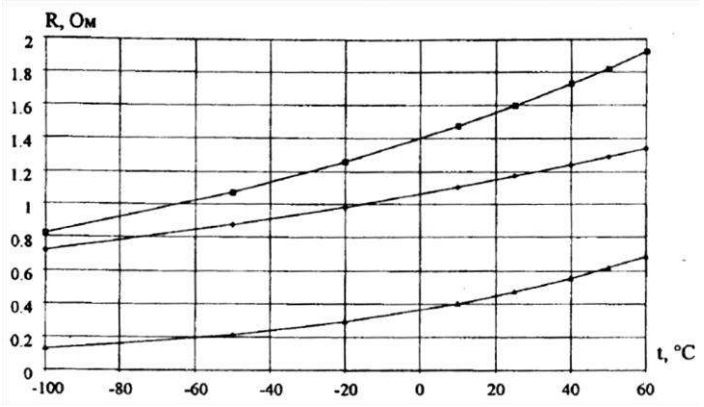

Рис. 6. Залежність величини опору $R_п$ від температури

Висновки

Таким чином, розроблені моделі продемонстрували свою адекватність до температур порядку –50 °С. При необхідності зробити екстраполяцію до більш низьких температур, необхідно вжити спеціальних заходів, з яких найбільш простий в реалізації буде, наприклад, застосування спеціальної лінійної або фрагментарно-лінійної функції, що характеризує залежність коефіцієнта *A* від температури.

Список літератури:

1. Раушенбах Г. Довідник з проєктування сонячних батарей ; пер. с англ. Москва : Енергоатомвид, 1983. 357 с.
2. Бортові енергосистеми космічних апаратів на базі сонячних та хімічних батарей / Н.В. Бєлан, К.В. Безручко, В.Б. Єлісєєв та ін. ; у 2 т. Харків, 1992.
3. Тімашев С.В. Фотоелектричні перетворювачі сонячної енергії : учеб. пособ. / С.В. Тімашев, В.А. Гріліхєс. Москва : Енергія, 1985. 300 с.
4. Бордіна Н. М. Моделювання вольт-амперних характеристик сонячних елементів та сонячних батарей / Н. М. Бордіна, В.О. Лєтін // Електротехнічна промисловість. Сер. Хім. і фіз. джерела струму. 1986. С. 1858–1866.
5. Бузанова Л. К. Напівпроводникові фотоприймачі / Л. К. Бузанова, А. Я. Глібєрман. Москва : Енергія, 1976. 486 с.
6. Glynn, Larry W., McDermoff, Josef K., Oss John P. Saber digital computer simulation of an electrical power subsystem // Proc. 23rd intersoc. Energy Conv. Eng. Conf. August 1988. Vol. 3. P. 543–546.
7. Васильєв В.В. Переходні процеси в ланцюгах із фотоперетворювачами / В. В. Васильєв, В. Р. Заявлін, В. О. Лєтін, Ю. П. Хотунцев. Геліотехніка. 1987. 586 с.
8. Slonim M.A., Tslaf A.L. Experimental investigation of transient phenomena in solar sell panels // Proc. 16th Convention of IEEE in Israel, Tel-Aviv. 1989. P. 1–3.
9 Нєкрасов М.М. Випробовування елементів радіоелектронної апаратури / М. М. Нєкрасов, В. В. Платонов, Л. І. Дадєнко. К. : Вища шк., 1981. 304 с.
10. Oesen D.R., Derg H.M. Properties Die Bond alloys relating to thermal fatigue // IEEE Transact on component, hybrids and manufacturing technology. 1979/
11. Miller P.J. Engineering to counter the EMT theat // Radio and Electron. Eng. 1983. Vol. 53. №11–12. P. 387–392.
12. Gates M.J., Goldhammer L.J. Solar current degradation factors // Proc. 16th Intersoc. Energy conversion Engineering Conf. Technologies for the Transition Atlanta, Ga. 1981. N. Y. 1981.

Надійшла до редколегії 05.03.2025

Відомості про авторів:

Меняйло Олександр Дмитрович – канд. техн. наук, доцент, Харківський національний університет радіоелектроніки, доцент кафедри проєктування та експлуатації електронних апаратів, Україна; e-mail: oleksandr.meniailo@nure.ua; ORCID: https://orcid.org/0000-0002-3760-0523

Григор'єва Ольга Володимирівна – Харківський національний університет радіоелектроніки, старший викладач кафедри проєктування та експлуатації електронних апаратів, Україна; e-mail: olha.hryhorieva@nure.ua; ORCID: https://orcid.org/0000-0002-5759-8897

Махонін Віктор Геннадійович – Харківський національний університет радіоелектроніки, асистент кафедри проєктування та експлуатації електронних апаратів Україна; e-mail: viktor.makhonin@nure.ua; ORCID: https://orcid.org/0009-0003-5608-0513

УДК 621.385 **DOI:10.30837/rt.2025.2.221.14**

І.М. БОНДАРЕНКО, д-р фіз.-мат. наук, О.С. ГНАТЕНКО, канд. фіз.-мат. наук,
О.В. ГРИЦУНОВ, д-р фіз.-мат. наук, О.Г. ПАЩЕНКО, канд. фіз.-мат. наук,
В.П. КАРНАУШЕНКО, М.А. КОПОТЬ

АРХІТЕКТУРА ПРОГРАМНОЇ СИСТЕМИ TULIPGM ДЛЯ ПРОЄКТУВАННЯ ВАКУУМНИХ ПІДСИЛЮВАЧІВ І ГЕНЕРАТОРІВ НВЧ-ДІАПАЗОНУ

Вступ

В наш час різноманітні за класом безпілотні літальні апарати (БПЛА) [1] становлять значну загрозу безпеці суспільства. Заходи протидії їм постійно розроблюються та впроваджуються, але на сьогодні ситуація далека від ідеальної. В той час як великі БПЛА (з розмірами, порівнянними з пілотованими літаками) за принципами їх виявлення і засобами протидії (насамперед, це засоби ППО) непринципово відрізняються від традиційних літальних апаратів, малі БПЛА створюють значні труднощі для протидії їм. Ці БПЛА характеризуються мізерною ефективною площею розсіювання (ЕПР) радіохвиль, в першу чергу через невеликі розміри та широке застосування в їх конструкції пластмас. Вони також мають незначні теплову, акустичну та оптичну сигнатури. Внаслідок невеликої маси їм притаманна висока маневреність, що дає змогу за необхідності виходити з-під прицілу відносно масивної ракети ППО. Одночасна кількість їх у «рої» також може бути доволі значною.

Навіть у разі розв’язання проблеми виявлення, питання ураження чи протидії малим БПЛА стоїть дуже гостро. Вартість зенітної ракети в кілька разів (іноді в десятки разів) перевищує вартість БПЛА, що вражається, а засоби наведення та конструкції підривників не розраховані на відпрацювання малорозмірних і низькошвидкісних цілей. Застосування тактики «рою» (коли об’єкт, що охороняється, або сам комплекс ППО атакують одночасно безліч БПЛА з одного або різних напрямків) призводить до виснаження боєзапасу та прориву принаймні частини БПЛА до об’єкта атаки. Інша проблема – використання низьковисотного профілю польоту: у цьому випадку радіогоризонт визначає дальність виявлення цілі. Як і для будь-якої цілі ППО, для протидії БПЛА потрібно їх виявити та знищити фізично та/або вивести з ладу їхні канали управління, навігації, спостереження чи функціонування [2]. Основними нерадіотехнічними засобами придушення та знищення БПЛА є:

– кінетичне ураження уламками зенітного снаряда чи зенітної ракети;

– перехоплення БПЛА заздалегідь поставленими механічними перепонами (сітками) або дроном-винищувачем;

– пошкодження чи руйнування корпусу інтенсивним лазерним випромінюванням.

До радіотехнічних методів відносяться:

– постановка завіси радіоелектронних завад;

– перевантаження нелінійних електронних кіл постійним мікрохвильовим випромінюванням достатньої потужності;

– невідновне ураження електроніки БПЛА короткими електромагнітними імпульсами потужного НВЧ генератора [3, 4].

Кожен з перелічених методів має свої переваги, недоліки та типову тактику застосування. Радіотехнічні засоби можна класифікувати з точки зору потужності кінцевих каскадів відповідного радіоелектронного обладнання. Для створення завіси радіоелектронних завад ця потужність вимірюється ватами (в безперервному режимі). Для неруйнуючого перевантаження вхідних кіл приймачів БПЛА – кіловатами (також в безперервному режимі). Необоротну деградацію напівпровідникових приладів БПЛА на тактично прийнятній відстані можна викликати лише електромагнітними імпульсами з піковою потужністю порядку мегават і більше. Розвиваючи доробок однієї з відомих наукових шкіл Харкова, подальші зусилля сконцентруємо на дослідженні методів комп’ютерного аналізу, проєктування та оптимізації сучасних НВЧ приладів, призначених для формування саме таких імпульсів.

Огляд сучасного стану наукової проблеми

До найбільш відомих джерел потужного НВЧ випромінювання на сьогодні відносяться [5]:

– підсилювачі та генератори з поздовжньою взаємодією (прилади О-типу): багаторезонаторні пролітні клістрони, лампи біжучої хвилі (ЛБХ) О-типу тощо;

– генератори й підсилювачі зі схрещеними полями (прилади М-типу): магнетрони (в тому числі релятивістські), амплітрони, ЛБХ М-типу та ін.;

– мазери на циклотронному резонансі (ґірорезонансні прилади): ґіротрони.

Наразі, як і раніше, неможливо однозначно віддати перевагу якомусь з зазначених типів приладів з точки зору застосування їх для ураження БПЛА. Ґіротронам та пролітним клістронам властиві найбільші досягнуті на цей час потужності, але їхні конструкції більше орієнтовані на використання в стаціонарних умовах, ніж на базі автомобільного транспорту. ЛБХ О- та М-типів притаманна широкосмуговість, що дає змогу більш гнучко керувати тривалістю та формою робочих імпульсів. Однак потужності цих підсилювачів далеко не максимальні. Нарешті, прилади М-типу не є рекордними, з точки зору жодних електромагнітних параметрів і характеристик, але натомість мають унікальні конструктивні особливості: граничну простоту конструкції, ударо- та вібростійкість, мінімальну масу в поєднанні з порівняно низькими робочими напругами. Це робить магнетронні прилади практично ідеальними для застосування в польових умовах.

В цілому, крім військових використань, існує постійний інтерес до створення потужних, високоефективних джерел мікрохвильового випромінювання, що працюють у гігагерцовому, терагерцовому та субтерагерцовому (аж до інфрачервоного) діапазонах частот [6]. Такі джерела необхідні для низки важливих технічних та наукових застосувань, зокрема:

– нагрівання та діагностики плазми в новому поколінні установок для керованого термоядерного синтезу;

– прискорення елементарних часток;

– терагерцової спектроскопії та магнітометрії;

– експериментальних досліджень та контролю різних середовищ, включаючи біологічні;

– використання потужних імпульсів субтерагерцового випромінювання як ондуляторів для короткохвильових лазерів на вільних електронах. Є також численні застосування потужних НВЧ приладів у фізиці плазми (наприклад, створення інтенсивних джерел ультрафіолетового випромінювання на основі терагерцового розряду), космічному зв’язку тощо.

Існує перспективна ідея повторення вражаючого успіху в покращенні конструкцій ЛБХ та пролітних клістронів у 1970–80-х роках. Тоді вдалося різко підвищити ефективність цих приладів, надавши тим самим перевагу їм над магнетронами. Поздовжня оптимізація процесу взаємодії хвилі з електронним потоком була головним «секретом» такого прогресу.

На відміну від 1970–80-х років, зараз саме комп’ютерні експерименти повинні відігравати ключову роль у подібній оптимізації. Тому потрібні відповідні математичні інструменти, як для електродинамічного («холодного»), так і для електронного («гарячого») моделювання НВЧ приладів. Загалом, під цим розуміються розрахунки довільних нестаціонарних немонохроматичних полів у дисперсійних тривимірних (3D) електродинамічних системах (електродинамічних лініях) без електронних потоків або з ними відповідно (наприклад, періодичних сповільнюючих структурах для ЛБХ, клістронів та приладів М-типу, гладкостінних хвилеводах для пристроїв швидкої хвилі тощо).

Перспективні розробки, розпочаті у 1970-х роки відомою науковою школою Харкова за ініціативи професора О.Г. Шеїна, включали, зокрема, повноформатне та 3D PIC [7] моделювання приладів зі схрещеними полями [8]. В результаті одним з авторів цієї статті був написаний двовимірний (2D) повноформатний нестаціонарний PIC код TULIPgm (TUbe modeLIng Program) [9]. Спочатку він був призначений для моделювання нестаціонарних явищ у підсилювачах зворотної хвилі М-типу з розподіленою емісією та замкнутим електронним потоком (амплітронах). Однак через значні переваги нового на той час повноформатного підходу над

популярним тоді наближенням «рухомого вікна», код розвивався далі. Було додано модель автогенератора зі схрещеними полями (магнетрона), на черзі була реалізація моделей дематрона та ЛББХ М-типу. Можливості, які дає одночасне моделювання всього внутрішнього простору НВЧ приладу, дозволяють аналізувати нові практично значимі явища в НВЧ генераторах та підсилювачах і підвищують точність модельної оцінки їхніх технічних параметрів. За допомогою системи TULIPgm проводилися різноманітні дослідження явищ у схрещених полях, а також розрахунки параметрів і характеристик реальних магнетронних приладів.

Серед цих досліджень можна згадати пошук способів підвищення коефіцієнта підсилення амплітронів з катодним збудженням [10]. Добре відоме тепер вторинно-емісійне групування потоку електронів у схрещених полях поблизу поверхні розподіленого катоду [11] було відкрито в 1984 р. за допомогою вказаного вище коду. На жаль, через низьку роздільну здатність символьних принтерів, спочатку воно помилково інтерпретувалося як зародження солітонів. Пізніше спостерігалися також інші види нестійкості електронної хмари: власні коливання замкнутого потоку, істинні солітони та конвективні явища у втулці та спицях [11]. Досліджено особливості конкуренції нормальних мод сповільнюючої системи в амплітронах і магнетронах. Тривимірне повноформатне моделювання приладів М-типу також було реалізовано, але на той час (1990-ті роки) основні зусилля вже були зосереджені на реалізації в коді TULIPgm так званих спектральних моделей.

Спектральний підхід [12, 13] полягає в урахуванні всіх суттєвих часових гармонік процесу взаємодії полів і часток у частотному континуумі та отриманні в результаті моделювання реальних частотних характеристик приладу. Спектральний метод реалізується непрямим шляхом, тобто, у часовій області. Спектр вхідного сигналу пристрою перетворюється на спектр вихідного сигналу за допомогою двох перетворень Фур'є, розділених нестаціонарним моделюванням поширення негармонійної електромагнітної хвилі через електродинамічну систему з урахуванням нелінійної взаємодії з електронним потоком. Отримані частотні розподіли представляють у графічній формі та відображають на моніторі комп'ютера, як на звичайному аналізаторі спектру.

Метою статті є аналіз архітектури та можливостей спеціалізованої програмної системи (пакета прикладних програм) TULIPgm, призначеної для розрахунків та оптимізації параметрів і характеристик потужних вакуумних НВЧ приладів, що можуть бути використані в системах протидії малим та середнім безпілотним літальним апаратам, а також в інших застосуваннях, де потрібна генерація електромагнітних НВЧ імпульсів великої інтенсивності.

Архітектура програмної системи

Незважаючи на значну кількість наявних спеціалізованих програм, розроблених протягом минулих десятиліть відомими науковими колективами відповідного профілю за замовленнями провідних радіоелектронних, авіакосмічних, військово-морських та інших корпорацій (Raytheon, Northrop Grumman, Lockheed Martin, NRL, MIT тощо), а також більш або менш універсальних комерційних програм, що реалізують так звані «Particle-in-Cell» (PIC) алгоритми [7] (наприклад, Magic, Magic3D, COMSOL Multiphysics тощо), потреба в аналогічних вітчизняних програмних системах залишається актуальною. При цьому серед їхніх найважливіших характеристик слід зазначити конкретні алгоритми, що застосовуються для розрахунку електромагнітних полів в об'ємі НВЧ приладу (алгоритми для моделювання часток розрізняються лише деталями). Методи скінченних різниць та скінченних елементів у часовій області (FDTD та FETD відповідно) [14, 15] є універсальними та найбільш придатними для цієї мети, але вони занадто ресурсоємні, особливо для приладів зі складними внутрішніми границями. Враховуючи, що електронний потік займає лише невелику частину загального внутрішнього об'єму пристрою, у таких випадках може бути ефективним метод розділення змінних (Фур'є). Розділення змінних зменшує обсяг обчислень, оскільки ресурсоємні базові цикли електродинамічного («холодного») моделювання використовуються лише для одно-

прохідного розрахунку власних функцій електродинамічної системи, які потім зберігаються в просторових межах електронного потоку.

На жаль, класичний метод розділення змінних погано адаптовано для відкритих або/та узгоджених електродинамічних систем, оскільки вони мають континуальні спектри власних функцій. Нещодавно запропоновано перспективну модифікацію метода Фур'є, де континуальний набір власних функцій відкритих або узгоджених електродинамічних систем замінюється скінченною дискретною множиною нових просторово локалізованих функцій: так званих парціальних мод електродинамічної системи або осцилетів (oscillets) [16]. Цей підхід також може спростити моделювання НВЧ приладів з нерегулярними вздовж напрямку групової швидкості хвилі сповільнюючими системами. Саме вказані вище перспективні алгоритми реалізовано в програмній системі TULIPgm, яку, таким чином, можна вважати чисельно-аналітичною (на відміну від повністю чисельних універсальних комерційних програм, про які згадувалося вище). Розглянемо спершу особливості її архітектури.

Структура програми. Програмну структуру системи TULIPgm визначено на двох рівнях: логічному та фізичному. Перший описує алгоритми, структури даних і логіку взаємодії частин системи. Фізичний рівень стосується програмної реалізації та подальшого використання логічних частин системи. Логічний рівень поділяється на два підрівні: програмні об'єкти та логічні програмні модулі. Кожен підрівень пов'язано з певним етапом розробки програмного забезпечення.

Програмні об'єкти – це елементи мови програмування, які описують дані (інформаційні об'єкти: змінні, масиви, структури тощо) або процедури (процедурні об'єкти: підпрограми, функції). Вони важливі на етапі структурного проєктування системи. Логічні програмні модулі (ЛПМ) – це сукупності програмних об'єктів, які доцільно програмувати або використовувати спільно. Вони з'являються на етапі реалізації програмного забезпечення.

Повний набір логічних модулів системи TULIPgm розділено на підмножину модулів обслуговування й моніторингу системи (так званий Диспетчер) і кілька підмножин модулів власне моделювання, які називаються Задачами (Problems, українською з великої літери). Кожна Задача призначена для моделювання певного НВЧ приладу (наприклад, магнетрона) або групи з кількох конструктивно подібних приладів.

На фізичному рівні кожен логічний модуль може бути реалізований у кількох варіантах (так звані фізичні програмні модулі, ФПМ). Відмінність варіантів модуля полягає в різній реалізації одних і тих самих програмних об'єктів. Це може стосуватися особливостей приладу (наприклад, прямокутна або циліндрична геометрія), або особливостей моделі (2D або 3D). По суті, зміни варіантів модулів не впливають на логічну структуру системи, оскільки інтерфейси всіх варіантів ФПМ, що реалізують той самий ЛПМ, є аналогічними.

З іншого боку, оскільки надто універсальна логічна структура Задачі може виявитися дуже розгалуженою та заплутаною, замість неї розробляються кілька так званих конфігурацій тієї самої Задачі з різними логічними структурами, які позначаються шістнадцятковими номерами від 00 до FF. Існує кілька моделюючих конфігурацій кожної Задачі (з номерами 00…0F), які реалізують основні алгоритми PIC моделювання НВЧ приладу. Допоміжні конфігурації (10…7F) виконують вторинні розрахункові процедури. Нарешті, сервісні конфігурації (80…FF) реалізують обслуговуючі функції, наприклад, підготовку вхідних даних або діагностику результатів моделювання.

Коли всі фізичні модулі розроблено, необхідно виконати їх компонування та запуск. Залежно від можливостей операційної системи (ОС) розрізняють динамічне та статичне збирання програмної системи. Перше полягає в початковому завантаженні в оперативну пам'ять і виконанні лише ФПМ Диспетчера. ФПМ Задачі вибираються та завантажуються пізніше, засобами Диспетчера. При статичному збиранні фізичні модулі Диспетчера та Задачі завантажуються в оперативну пам'ять лише засобами ОС (одночасно).

Обчислювальний процес. Обчислювальний процес у системі TULIPgm також розглядається на двох рівнях. Логічний рівень описує потік моделювання незалежно від реальних запусків програми на виконання. Фізичний стосується фактичних пусків та зупинок системи. Розділення рівнів забезпечується механізмом контрольних точок (Checkpoints).

З логічної точки зору обчислювальний процес складається із «сесій» (Sessions), які не пов'язані одна з одною даними. Кожна сесія починається з «холодного запуску» системи, під час якого очищуються так звані файли зв'язку завдань (Job link files, JLF). Це відповідає початку моделювання нового приладу. Сесія розділена на «завдання» (Jobs), які пов'язані між собою даними за допомогою JLF. Вхідні та вихідні параметри приладу поступово накопичуються в JLF. Це забезпечує безперервність процесу моделювання. Наприклад, після завдань, які виконують «холодні» обчислення пристрою (визначення напруги Хартрі, узгодження входу і виходу електродинамічної системи [17] тощо), завдання «гарячого» моделювання цього ж приладу можуть виконуватися без повторного введення вхідних параметрів. Якщо має місце динамічне збирання системи, модулі потрібної Задачі завантажуються в ОП під час ініціалізації завдання та вивантажуються з неї після його завершення.

Кожне завдання складається з «задач» (Tasks, українською з малої літери, на відміну від Problems). Їх метою є багаторазове повторення однієї й тієї ж процедури моделювання з різними вхідними даними. Це є основою для подальшого впровадження алгоритмів оптимізації НВЧ приладів. Наразі задачі використовуються лише для повторного моделювання того самого приладу з його «холодного» стану. Задачі поділяються на кроки задачі (Task steps). Завдяки циклічним, в основі, алгоритмам моделювання НВЧ приладів, вони дозволяють керувати основним циклом нестаціонарного або ітераційного розрахунку.

На фізичному рівні обчислювальний процес складається з «прогонів» (Runs). Це реальні запуски виконуваної програми, яка містить лише Диспетчер або Диспетчер і Задачу разом.

Оскільки логічний і фізичний рівні, як правило, не узгоджуються (наприклад, кілька коротких завдань можуть бути виконані під час одного прогону при динамічній збірці системи, тоді як довгий розрахунок може бути завершений лише протягом кількох прогонів), важливо забезпечити безперервність логічної структури обчислювального процесу. Це гарантується механізмом контрольних точок. Під час запису контрольних точок модулі Диспетчера й Задачі зберігають усю інформацію, що визначає поточний стан програмної системи, у так званих файлах контрольних точок (Checkpoint files, CPF). При наступному прогоні завантажені в ОП «порожні» (тобто без даних) фізичні модулі можуть зчитувати ці дані, забезпечуючи точно відновлений стан системи на момент запису відповідної контрольної точки.

Події та їх обробка. У логічній структурі обчислювального процесу є кілька місць, де необхідна одночасна активація багатьох ЛПМ системи. Це, наприклад, початок завдання або початок прогону, коли модулями повинні бути введені відповідно вхідні дані чи дані з CPF. На початку задачі потрібно один раз розрахувати певні коефіцієнти, щоб не перераховувати їх на кожному кроці задачі. Ще одна причина – запис контрольної точки. Вставка відразу багатьох викликів ЛПМ у відповідні точки алгоритму затьмарює його суть і вимагає змін після кожної зміни списку модулів. У цьому випадку більше підходить так званий механізм подій.

«Подією» (Event) в системі TULIPgm є переривання послідовного виконання алгоритму моделювання з почерговою передачею управління всім завантаженим в оперативну пам'ять ЛПМ. Існує дескриптор типу («розташування») події Event_Type (наприклад, "RunBegin", "RunEnd", "JobBegin", "JobEnd", "ChkPoint") і два модифікатори типу: Event_TypeM1 і Event_TypeM2, які детальніше описують умови виникнення події (наприклад, це запис чи зчитування контрольної точки). Збудження події (Event raise) полягає у виклику спеціальної підсистеми Диспетчера, яка містить списки ЛПМ Диспетчера і завантаженої Задачі і забезпечує передачу управління цим модулям.

Оскільки порядок активації ЛПМ не визначено заздалегідь, для забезпечення інформаційного зв'язку між модулями при обробці події ця подія розбивається на кілька рівнів

```
Module LocField_I00
  Real :: LocField_Ey
  Real :: LocField_Ez
  Interface
    Subroutine LocField_Electric ( Y, Z )
      Real :: Y, Z
    End subroutine LocField_Electric
  End interface
End module LocField_I00
```

Рис. 1. Інтерфейс модуля (файл LocField_I00.f90)

Event_Level (0, 1, 2, …). На кожному рівні всі завантажені модулі знову активуються по черзі. Якщо під час обробки події модуль 1 розраховує інформаційний об'єкт A, а модуль 2 обчислює інформаційний об'єкт B, використовуючи значення A, розрахунок A повинен бути розміщений на рівні *n*, а обчислення B – на рівні *n*+1 або більше. Крім того, модуль 1 потім може розрахувати інформаційний об'єкт C за допомогою значення B, якщо це зробити на рівні *n*+2 або більше і т.д. Для кожного типу події Event_Type визначено максимальний рівень обробки Event_MaxLev.

ЛПМ містять спеціальні процедури EventProc, які складаються з кількох так званих блоків обробки подій (Event processing blocks, EPB). Кожен EPB обробляє лише один тип і один рівень події. Інші типи або рівні при цьому ігноруються. Якщо модуль не містить відповідного EPB, його процедура EventProc відпрацьовує «вхолосту» на поточному типі та рівні події.

На жаль, при такому розподілі обробки подій з'являється новий тип «зчеплення» ЛПМ [18], який можна назвати «зчепленням за рівнем події». Його небажані наслідки можна зменшити шляхом ретельного планування глобальних (тобто загальносистемних) графіків обробки подій.

Таким чином, події в системі TULIPgm багато в чому подібні до механізму програмних переривань більшості з відомих архітектур комп'ютерів [19]. Новою є лише багаторівнева обробка подій з відповідним забезпеченням зв'язку ЛПМ за даними (інформаційними об'єктами). Замість активації довгих списків ЛПМ у певних точках алгоритму, в них розміщуються лише оператори збудження події. Модулі самостійно здійснюють обробку цих подій. Якщо список модулів змінюється (наприклад, після зміни Задачі), це впливає лише на підсистему обробки подій, а не на весь код програми.

Організація модулів. ЛПМ системи TULIPgm складається з двох частин: інтерфейсу модуля та реалізації модуля. Це ілюструють рис. 1 і 2, де показано демонстраційний модуль LocField з варіантом 00. Інтерфейсною частиною є модуль Fortran 90 LocField_I00, який включає експортовані програмні об'єкти (дані LocField_Ey, LocField_Ez та інтерфейс підпрограми LocField_Electric). Множина експортованих усіма модулями інформаційних об'єктів утворює єдину глобальну структуру даних – інформаційну основу програмної системи, на якій виконуються ті чи інші сценарії моделювання. Реалізуючою

```
Module LocField_R00
  Real :: CoeffY, CoeffZ
Contains
  Real function Interpol ( Coord, Coeff )
    Real :: Coord, Coeff
    Interpol = Coord * Coeff / 2.87
  End function Interpol
End module LocField_R00

Recursive subroutine LocField_EventProc
  Use Event_I00
  Use LocField_I00
  Use LocField_R00
  If ( Event_Type.eq."JobBegin" .and. Event_Level.eq.05 )
then
    CoeffY = 3.62                    ! EPB JobBegin_05
    CoeffZ = 4.12
  End if
End subroutine LocField_EventProc

Subroutine LocField_Electric ( Y, Z )
  Use LocField_I00
  Use LocField_R00
  Real :: Y, Z
  LocField_Ey = Interpol ( Coord=Y, Coeff=CoeffY )
  LocField_Ez = Interpol ( Coord=Z, Coeff=CoeffZ )
End subroutine LocField_Electric
```

Рис. 2. Реалізація модуля (файл LocField_R00.f90)

eISSN 2786-5525

```
        .........
Use LocField_I00
        .........
Call LocField_Electric ( Y=ParticleY, Z=ParticleZ )
SumEy = SumEy + LocField_Ey
SumEz = SumEz + LocField_Ez
        .........
```

Рис. 3. Використання модуля (OtherFile_R00.f90)

частиною є сукупність кількох елементів:

– модуля Fortran 90 LocField_R00, який містить приватні (не експортовані з LocField) інформаційні та процедурні об'єкти (дані CoeffY, CoeffZ і функція Interpol);

– рекурсивної процедури обробки подій LocField_EventProc;

– однієї або кількох експортованих процедур (функцій), таких як LocField_Electric. Елемент LocField_R00 пов'язує всі інші зазначені вище елементи. Оскільки файл LocField_R00.mod не заноситься в каталог системних модулів під час компіляції реалізації ЛПМ (на відміну від LocField_I00.mod під час компіляції інтерфейсу), він є недоступним з інших модулів. Підпрограму LocField_EventProc не описано в інтерфейсній частині, оскільки вона викликається спеціальною процедурою на асемблері, а не модулем Fortran 90, як LocField_Electric (рис. 3).

Елементи LocField_I00 і LocField_R00 містять усю інформацію, що описує стан модуля LocField під час його неактивності. Тому їхній вміст записується в CPF і зчитується з них за допомогою процедури EventProc (це не показано на рис. 2).

Модулі TULIPgm розділено на інтерфейсну та реалізуючу частини, оскільки Fortran 90 не підтримує важливу функцію мови Ада [20], а саме, окрему компіляцію інтерфейсу модуля та його тіла. За її відсутності будь-яка незначна переробка в реалізації модуля може призвести до «ланцюгової реакції» повторної компіляції викликаючих модулів. Крім того, це звільняє шлях до перехресного використання модулів, якщо це бажано. Також це причина, чому експортовані процедури (такі, як LocField_Electric) не розміщуються в модулях Fortran 90.

Збирання системи. Збирання системи TULIPgm з модулів (як динамічне, так і статичне) виконується в два етапи. По-перше, це вибір Задачі разом із її конфігурацією, тобто вибір списку ЛПМ для виконання. На цьому етапі визначається логічна структура програми. Другий етап – підбір варіантів модулів, тобто складання набору ФПМ. Після визначення таким чином фізичної структури системи, Задача або вся система завантажується в оперативну пам'ять і виконується.

Розглянемо детальніше динамічне збирання системи, як більш досконале. Коли попереднє завдання завершено, а наступне ще не розпочато, в оперативній пам'яті знаходиться лише Диспетчер, а не модулі Задачі. Назва потрібної Задачі (наприклад, CFD) і конфігурація (наприклад, 02) вводяться користувачем під час ініціювання нового завдання. Вони дозволяють Диспетчеру вибрати необхідний список логічних модулів (CFD_02.tbl) з-поміж попередньо визначених для різних Задач та їх конфігурацій.

Кожен логічний модуль має так званий дескриптор суфіксу, який являє собою ланцюжок з восьми двійкових ключів збірки (Assembling keys). Ключі однозначно визначають усі структури даних і особливості алгоритмів модуля. Варіант ЛПМ, тобто суфікс відповідного фізичного модуля, записується як двозначний шістнадцятковий еквівалент восьмизначного двійкового числа, яке утворюється конкретними значеннями ключів збірки.

Чотири старші біти дескриптора суфіксу є так званими «сильними» ключами. Вони впливають як на інтерфейсну, так і на реалізуючу частини відповідного модуля. Чотири молодші біти є «слабкими» ключами, які визначають лише особливості реалізації модуля. Кожна задача має свій набір ключів збірки. Додаток містить список ключів, які стосуються Задачі CFD (див. далі).

Припустимо, що логічний модуль LocField може бути реалізований у восьми варіантах:

– для 2D і 3D моделей;

– прямокутної і циліндричної геометрії приладу;

– приладів біжучої та стоячої хвилі. Нехай інтерфейсна частина модуля залежить лише від розмірності моделі, а реалізація ЛПМ визначається всіма перерахованими варіантами.

У результаті дескриптор суфіксу модуля може бути написаний, наприклад, як

NullKey NullKey NullKey TwoDims NullKey NullKey RectAng StaWave ,

де NullKey – «порожній» ключ, який завжди дорівнює нулю.

Зрозуміло, що фізичний модуль, який реалізовуватиме логічний модуль LocField для 3D моделі циліндричного приладу біжучої хвилі, матиме двійковий суфікс 00000000 (тобто шістнадцятковий 00). Суфікс модуля, що реалізує 2D модель прямокутного приладу стоячої хвилі, – 00010011 (або 13 відповідно) і т.д. Назви інтерфейсних частин модулів – LocField_I00 і LocField_I10; імена реалізуючих частин – LocField_R00 і LocField_R13 відповідно. Зрозуміло, що в загальному випадку кількість варіантів реалізації модуля може бути більшою, ніж кількість варіантів його інтерфейсу.

Алгоритм підбору варіантів модулів Задачі досить очевидний, якщо врахувати, що для всіх модулів системи існує список логічних суфіксів дескрипторів SuffDesc.tbl. Після введення користувачем значень ключів збірки Диспетчер генерує набір необхідних фізичних модулів (як інтерфейсних частин, так і реалізацій), які завантажуються в ОП.

Статичне збирання системи відрізняється від описаного вище динамічного тим, що список усіх фізичних модулів визначається перед запуском Диспетчера (оскільки в оперативну пам’ять модулі Задачі завантажуються одночасно з модулями Диспетчера). Тому неможливо змінити назву та конфігурацію Задачі, а також значення ключів збірки під час прогону.

Алгоритми програмної системи

Сьогодні в систему TULIPgm включено три Задачі, які називаються «CFD», «Cyclam» і «Magnol». Задача CFD (Crossed-Field Device) є універсальною, яка використовує кілька ключів збірки (див. Додаток) і дозволяє моделювати різні прилади зі схрещеними полями. Очевидно, що така модель не може врахувати надто дрібні деталі конструкцій приладів, наприклад внутрішні конструкції електронних гармат чи колекторів. Алгоритм цієї Задачі обмежений моделюванням простору взаємодії приладу разом із короткими відрізками зазорів, які розміщені між торцями ламелей сповільнюючої системи та між ними та торцевими екранами (див. рис. 4, де показано лінійний підсилювач зі схрещеними полями змішаного променево-розподілено-емісійного типу). Розробку цієї універсальної Задачі зараз призупинено. Замість неї розроблено дві спрощені Задачі, менш трудомісткі та дорогі. Задачу Cyclam (CYlindrical Closed AMplifier) призначено для 2D моделювання звичайних амплітронів і амплітронів з катодним збудженням, а також підсилювачів з простором дрейфу (SFD). Задача Magnol (MAGNetron OsciLlator) дозволяє також двовимірне моделювання звичайних та інвертованих магнетронів.

Алгоритми Задач Cyclam і Magnol досить схожі між собою і є підмножинами процедур Задачі CFD при певних значеннях ключів збірки. Тому подальший опис стосується модельних конфігурацій усіх трьох Задач. Як це типово для самоузгоджених нестаціонарних моделей електровакуумних приладів, алгоритми містять циклічні повторення моделювання руху заряджених часток і розрахунку полів.

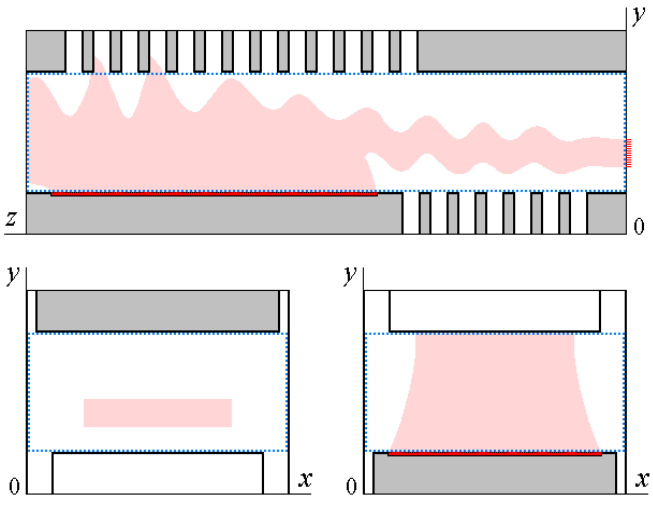

Рис. 4. Приклад геометрії системи, що моделюється

Динаміка часток. Кінетичне рівняння для електронного потоку розв’язується, як зазвичай, методом часток [7]. Два види моделей відрізняються визначенням значень зарядів часток. Алгоритми з фіксованим зарядом часток використовуються, як правило, за

наявності електронної гармати або термоелектронного катода. Вони розглядають число електронів у частці як постійне в часі й однакове для всіх часток. Моделі зі змінним зарядом часток доречні, якщо присутній лише холодний вторинно-емісійний катод. На першому етапі моделювання кожна частка тут дорівнює одному електрону. Під час перехідного процесу розміри часток багаторазово збільшуються при актах вторинної емісії. Щоб уникнути суттєвої диференціації зарядів, виконується видалення надто малих часток разом з «розщепленням» великих замість збільшення їх зарядів при подальших актах вторинної емісії.

Рівняння руху часток розв'язується за схемою Рунге–Кутта четвертого порядку [21]. Інтерполяція значень полів між точками сітки дискретизації перед підстановкою в праву частину рівняння здійснюється за допомогою чотиривимірного методу PWS (Polynomials with Smoothing) [22]. Використовується інтерполяційний поліном першого порядку

$$\vec{E}(t,x,y,z) = P\vec{E}_0 + P\vec{E}_t \cdot (t-t_0) + P\vec{E}_x \cdot (x-x_0) + P\vec{E}_y \cdot (y-y_0) + \vec{E}_z \cdot (z-z_0),$$

де $P\vec{E}_0, P\vec{E}_t, P\vec{E}_x, P\vec{E}_y, P\vec{E}_z$ – векторні коефіцієнти поліному; t_0, x_0, y_0, z_0 – координати центру чотиривимірної комірки, в якій перебуває частка.

Вирази для множників $P\vec{E}_0$ К $P\vec{E}_z$, а також інвертовану форму для розподілу зарядів часток на точки сітки дискретизації наведено в [22]. Екстраполяція координати частки $\vec{r}$ і її швидкості $\vec{v}$ на кінець наступного часового кроку (для передбачення значень полів у цей момент) виконується за формулами:

$$\vec{v}_X = \vec{v}_E + (\vec{v}_E - \vec{v}_B); \qquad \vec{r}_X = \vec{r}_E + (\vec{v}_E + \vec{v}_X)\Delta t/2,$$

де індекс *B* (Begin) відноситься до початку часового кроку Δt, індекс *E* (End) – до його кінця, індекс *X* (eXtrapolated) – до кінця наступного часового кроку. Таким чином, моделюючий алгоритм перетворюється на своєрідний метод прогнозу та корекції. Деяке збільшення обсягу розрахунків цілком компенсується зменшенням шуму моделі за рахунок часової інтерполяції полів.

Флуктуації вихідних параметрів, що залежать від часу, додатково зменшуються шляхом згладжування за допомогою моделі лінійної регресії $f(t) = a_0 + a_1 t$ на інтервалі довжиною до 256 часових кроків. Це забезпечує значно меншу затримку вихідних даних під час перехідного процесу порівняно з усередненням, яке зазвичай використовується в таких випадках.

Одним з незначних, але дуже корисних на практиці нововведень, є автоматичне визначення заряду частки (якщо використовується модель з фіксованим зарядом), що звільняє користувача від виснажливої «підгонки» цього значення. Це здійснюється за допомогою аналітичного прогнозування характеристик майбутньої хмари Бріллюена у приладі.

Потенціальні поля. Потенціальні поля розраховуються як суперпозиція розв'язків рівнянь Лапласа та Пуассона. Перше розв'язується методом SOR з прискоренням Чебишова [7] один раз на початку завдання. В результаті для всіх електродів знаходяться й табулюються одиничні структурні функції електричного поля, які потім множаться на потенціали відповідних електродів у кожен момент часу. Для двократного розв'язування рівняння Пуассона на кожному кроці задачі використовується метод FACR [7] з нульовими граничними умовами на всіх електродах і періодичними або дзеркальними в напрямку дрейфу потоку (залежно від значення ключа ReEntra). Пунктирні лінії на рис. 4 обмежують область, де розв'язується рівняння Пуассона.

Соленоїдні поля. Три конфігурації кожної з зазначених вище Задач розрізняються підходом до розрахунку вихрових полів. Наприклад, в Magnol_00 соленоїдні поля взагалі не враховуються, тобто моделюється магнетронний діод. Конфігурація Magnol_01 реалізує модель другого рівня [12], що означає розрахунок вихрових полів методом комплексних амплітуд [17]. У Magnol_02 використовується модель першого рівня, у якій соленоїдні поля оцінюються методом миттєвих значень [17].

Розв’язання рівняння збудження другого порядку використовується за схемою $P(EC)^3E$ Адамса–Бешфорта четвертого порядку [21]. Електродинамічне узгодження входу і виходу сповільнюючої системи виконується з моделюванням реальних опорів зв’язку [17].

Використовується форма Фур’є рівняння збудження першого порядку для StaWave=1 і форма Даламбера для StaWave=0 [16], як більш природні. Друга форма розв’язується за допомогою неявної скінченно-різницевої схеми другого порядку. Кожен високочастотний сигнал в сповільнюючій системі моделюється як суперпозиція основної та додаткової частин. Вони відповідають прямій та зворотній хвилям відповідно (якщо StaWave=0) або двократно виродженим нормальним модам сповільнюючої системи (якщо StaWave=1), крім видів коливань 0_1 і π, де додаткові частини завжди дорівнюють нулю.

Допоміжні процедури. Для підтримки описаних алгоритмів моделювання різними математичними методами до системи TULIPgm включено невеликий «пакет наукових підпрограм». Він містить найкращі чисельні процедури, спеціально відібрані та адаптовані для задач спектрального моделювання (усі наявні у вихідних кодах). Наприклад, в нього входять генератори випадкових чисел з різними законами розподілу, розв’язувачі нелінійних рівнянь, програми швидкого перетворення Фур’є тощо. Особливо слід згадати параметричні процедури для спектрального й гармонійного оцінювання, як «sanctum sanctorum» алгоритмів спектрального моделювання. Існують процедури спектрального аналізу дійсних і комплексних часових рядів за допомогою модифікованого коваріаційного методу [23], а також для гармонійного розкладання в ряди Фур’є за допомогою первинних методів Проні і методів найменших квадратів Проні (включаючи змішаний підхід [24]) та усіх подальших їх покращень.

Системний інтерфейс програми

Існують три фізичні канали для обміну інформацією між системою TULIPgm та зовнішнім середовищем:

– файли JLF та CPF, де використовуються неформатовані (двійкові) дані;

– інтерактивне введення та відображення форматованої (тобто, орієнтованої на користувача) інформації через клавіатуру та монітор відповідно;

– механізм зовнішніх переривань, який не передає жодних даних, але змінює стан програмної системи.

Сучасні алгоритми моделювання потребують досить складних процедур підготовки даних, а також діагностичних процедур (наприклад, при визначенні геометрії приладу, призначенні частотного розподілу вхідних сигналів, аналізі стану електронного потоку, візуалізації спектрів вихідних сигналів тощо). Якщо усі ці процедури включити в моделюючі конфігурації Задачі (00…0F), – вони стануть схожими на динозаврів: величезними, незграбними і незмінними. Щоб уникнути аналогічного кінця еволюції, до моделюючих конфігурацій включено лише найпростіші процедури введення даних і діагностики. Більшість процедур підготовки вхідної інформації та обробки вихідних даних і візуалізації виносяться в допоміжні й сервісні конфігурації Задачі, які виконуються окремо від моделюючих, тобто в інших екземплярах Диспетчера (синхронно або асинхронно: до моделювання чи після нього). Передача інформації між моделюючими, допоміжними та сервісними конфігураціями тієї самої Задачі виконується за допомогою файлів JLF та CPF. Інформаційний зв’язок між різними Задачами не передбачено.

Крім простоти розробки невеликих програм, такий підхід має ще одну перевагу. А саме: якщо користувач розуміє деякі правила написання Задачі або (альтернативно) знає формат кодування інформації в файлах JLF і CPF, він може створити власні програми підготовки даних і діагностики, якщо вони знадобляться. Більше того, це можна здійснити навіть під час виконання моделюючої конфігурації Задачі, наприклад для «миттєвого фотографування» якоїсь незвичайної конфігурації електронного потоку.

Усі форматовані дані системи (за винятком функцій розподілу та повідомлень) являють собою логічний набір так званих вхідних-вихідних параметрів (Input-Output Parameters, IOP).

Вони можуть бути скалярами (наприклад, Tube_Width) або векторами [як DelayLine2_VanesWidth(1:DelayLine2_VanesNumb)]. Їх мнемонічні назви (на додачу до цифрових, наприклад, Z101-11) є унікальними в межах Задачі та раціонально корелюють між різними Задачами, якщо ними моделюються схожі за конструкцією прилади (скажімо, між Задачами CFD, Cyclam і Magnol). Більшість IOP подібні до відповідних інформаційних об'єктів логічної структури програмної системи. Проте, для зручності користувача їхні одиниці виміру можуть відрізнятися (наприклад, міліметри замість метрів). Формати IOP та інформаційного об'єкта можуть також відрізнятися, якщо інформаційний об'єкт являє собою матрицю або структуру (оскільки IOP може бути лише скаляром або вектором) [наприклад, DelayLines_VanesWidth(1:DelayLines_Numb, 1:DelayLines_VanesMaxNumb)].

Об'єми вхідної та вихідної інформації в процесі прогону можна варіювати в широких межах (від максимального до нуля) за допомогою так званих чисел стану вводу-виводу (Input-Output Condition Numbers, IOCN), від 0 до 6. Кожному вхідному та вихідному параметру заздалегідь присвоюється певне число вводу-виводу (Input-Output Number, ION), від 1 до 7 залежно від його інформаційної цінності (1 – найважливіші параметри, 7 – приховані). Параметр вводиться або виводиться лише у випадку, якщо його ION менше або дорівнює поточному IOCN. При IOCN = 0 програмна система тимчасово стає «річчю в собі», що зручно при тривалих прогонах.

Загальний вигляд «лицьової панелі» системи TULIPgm наведено на рис. 5. У її верхній частині розміщене головне вікно, де відображається найважливіша інтерактивна інформація, включаючи поточний розподіл електронного потоку в приладі, значення деяких IOP, довідкову інформацію, логотипи тощо. Під цим вікном розташовано область повідомлень з кількома найпізнішими вхідними та вихідними звітами у форматі «телетайп». У нижній частині панелі розміщено віконце вводу для контрольного відображення інформації, що вводиться з клавіатури та миші. В недіалоговому режимі системи (під час відсутності вводу) воно затінене. Праворуч від області повідомлень розташовані кнопки зовнішніх переривань.

Приклади застосування системи TULIPgm

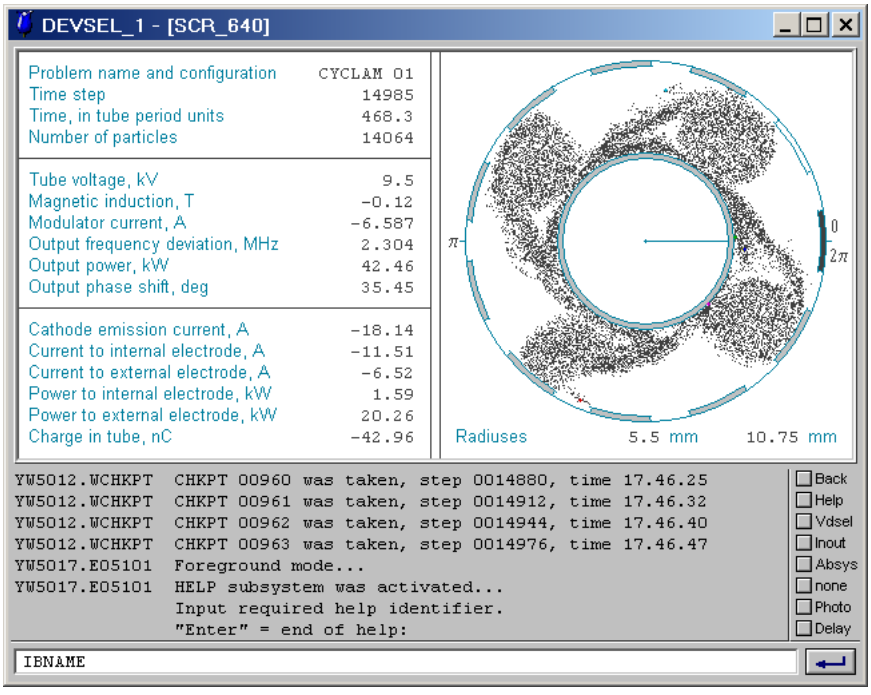

Рис. 5. Загальний вигляд працюючої системи TULIPgm

Система моделювання TULIPgm може бути використана як для дослідження фізичних явищ взаємодії електронних потоків з електромагнітними хвилями, так і для конструкторського аналізу та оптимізації НВЧ приладів. Реалізація спектрального підходу дозволяє використовувати цю систему для вирішення задач електромагнітної сумісності при розробці нових приладів [12]. Спільне використання різнорівневих спектральних моделей [17] забезпечує широкосмуговий спектральний моніторинг вихідних сигналів з достатньою точністю.

Як зразок моделювання перехідних процесів у приладах М-типу на рис. 5 показано конвективні явища в 40-кВт амплітроні D-діапазону. Обертові солітоноподібні хмари на вершинах спиць можуть збільшити потужність анодного бомбардування, оскільки швидкість часток на зовнішніх межах хмар збільшується. Крім того, коливання розмірів і форм хмар від спиці до спиці підвищують рівень шуму приладу.

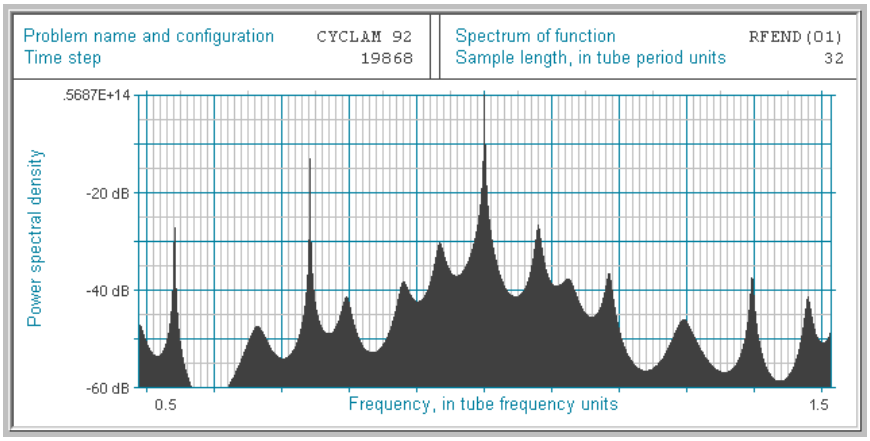

Рис. 6. Спектр вихідного сигналу амплітрона

Як зразок спектрального моделювання на рис. 6 показано розподіл спектральної щільності потужності (PSD) вихідного сигналу амплітрона в діапазоні частот від 625 до 1875 МГц за умови, що вхідний сигнал є чисто гармонійним. Підвищені значення PSD поблизу несучої частоти викликані, зокрема, шумом алгоритму PIC. Проте флуктуації електронної хмари також викликають стохастичну низькочастотну модуляцію вихідного сигналу. Його частотний розподіл можна знайти як межу загальної функції PSD при зростанні кількості часток.

Усі чисельні результати, наведені у [8–12], також були отримані за допомогою системи TULIPgm.

Висновки

1. Сучасний етап розвитку збройних сил України потребує проведення масштабних досліджень у наукових та навчальних установах відповідного профілю щодо розробки ефективних засобів протидії масованим атакам малих безпілотних літальних апаратів, зокрема, заснованих на принципах невідновного ураження електроніки БПЛА короткими електромагнітними імпульсами потужного НВЧ генератора. Одними з перспективних видів джерел електромагнітних коливань для цієї мети слід вважати вакуумні НВЧ прилади.

2. Незважаючи на досить довгу історію розробки, система моделювання вакуумних НВЧ приладів TULIPgm залишається цілком сучасною системою. Це результат кількох радикальних реконструкцій коду, з усуненням застарілих і непотрібних елементів, з одного боку, і імплантацією перспективних та корисних функцій моделі та програми – з іншого. Такий підхід, природно, більш трудомісткий і дорогий, однак альтернатива йому – поступова еволюція – призводить, як правило, до накопичення непотрібних фрагментів з застарілих мов програмування й операційних систем.

3. Поряд з кодуванням нової версії системи TULIPgm найближчим завданням є переклад усіх коментарів до програми та інтерфейсних текстів англійською мовою. Серед довгострокових перспектив удосконалення системи можна зазначити:

– завершення основної Задачі CFD, включаючи її 3D модель;

– реалізацію спектрального підходу для ЛБВ та клістронів;

– впровадження алгоритмів, заснованих на безпосередньому інтегруванні рівнянь Максвелла методом скінчених різниць (так званих спектральних моделей нульового рівня [17]) для моделювання релятивістських магнетронів.

Додаток. Ключі збірки Задачі CFD

RectAng = 0 для циліндричних приладів (як магнетрон); 1 для прямокутних (як лінійна ЛБХ М-типу).

ReEntra = 0 для приладів з незамкнутим електронним потоком (як дематрон); 1 для приладів з замкнутим електронним потоком (як амплітрон).

StaWave = 0 для приладів біжучої хвилі (як амплітрон); 1 для приладів стоячої хвилі (як магнетрон).

TwoDims = 0 для 3D моделей [(z,r,φ) або (x,y,z)]; 1 для 2D моделей [(r,φ) або (y,z)].

VarChar = 0 для моделей з фіксованим зарядом часток; 1 для моделей зі змінним зарядом часток.

Подяки

Визначення напряму досліджень, постійна увага та всебічна підтримка на перших, найбільш відповідальних етапах розробки програмної системи TULIPgm здійснювалися проф. О.Г. Шеїним. Вагомою була ґрунтовна багаторічна допомога колективу обчислювального центру Фізико-технічного інституту низьких температур (Харків), керівники центру на той час – К.В. Маслов і В.Р. Літвінов.

Список літератури:

1. Rogers J.P. (2024) De Gruyter Handbook of Drone Warfare. 1st edn. De Gruyter. Available at: https://www.perlego.com/book/4512899/de-gruyter-handbook-of-drone-warfare-pdf (Accessed: 3 May 2025).

2. R.R.U. Inc. (2025) -drone Technology to Detect and Stop 10 Types of Counter Drones Today. Available at: https://www.robinradar.com/resources/10-counter-drone-technologies-to-detect-and-stop-drones-today (Accessed: 04 May 2025).

3. Atherton K.D. (2023) The Air Force Used Microwave Energy to Take Down a Drone Swarm. Available at: https://www.popsci.com/technology/thor-weapon-drone-swarm-test/ (Accessed: 03 May 2025).

4. Nikolov B. (2025) UK's new microwave weapon neutralizes drone swarms for pennies, Bulgarian Military Industry Review. Available at: https://bulgarianmilitary.com/2025/04/17/uks-new-microwave-weapon-neutralizes-drone-swarms-for-pennies/ (Accessed: 04 May 2025).

5. Tsimring S.E. Electron Beams and Microwave Vacuum Electronics. Wiley-Interscience, 2006. 574 p.

6. Carter R.G. Microwave and RF Vacuum Electronic Power Sources. Cambridge Univ. Press., 2018. 808 p.

7. Hockney R.W., Eastwood J.W. Computer Simulation Using Particles. McGraw-Hill, Inc., 1981. 562 p.

8. Gritsunov A.V., Shein A.G. Computer simulation of transient processes during the interaction of an electron beam with a backward wave in M-type amplifiers with distributed emission // Radiotekhnika. 1983. No 65. P. 93–99.

9. Churyumov G.I., Gerasimov V.P., Gritsunov A.V., Zakorin V.A. Prospects of applying a computational experiment to the concept and the use of crossed-field devices // Telecommunications and Radio Engineering. 1998. V. 52. No 12. P. 39–48.

10. Gritsunov A.V., Kozorezov G.G., Kopot M.A. On increasing of the gain ratio of crossed field double-row amplifiers // Telecommunications and Radio Engineering. 2006. 65. No 8. P. 731–737.

11. Gritsunov A.V. On the reasons for noises in cross-field devices // Telecommunications and Radio Engineering. 2005. V. 64. No 11. P. 939–958.

12. Vasyanovich A.V., Gritsunov A.V., Nikitenko A.N., Horunzhii M.O. General principles of spectral modeling of microwave devices // Telecommunications and Radio Engineering. 2003. V. 60. No. 1–2. P. 88–99.

13. Gritsunov A.V. On a spectral approach to simulation of microwave devices // Journal of Communications Technology and Electronics. 2004. V. 49. No 7. P. 829–832.

14. Gedney S.D. Introduction to the Finite-Difference Time-Domain (FDTD) Method for Electromagnetics. Springer Cham, 2011. 236 p.

15. Jin J.-M. The Finite Element Method in Electromagnetics. Wiley-IEEE Press, 2014. 876 p.

16. Bilotserkivska A.I., Bondarenko I.M., Gritsunov A.V., Babychenko O.Yu., Sviderska L.I.,Vasianovych A.V. Decomposition of electromagnetic potentials in partial functions of dispersive electrodynamic lines // Ukrainian J. of Physics. 2024. V. 69. No 6. P. 382–394.

17. Gritsunov A.V. Methods of calculation of nonstationary nonharmonic fields in guiding electrodynamic structures // Journal of Communications Technology and Electronics. 2007. V. 52. No 6. P. 601–616.

18. Ziegler C.A. Programming System Methodologies. Prentice-Hall, Inc, 1983. 308 p.

19. Hyde R. The Art of Assembly Language Programming. No Starch Press, Inc., 2010. 732 p.

20. Feldman M.B., Koffman E.B. Ada: Problem Solving and Program Design. Addison-Wesley, 1993. 795 p.

21. Chapra S.C., Canale R.P. Numerical Methods for Engineers. McGraw-Hill Ed., 2015. 970 p.

22. Gritsunov A.V. About simulation of fields in large particles model // Proc. 1997 SBMO/IEEE MTT-S Int. Microwave and Optoelectronics Conf. Natal (Brazil). 1997. Vol. 2. P. 517–519.

23. Marple S.L., Jr., Digital Spectral Analysis with Applications. Prentice-Hall, Inc., 1987. 492 p.

24. Gritsunov A.V., Turenko L.Y. Harmonic decomposition of an exciting current in simulation of the electron devices // Telecommunications and Radio Engineering. 2002. V. 58. No 11–12. P. 56–67.

Надійшла до редколегії 05.03.2025

Відомості про авторів:

Бондаренко Ігор Миколайлович – д-р фіз.-мат. наук, професор, Харківський національний університет радіоелектроніки, завідуючий кафедрою мікроелектроніки, електронних приладів та пристроїв, Україна; e-mail: ihor.bondarenko@nure.ua, ORCID: https://orcid.org/0000-0003-3907-6785

Гнатенко Олександр Сергійович – канд. фіз.-мат. наук, доцент, Харківський національний університет радіоелектроніки, завідуючий кафедрою фізичних основ електронної техніки, Україна; e-mail: oleksandr.hnatenko@nure.ua, ORCID: https://orcid.org/0000-0001-7722-0923

Грицунов Олександр Валентинович – д-р фіз.-мат. наук, професор, Харківський національний університет радіоелектроніки, професор кафедри мікроелектроніки, електронних приладів та пристроїв, Україна; e-mail: alexander.gritsunov@nure.ua, ORCID: https://orcid.org/0000-0002-2258-4006

Пащенко Олексій Георгійович – канд. фіз.-мат. наук, доцент, Харківський національний університет радіоелектроніки, доцент кафедри мікроелектроніки, електронних приладів та пристроїв, Україна; e-mail: olexiy.pashchenko@nure.ua, ORCID: https://orcid.org/0000-0001-8927-3811

Карнаушенко Володимир Петрович – Харківський національний університет радіоелектроніки, старший викладач кафедри мікроелектроніки, електронних приладів та пристроїв, Україна; e-mail: vladimir.karnaushenko@nure.ua, ORCID: https://orcid.org/0000-0001-7744-2569

Копоть Михайло Андрійович – Харківський національний університет радіоелектроніки, завідуючий навчальною лабораторією кафедри програмної інженерії, Україна; e-mail: mykhaylo.kopot@nure.ua, ORCID: http://orcid.org/0000-0002-7163-8904

ABSTRACTS РЕФЕРАТИ

SYSTEMS AND METHODS OF INFORMATION PROTECTION
СИСТЕМИ І МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ

UDC 004.056.5

Optimization of digital signature calculation and verification operations for the FIPS 205 standard / *I.D. Gorbenko, O.G. Kachko, Ya.A. Derevianko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2025. No 221. P. 7 – 13.

Currently, significant efforts at the international and national levels are focused on the creation of practical quantum-resistant digital signature (DS) mechanisms. The first round of the international PQC competition has been conducted [1], which resulted in the creation and standardization of the finalists of the 3rd round of the competition, recommended as international standards, as US federal standards, in particular FIPS 205, a stateless digital signature standard based on a hash function (SPHINCS+ algorithm).

A hash-based signature is one of the most promising candidates (and perhaps the most conservative approach) for a post-quantum digital signature. The advantage of hash-based signatures is that their (classical and quantum) security strength is better understood (and easier to evaluate) than other candidates relying solely on the idealized strength of cryptographic hash functions.

The signature scheme standardized in FIPS 205 is constructed using other hash-based signature schemes as components: a few-time signature scheme, forest of random subsets (FORS), and a multi-time signature scheme, the eXtended Merkle Signature Scheme (XMSS).

The standard defines a DS scheme designed to withstand future quantum and classical quantum computer attacks that threaten the security of existing standards. Since the algorithm has already been standardized, an important task is to study its structure and practical implementation of the requirements for its components: parameter construction, key pair generation, DS production and verification, etc. Its solution depends to a large extent on improving the algorithm in terms of execution complexity (speed), which can be reduced to optimizing basic operations.

In this article, we consider and propose practical improvements to optimize the DS for the FIPS 205 algorithm based on the use of parallel computing. This is achieved mainly by optimizing the SHAKE256, SHA256, and SHA512 algorithms. The importance of optimizing the calculation of hash values is related to the fact that hashing is the main operation in FIPS 205.

The results obtained indicate the feasibility and relevance of the improvements made. Optimization provides a minimum speedup of 10% for all operations and all parameters.

Key words: post-quantum standards; parallel computing; optimization; hash functions; extendable-output functions; SHA3; SHA2.

11 tabl. Ref: 6 items.

УДК 004.056.5

Оптимізація операцій обчислення та перевірки цифрового підпису для стандарту FIPS 205 / *І.Д. Горбенко, О.Г. Качко, Я.А. Дерев'янко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2025. Вип. 221. С. 7 – 13.

Наразі суттєві зусилля на міжнародному та національному рівнях зосереджені на створенні практичних квантово-стійких механізмів цифрового підпису (ЦП). Проведено перший етап міжнародного конкурсу PQC [1], підсумком якого є створення та стандартизація в якості федеральних стандартів США фіналістів 3 раунду конкурсу, рекомендованих в якості міжнародних, зокрема FIPS 205 – стандарту ЦП без стану на основі геш функції (алгоритм SPHINCS+).

Підпис на основі гешу є одним із найперспективніших кандидатів (і, можливо, найбільш консервативним підходом) на постквантовий цифровий підпис. Перевага підписів на основі гешування полягає в тому, що їх (класичну та квантову) стійкість безпеки краще зрозуміти (і легше оцінити), ніж у інших кандидатів, покладаючись виключно на ідеалізовану надійність криптографічних геш функцій.

Схема підпису, стандартизована у FIPS 205, побудована з використанням інших схем підпису на основі гешу як компонентів: схеми одноразового підпису, лісу випадкових підмножин (FORS), та схеми багаторазового підпису, розширеної схема підпису Мерклі (eXtended Merkle Signature Scheme, XMSS).

У стандарті визначено схему ЦП, яка покликана протистояти майбутнім квантовим та класичним атакам квантових комп'ютерів, що загрожують безпеці існуючих стандартів. Оскільки алгоритм уже стандартизовано, то важливим завданням є дослідження його будови та практичної реалізації вимог до складових: побудови параметрів, генерування ключових пар, вироблення ЦП та їх верифікації, тощо. Його вирішення суттєвою мірою залежить від покращення алгоритму з точки зору складності виконання (швидкодії), що може бути зведено до оптимізації базових операцій.

Розглянуто та запропоновано практичні удосконалення з метою оптимізації ЦП для алгоритму FIPS 205 на основі застосування паралельних обчислень. Це досягається в основному за рахунок оптимізації алгоритмів SHAKE256, SHA256 та SHA512. Важливість оптимізації обчислення геш значень пов'язана з тим, що гешування є основною операцією у FIPS 205.

Отримані результати вказують на перспективність та актуальність проведених удосконалень. Застосування оптимізації забезпечує мінімальне прискорення для усіх операцій і всіх параметрів – 10 %.

Ключові слова: постквантові стандарти; паралельні обчислення; оптимізація; функції гешування; функції розширюваного виводу; SHA3; SHA2.

Табл. 11. Бібліогр.: 6 назв.

UDC 004.056.5:004.8

Research and analysis of international standards and regulatory requirements for artificial intelligence security, development of a security model for Ukraine / *Y.O. Lohachova, M.V. Yesina, D.Yu. Holubnychyi* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2025. No 221. P. 14 – 22.

The article presents a comprehensive analysis of international approaches to the regulation of artificial intelligence (AI) security and the potential for their application within the Ukrainian context. It examines contemporary cybersecurity challenges in the era of AI development, including threats of data breaches, attacks involving generative models, and the misuse of deepfake technologies. Key international standards are analyzed, such as the EU AI Act, the NIST AI Risk Management Framework, ISO/IEC 23894, as well as regulatory approaches implemented in the United States and the United Arab Emirates. Special emphasis is placed on the importance of a multi-level AI risk management system that takes into account technical, ethical, legal, and social aspects. Particular attention is given to the study of Ukraine's strategic documents aimed at developing a national AI policy aligned with European requirements. The concept of gradual implementation of ethical, legal, and technical norms into AI regulation is highlighted, through mechanisms such as certification, the establishment of regulatory sandboxes, and public consultations. The proposed author's model for AI security in Ukraine is based on the principles of multilateral interaction among the state, businesses, the academic community, civil society, and international partners, involving the active engagement of all stakeholders in the process of policy and standards development. The model envisions a risk-oriented approach to the development and deployment of AI systems, the introduction of a public ethical AI registry, the participation of citizens in audit and monitoring processes for high-risk systems, and the promotion of the responsible use of emerging technologies in socially significant sectors. The article emphasizes that Ukraine has a unique opportunity to offer the world its own approach to the secure and ethical use of AI, which is flexible, open, and adaptive, based on the principles of trust, responsibility, digital resilience, and respect for human rights.

Key words: cybersecurity; security; artificial intelligence; technology; standardisation; information model.

1 fig. Ref: 10 items.

УДК 004.056.5:004.8

Дослідження та аналіз міжнародних стандартів та регуляторних вимог щодо безпеки штучного інтелекту, розробка моделі безпеки для України / *Є.О. Логачова, М.В. Єсіна, Д.Ю. Голубничий* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2025. Вип. 221. С. 14 – 22.

Проведено комплексний аналіз міжнародних підходів до регулювання безпеки штучного інтелекту (ШІ) та можливість їх застосування в українському контексті. Розглянуто сучасні виклики кібербезпеки в епоху розвитку ШІ, зокрема загрози витоку даних, атаки із використанням генеративних моделей та зловживань deepfake технологіями. Проаналізовано основні міжнародні стандарти: EU AI Act, NIST AI Risk Management Framework, ISO/IEC 23894, а також підходи, що впроваджуються у США та Об'єднаних Арабських Еміратах. Акцент зроблено на важливості багаторівневої системи управління ризиками ШІ, яка враховує технічні, етичні, правові та соціальні аспекти. Особливу увагу приділено дослідженню стратегічних документів України, спрямованих на створення національної політики у сфері ШІ із урахуванням європейських вимог. Висвітлено концепцію поступового впровадження етичних, правових та технічних норм у регулювання ШІ через механізми сертифікації, створення регуляторних пісочниць і публічних консультацій. Запропонована авторська модель безпеки ШІ для України, що базується на принципах багатосторонньої взаємодії держави, бізнесу, академічної спільноти, громадського суспільства та міжнародних партнерів, що передбачає активне залучення всіх стейкхолдерів до процесу формування політик та стандартів. Модель передбачає ризик-орієнтований підхід до розробки та використання ШІ-систем, запровадження публічного етичного реєстру ШІ, участь громадян у процесах аудиту й моніторингу систем високого ризику, а також стимулювання відповідального використання новітніх технологій у суспільно важливих сферах. Підкреслюється, що Україна має унікальну можливість запропонувати світові власний підхід до безпечного та етичного використання ШІ – гнучкий, відкритий і адаптивний, заснований на принципах довіри, відповідальності, цифрової стійкості та дотримання прав людини.

Ключові слова: кібербезпека; безпека; штучний інтелект; технології; стандартизація; інформаційна модель.

Іл. 1. Бібліогр.: 10 назв.

UDC 004.056:519.2

The improved Levin's algorithm for constrained probabilistic pseudo-Boolean functions / *A.M. Alekseychuk, Y.R. Kindrat* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2025. No 221. P. 23– 30.

The problem of finding "highly probable" approximations of Boolean functions consists in generating a list of all linear Boolean functions that agree with a given Boolean function in at least a specified number of binary sets. If a

Boolean function is given by its truth table, the most well-known algorithm for solving this problem is the Fast Hadamard Transform. However, this method is not optimal in terms of complexity, even among deterministic algorithms. If the Boolean function is given by an oracle and depends on hundreds or thousands of variables, the application of deterministic algorithms for finding its linear approximations becomes practically infeasible. In this case, polynomial probabilistic algorithms are used, such as the Goldreich–Levin algorithm and its modifications. One of the fastest among them currently is the improved Levin's algorithm. In the language of coding theory, this algorithm performs list decoding of the Hadamard code, which involves the value vectors of all *n*-variable linear Boolean functions.

This paper presents a generalization of the improved Levin's algorithm to the case of constrained probabilistic pseudo-Boolean functions. The main result is a theorem establishing a lower bound on the probability that each sought approximation appears in a random list generated by the proposed algorithm. The consideration of such functions is necessary to extend the applicability of the improved Levin's algorithm (in place of the original Goldreich–Levin algorithm) within the well-known framework for proving the security of stream ciphers. In particular, the results of this paper enable a more efficient reduction of problems in proofs of pseudo-randomness for certain well-known keystream generators, assuming high computational complexity of decoding random linear block codes or solving random systems of nonlinear Boolean equations. The obtained results can also be used for finding linear approximations of encryption transformations of block ciphers, which is important for constructing linear attacks against them.

Key words: cryptographic protection of information; provably secure keystream generator; Goldreich–Levin theorem; improved Levin's algorithm; probabilistic function.

Ref: 15 items.

УДК 004.056:519.2

Удосконалений алгоритм Левіна для обмежених ймовірнісних псевдобулевих функцій / *А.М. Олексійчук, Ю.Р. Кіндрат* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2025. Вип. 221. С. 23 – 30.

Задача знаходження "високоймовірних" наближень булевих функцій полягає в тому, щоб сформувати список усіх лінійних булевих функцій, які співпадають із заданою булевою функцією не менше ніж на визначену кількість (яка є більше за половину усіх можливих) двійкових наборів. Якщо булева функція задається за допомогою таблиці істинності, то найвідомішим алгоритмом розв'язання цієї задачі є алгоритм швидкого перетворення Адамара, який, однак, не є оптимальним за складністю навіть серед детермінованих алгоритмів. Якщо булева функція задається за допомогою оракула і залежить від сотень або тисяч змінних, то застосування детермінованих алгоритмів знаходження її лінійних наближень є практично неможливим. В цьому випадку використовують поліноміальні ймовірнісні алгоритми, до яких відносяться алгоритм Гольдрайха–Левіна та його модифікації. Одним з найшвидших серед них на сьогодні є удосконалений алгоритм Левіна. Говорячи мовою теорії кодування, цей алгоритм здійснює списочне декодування коду Адамара, який складається з векторів значень усіх лінійних булевих функцій від *n* змінних.

Представлено узагальнення вдосконаленого алгоритму Левіна на випадок обмежених ймовірнісних псевдобулевих функцій. Основним результатом є теорема, яка встановлює нижню межу ймовірності потрапляння кожного шуканого наближення до випадкового списку, що формується з використанням наведеного алгоритму. Розгляд таких функцій є необхідним для розповсюдження можливості застосування вдосконаленого алгоритму Левіна (замість оригінального алгоритму Гольдрайха–Левіна) у відомій схемі доведення стійкості потокових шифрів. Зокрема, результати статті надають можливість отримати більш ефективну редукцію задач у доведеннях псевдовипадковості деяких відомих генераторів гами за умови високої обчислювальної складності декодування випадкових лінійних блокових кодів або розв'язання випадкових систем нелінійних булевих рівнянь. Отримані результати можуть бути використані для знаходження лінійних апроксимацій шифрувальних перетворень блокових шифрів, що є важливим при побудові лінійних атак на них.

Ключові слова: криптографічний захист інформації; обґрунтовано стійкий генератор гами; теорема Гольдрайха–Левіна; удосконалений алгоритм Левіна; ймовірнісна функція.

Бібліогр.: 15 назв.

UDC 004.056

Threat and adversary models for QRNG web services / *D.M. Morhul, O.P. Nariezhnii, T.O. Hrinenko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2025. No 221. P. 31 – 38.

Quantum Random Number Generators (QRNG), based on physical processes of quantum mechanics, provide a high level of entropy and unpredictability, making them a promising source of randomness for use in information and communication systems, particularly in the context of post-quantum cryptography.

However, using the QRNG in the format of a web service (e.g., via public APIs or cloud platforms) introduces new attack vectors that may compromise the trust in the generated data. This work develops a threat model and an offender model for a QRNG web service. The methodological foundation of the study is based on modern risk analysis standards, including the ISO/IEC 27005, STRIDE, and Common Criteria. Critical system assets are identified, potential threats are classified considering the specifics of quantum generation, and an offender profile is constructed.

Typical attack scenarios are considered, including random number interception, physical generator compromise, API service attacks, and insider threats. For each scenario, a risk assessment is performed based on the likelihood of occurrence and potential consequences. A comprehensive set of protection measures is proposed, including technical

(TLS, post-processing, monitoring), organizational (access control, auditing), and procedural (incident response) solutions.

The results of this work can be used to develop secure QRNG services integrated into critical cryptographic systems and serve as a basis for further research in the field of quantum technology security modeling.

Key words: STRIDE; QRNG; web service; entropy; information security; cryptography; threat model; adversary model; randomness post-processing.

4 tab. 3 fig. Ref.: 14 items.

УДК 004.056

Модель порушника та модель загроз для веб-сервісу QRNG / *Д.М. Моргуль, О.П. Нарєжній, Т.О. Гріненко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2025. Вип. 221. С. 31 – 38.

Квантові генератори випадкових чисел (Quantum Random Number Generators, QRNG), що базуються на фізичних процесах квантової механіки, забезпечують високий рівень ентропії та непередбачуваності, що робить їх перспективним джерелом випадковості для застосування в інформаційно-комунікаційних системах, зокрема в умовах постквантової криптографії.

Однак при використанні QRNG у форматі веб-сервісу (наприклад, через відкриті API або хмарні платформи) виникають нові вектори атак, які можуть порушити довіру до згенерованих даних. У роботі розроблено модель загроз і модель порушника для веб-сервісу QRNG. Методологічну основу дослідження складають сучасні стандарти аналізу ризиків, зокрема ISO/IEC 27005, STRIDE та Common Criteria. Визначені критичні активи системи, класифіковані потенційні загрози з урахуванням специфіки квантової генерації, а також побудований профіль порушника.

Розглянуто типові сценарії атак, включаючи перехоплення випадкових чисел, компрометацію фізичного генератора, атаки на API-сервіс та внутрішнє втручання оператора. Для кожного сценарію здійснена оцінка ризику з урахуванням ймовірності реалізації та можливих наслідків. Запропонований комплекс заходів захисту, що включає технічні (TLS, постобробка, моніторинг), організаційні (розмежування доступу, аудит) та процедурні (реагування на інциденти) рішення.

Результати роботи можуть бути використані для побудови захищених QRNG-сервісів, інтегрованих у критично важливі криптографічні системи, та в якості основи для подальших досліджень при моделюванні безпеки квантових технологій.

Ключові слова: STRIDE; QRNG; веб-сервіс; ентропія; інформаційна безпека; квантовий генератор випадкових чисел; криптографія; модель загроз; модель порушника; постобробка випадковості.

Табл. 4. Іл. 3. Бібліогр.: 14 назв.

UDC 004.056.5:004.8

Digital identity and ZKP: anonymous data and secure authentication / *D.O. Koziuberda, M.V. Yesina, Yu.L. Golikov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2025. No 221. P. 39 – 45.

The article presents a comprehensive analysis of the transition from traditional centralized digital identity models to an innovative decentralized paradigm based on block-chain technologies and zero-knowledge proofs (ZKP). It highlights the fundamental problems of existing systems that rely on centralized registries, passwords, and social logins. Such approaches create significant vulnerabilities, including risks of data breaches, mass surveillance, and manipulation, as centralized intermediaries act as sole controllers of personal information, depriving users of control over their data.

In response to these challenges, the article discusses the concept of Decentralized Identity (DID). This model enables individuals to own, store, and control their digital credentials independently, without involving intermediaries. The key technological components of this ecosystem include Verifiable Credentials (VC), Digital ID Wallets, and Decentralized Identifiers (DID), which are typically stored on a block-chain to ensure immutability and security. A triadic trust model involving the Issuer, Holder, and Verifier is described, allowing data verification without direct contact with the issuing organization.

Special attention is given to the concept of Self-Sovereign Identity (SSI) as a specific philosophy within DID that emphasizes user autonomy, data minimization, and privacy by design. Unlike the broader DID concept, in the SSI model, the user makes the final decision regarding the disclosure of their data.

A central technology ensuring privacy in decentralized systems is zero-knowledge proofs (ZKP). ZKP allow the validation of the truthfulness of a statement without revealing the underlying information. The article provides a detailed analysis of the benefits of using ZKP in the context of DID, including selective attribute disclosure (e.g., proving legal age without revealing the date of birth), minimizing the amount of shared data, preventing correlation and user activity tracking, as well as creating reputation systems that preserve anonymity. Practical application scenarios such as private electronic voting and confidential medical data protection are examined.

The paper also addresses standardization, which is key to ensuring compatibility and widespread adoption of DID solutions. Leading initiatives such as W3C Verifiable Credentials, the Decentralized Identity Foundation (DIF), and projects like Hyperledger Indy and Aries are mentioned. Examples of advanced implementations already in use are provided: Polygon's zkKYC for private verification in DeFi, the Sismo protocol for creating anonymous reputation badges in Web3, and Evernym's SSI platform based on Hyperledger Indy.

In conclusion, it is emphasized that the combination of DID and ZKP forms a new paradigm for digital identity management focused on security and user autonomy. Despite challenges related to usability complexity, key loss risk, and legal uncertainty, the technology is actively evolving and moving from conceptual to practical application, which may eventually become the foundation for a global sovereign digital identity.

Key words: digital identity; verifiable credentials; zero-knowledge proofs; self-sovereign identity; anonymous attestations; authentication; cryptography; decentralized identification; information security.

1 tab. 2 fig. Ref: 7 items.

УДК 004.056.5:004.8

Цифрова ідентичність і ZKP: анонімні дані та безпечна автентифікація / *Д.О. Козюберда, М.В. Єсіна, Ю.Л. Голіков* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2025. Вип. 221. С. 39 – 45.

Представлено комплексний аналіз переходу від традиційних централізованих моделей цифрової ідентичності до інноваційної децентралізованої парадигми, що ґрунтується на технологіях блокчейну та доказах з нульовим розголошенням (ZKP). Висвітлюються фундаментальні проблеми існуючих систем, які покладаються на централізовані реєстри, паролі та соціальні логіни. Такі підходи створюють значні вразливості, зокрема ризики витоку даних, масового стеження та маніпуляцій, оскільки централізовані посередники виступають одноосібними контролерами персональної інформації, позбавляючи користувачів контролю над нею.

Як відповідь на ці виклики, розглядається концепція децентралізованої ідентичності (Decentralized Identity, DID). Ця модель дозволяє індивідам самостійно володіти, зберігати та контролювати свої цифрові атестації без залучення посередників. Ключовими технологічними компонентами цієї екосистеми є посвідчення, що перевіряються (Verifiable Credentials, VC), цифрові гаманці (Digital ID Wallets) та децентралізовані ідентифікатори (DID), які зазвичай зберігаються на блокчейні для забезпечення незмінності та безпеки. Описано тристоронню модель довіри, що включає Емітента (Issuer), Власника (Holder) та Перевіряючого (Verifier), яка дозволяє підтверджувати дані без прямого звернення до організації, що їх видала.

Особливу увагу приділено концепції самосуверенної ідентичності (Self-Sovereign Identity, SSI) як специфічної філософії в межах DID, що ставить максимальний акцент на автономію користувача, мінімізацію даних та конфіденційність за дизайном. На відміну від ширшого поняття DID, у моделі SSI саме користувач ухвалює фінальне рішення щодо передачі своїх даних.

Центральною технологією, що забезпечує приватність у децентралізованих системах, є докази з нульовим розголошенням (ZKP). ZKP дозволяють підтвердити достовірність певного твердження, не розкриваючи саму інформацію, на якій воно ґрунтується. Детально аналізуються переваги використання ZKP в контексті DID, зокрема: вибіркове розкриття атрибутів (наприклад, підтвердження повноліття без розкриття дати народження), мінімізація обсягу переданих даних, запобігання кореляції та відстеження активності користувача, а також створення систем репутації, що зберігають анонімність. Розглянуто практичні сценарії застосування, як-от приватне електронне голосування та захист конфіденційних медичних даних.

Висвітлено питання стандартизації, яка є ключовою для забезпечення сумісності та масового впровадження DID-рішень. Згадано провідні ініціативи, такі як W3C Verifiable Credentials, Decentralized Identity Foundation (DIF) та проєкти Hyperledger Indy та Aries. Наведено приклади передових реалізацій, що вже використовуються на практиці: zkKYC від Polygon для приватної верифікації у DeFi , протокол Sismo для створення анонімних репутаційних бейджів у Web3 та платформа SSI від Evernym, що базується на Hyperledger Indy.

Підкреслюється, що поєднання DID та ZKP формує нову парадигму управління цифровою ідентичністю, орієнтовану на безпеку та автономію користувача. Попри наявність викликів, пов'язаних зі складністю використання, ризиком втрати ключів та правовою невизначеністю, технологія активно розвивається і переходить від концептуального рівня до практичного застосування, що в перспективі може стати основою глобальної суверенної цифрової ідентичності.

Ключові слова: цифрова ідентичність; посвідчення, що перевіряються; доведення з нульовим розголошенням; самосуверенна ідентичність; анонімні атестації; автентифікація; криптографія; децентралізована ідентифікація; інформаційна безпека.

Табл. 1. Іл. 2. Бібліогр.: 7 назв.

UDC 004.056.5

Ensuring data integrity in industrial Internet of Things systems using error-correcting codes / *A.M. Yevheniev, Z.M. Sydorenko, O.V. Sievierinov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2025. No 221. P. 46 – 50.

The article explores the challenges of ensuring data integrity and error resistance in Industrial Internet of Things (IIoT) systems, which are critically important for the functioning of automated manufacturing processes. A comprehensive analysis of key IIoT security issues is presented, along with an overview of current data protection approaches.

The focus is placed on the use of error-correcting codes, particularly Goppa codes, which demonstrate high efficiency in detecting and correcting errors and show strong potential for integration into cryptographic systems. It is shown that Goppa codes can ensure not only error resistance but also data integrity due to the vast number of encoding rules, making them suitable for use in post-quantum cryptography scenarios.

The results demonstrate that using Goppa codes allows for the preservation of data integrity and a significant reduction in the likelihood of introducing false data while maintaining the required level of error resistance. This confirms the feasibility of integrating such codes into the IIoT environment.

Key words: Industrial Internet of Things; IIoT; data integrity; error-correcting coding; Goppa codes; code-based cryptosystems; McEliece; post-quantum cryptography.

2 fig. Ref.: 10 items.

УДК 004.056.5

Забезпечення цілісності даних у системах промислового інтернету речей на основі використання завадостійких кодів / *А.М. Євгеньєв, З.М. Сидоренко, О.В. Сєвєрінов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2025. Вип. 221. С. 46 – 50.

Розглянуто проблеми забезпечення цілісності та завадостійкості даних у системах промислового Інтернету речей (IIoT), що є критично важливим для функціонування автоматизованих виробничих процесів. Проведено аналіз основних проблем безпеки IIoT, здійснено аналіз наявних підходів до захисту даних.

Основну увагу зосереджено на використанні завадостійких кодів, зокрема кодів Гоппи, які мають високу ефективність у виявленні та виправленні помилок, а також на потенціалі до інтеграції в криптографічні системи. Показано, що коди Гоппи здатні забезпечити не лише завадостійкість, а й цілісність інформації завдяки великій кількості правил кодування, що робить їх придатними для застосування в умовах постквантової криптографії.

Результати роботи демонструють можливість забезпечення цілісності даних та зниження ймовірності нав'язування помилкових даних при використанні кодів Гоппи зі збереженням заданих вимог по завадостійкості, що підтверджує доцільність їх впровадження в IIoT-середовище.

Ключові слова: промисловий Інтернет речей; IIoT; цілісність даних; завадостійке кодування; коди Гоппи; кодові криптосистеми; McEliece; постквантова криптографія.

Іл. 2. Бібліогр.: 10 назв.

UDC 004.056.5

The idea of cracking a hash function at quantum speed */ K.Ye. Lysytskyi, I.V. Lysytska, I.M. Galtseva* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2025. No 221. P. 51 – 56.

The scientific article reviews and analyzes the current stage of cryptography development in the context of the inevitable post-quantum era. It is emphasized that post-quantum cryptography (PQC) is gaining the status of a key priority in the national security strategies of the world's leading developed countries, which are actively preparing for a fundamental transition to quantum-safe cryptographic practices. The consequence of the above is the urgent need for intensive development of the latest cryptographic algorithms, which by their nature will be resistant to attacks from powerful quantum computers. Today, several promising approaches to the creation of such quantum-safe algorithms based on various mathematical concepts and cryptographic primitives are already being actively studied. The article pays special attention to cryptography based on hash functions, which is considered one of the most promising areas in the context of developing reliable quantum-safe cryptographic tools. The potential for cracking cryptographic hash functions using quantum algorithms is analyzed. The article considers an original approach to assessing the quantum stability of hash functions, which consists in encoding the hash function itself in a quantum oracle, rather than its separate solution. A simplified (toy) hash function is used to clearly demonstrate the proposed idea. Based on the results of the experimental study, important conclusions are formulated, which indicate that quantum computers are indeed capable of significantly accelerating the process of inversion of cryptographic hash functions. This, in turn, provides strong grounds for serious concern about the cryptographic stability of various cryptographic primitives based on combinatorial problems. It is worth emphasizing that this problem is not limited to hash functions. This critically important observation means that to maintain a similar level of cryptographic security in the coming quantum era, the size of the input value of hash functions will likely need to be increased by at least half to compensate for the speedup provided by quantum algorithms.

Key words: cybersecurity; cryptography; quantum computing; Grover's algorithm; hash function; post-quantum cryptography; quantum security; quantum attacks.

2 fig. Ref.: 11 items.

УДК 004.056.5

Ідея зламу геш-функції на квантовій швидкості / *К.Є. Лисицький, І.В. Лисицька, І.М. Гальцева* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2025. Вип. 221. С. 51 – 56.

Здійснено огляд та аналіз актуального етапу розвитку криптографії в контексті неминучої постквантової епохи. Підкреслено, що постквантова криптографія (PQC) набуває статусу ключового пріоритету в стратегіях національної безпеки провідних розвинених держав світу, які активно готуються до фундаментального переходу на квантово-безпечні криптографічні практики. Наслідком зазначеного є нагальна необхідність інтенсивної розробки новітніх криптографічних алгоритмів, які за своєю природою будуть стійкими до атак з боку потужних квантових обчислювальних машин. На сьогодні вже активно досліджуються декілька перспективних підходів до створення таких квантово-безпечних алгоритмів, що базуються на різних математичних концепціях та криптографічних примітивах. Особливу увагу приділено криптографії на основі геш-функцій, яка розглядається як один із найбільш перспективних напрямків у контексті розбудови надійних квантово-безпечних криптогра-

фічних засобів. Проведено аналіз потенційної можливості зламу криптографічних геш-функцій з використанням квантових алгоритмів. Розглядається оригінальний підхід до оцінки квантової стійкості геш-функцій, який полягає у кодуванні самої геш-функції в квантовому оракулі, а не її окремого рішення. Для наочної демонстрації запропонованої ідеї використовується спрощена (toy) геш-функція. За результатами експериментального дослідження сформульовано важливі висновки, які свідчать, що квантові комп'ютери дійсно здатні значно прискорити процес інверсії криптографічних геш-функцій. Це, в свою чергу, надає вагомі підстави для серйозного занепокоєння щодо криптографічної стійкості різноманітних криптографічних примітивів, в основі яких лежать комбінаторні задачі. Варто наголосити, що ця проблема не обмежується лише геш-функціями. Це критично важливе спостереження означає, що для підтримки аналогічного рівня криптографічної безпеки в майбутню квантову еру розмір вихідного значення геш-функцій, ймовірно, знадобиться збільшити щонайменше вдвічі, щоб компенсувати прискорення, яке забезпечують квантові алгоритми.

Ключові слова: кібербезпека; криптографія; квантові обчислення; алгоритм Гровера; геш-функція; постквантова криптографія; квантова безпека; квантові атаки.

Іл. 2. Бібліогр.: 11 назв.

UDC 004.056.5

Using intel virtualization technologies to create information protection systems based on an open portable trusted execution environment (OP-TEE) / *P.V. Shulik, O.I. Fediushyn, D.O. Viukhin, O.Y. Morozov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2025. No 221. P. 57 – 61.

The purpose of the article is to create an information security system based on the integration of the OP-TEE framework with Intel-x86 platforms using virtualization technologies. The subject of the study is software tools for integrating the OP-TEE framework with the Intel-x86.

The solution proposed in the article is based on the isolation of the secure world into a separate virtual machine. Hardware support is also based on the Intel x86 VT-x, but secure world exists entirely in a separate virtual machine. Thus, we have two virtual machines - one for the normal world, where the main operating system is running, and the second virtual machine for the OP-TEE. The ACRN is used as a hypervisor.

The article will be useful to specialists in the field of the information security, dealing with data protection in the operating systems of computer systems.

Key words: OP-TEE; Intel x86; hypervisor; ARM Trust Zone.

4 fig. Ref.: 9 items.

УДК 004.056.5

Використання технологій віртуалізації intel для створення систем захисту інформації на базі open portable trusted execution environment (OP-TEE) / *П.В. Шулік, О.І. Федюшин, Д.О. В'юхін, О.Ю. Морозов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2025. Вип. 221. С. 57 – 61.

Метою статті є створення системи захисту інформації на основі інтеграції OP-TEE фреймворка з Intel-x86 платформами з використанням технологій віртуалізації. Предметом дослідження є програмні засоби інтеграції OP-TEE фреймворка з Intel-x86.

Запропоноване в роботі рішення базується на ізоляції secure world в окрему віртуальну машину. Апаратна підтримка теж базується на Intel x86 VT-x, але secure world існує повністю в окремій віртуальний машині.Таким чином ми маємо дві віртуальні машини – одна для normal world, де виконується основна операційна система, а друга віртуальна машина для OP-TEE. У якості гіпервізора використовуються гіпервізор ACRN.

Стаття буде корисною фахівцям у галузі інформаційної безпеки, які займаються питаннями захисту даних в операційних системах комп'ютерних систем.

Ключові слова: OP-TEE; Intel x86; гіпервайзор; ARM Trust Zone.

Іл. 4. Бібліогр.: 9 назв.

UDC 004.056.5

Analysis of cryptographic providers usage in the TLS Protocol / *A.A. Telnova, D.S. Balagura, V.O. Frolenko, V.M. Sukhoteplyi, S.V. Florov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2025. No 221. P. 62 – 71.

The relevance of this work lies in the need to identify optimal implementations of cryptographic protocols depending on the conditions under which the TLS protocol is used. It is known that the TLS is utilized in various software products, across different platforms and operating systems. Therefore, it is not always feasible to rely on a single cryptographic provider or library to perform cryptographic operations and manage keys.

The goal of this study is to analyze the efficiency of cryptographic providers in the TLS protocol and to identify the features that influence their selection and usage based on specific implementation environments and protocol operation aspects.

As part of the research, a comparative analysis was conducted on cryptographic provider implementations, including OpenSSL, BoringSSL, and various versions of CryptoAPI. Based on the results of the analysis, recommendations were formulated on the feasibility of using certain cryptographic providers in TLS implementations.

Key words: TLS protocol; cryptographic provider; OpenSSL; BoringSSL; Crypto API.

2 tab. 1 fig. Ref.: 21 items.

УДК 004.056.5

Аналіз використання криптопровайдерів у протоколі TLS / *А.А. Тельнова, Д.С. Балагура, В.О. Фроленко, В.М. Сухотеплий, С.В. Флоров* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2025. Вип. 221. С. 62 – 71.

Актуальність цієї роботи полягає у необхідності визначення оптимальних реалізацій криптографічних протоколів залежно від умов, у яких функціонує імплементація протоколу TLS. Відомо, що TLS використовується в різноманітних програмних продуктах, на різних платформах та операційних системах. У зв'язку з цим не завжди можливо застосовувати єдиний криптопровайдер або криптобібліотеку для реалізації криптографічних перетворень та управління ключами.

Метою роботи є аналіз ефективності функціонування криптопровайдерів у протоколі TLS, а також виявлення їх особливостей, що впливають на вибір та використання в залежності від специфіки середовища та аспектів реалізації протоколу.

У рамках дослідження проведено порівняльний аналіз реалізацій криптографічних провайдерів, зокрема OpenSSL, BoringSSL та CryptoAPI різних версій. На основі результатів аналізу сформульовано рекомендації щодо доцільності використання тих чи інших криптографічних провайдерів у реалізаціях TLS.

Ключові слова: протокол TLS; криптографічний провайдер; OpenSSL; BoringSSL; Crypto API.

Табл. 2. Іл. 1. Бібліогр.: 21 назв.

UDC 621.391:519.2

Cryptographic competitiveness of cryptosystems based on noncommutative groups / *Y.V. Kotukh, G.Z. Khalimov, I.Y.Dzhura* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2025. No 221. P. 72 – 82.

The rapid development of quantum computing poses a direct threat to RSA, DSA, and ECC modern cryptographic systems due to the Shor's algorithm potential application. In response to this threat, the NIST is conducting post-quantum cryptography standardization, having selected lattice-based and hash-function-based algorithms in 2022. Cryptosystems based on noncommutative groups, despite their potential resistance to quantum attacks owing to natural properties of noncommutative algebraic structures, were not included in the first set of standards due to the complexity of security analysis. This research conducts a comprehensive analysis of the cryptographic competitiveness of noncommutative group-based systems, evaluates their advantages and disadvantages compared to existing post-quantum solutions, and determines prospects for practical application as an alternative or complementary solution to ensure cryptographic diversification under quantum threats.

Key words: post-quantum cryptography; noncommutative groups; MST3; logarifmic signature; quantum computing; cryptographic security.

Tab. 1. Ref: 30 items.

УДК 004.056.55

Криптографічна конкурентоспроможність криптосистем на основі некомутативних груп / *Є.В. Котух, Г.З. Халімов, І.Є. Джура* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2025. Вип. 221. С. 72 – 82.

Стрімкий розвиток квантових обчислень створює пряму загрозу для сучасних криптографічних систем RSA, DSA та ECC через можливість застосування алгоритму Шора. У відповідь на цю загрозу NIST проводить стандартизацію постквантової криптографії, обравши у 2022 р. алгоритми на основі решіток та геш-функцій. Криптосистеми на некомутативних групах, попри їх потенційну стійкість до квантових атак завдяки природним властивостям некомутативних алгебраїчних структур, не увійшли до першого набору стандартів через складність аналізу безпеки. Дослідження здійснює комплексний аналіз криптографічної конкурентоспроможності систем на основі некомутативних груп, оцінює їх переваги і недоліки порівняно з існуючими постквантовими рішеннями та визначає перспективи практичного застосування як альтернативного або доповнюючого рішення для забезпечення криптографічної диверсифікації в умовах квантової загрози.

Ключові слова: постквантова криптографія; некомутативні групи; MST3; логаріфмічний підпис; квантові обчислення; криптографічна стійкість.

Табл. 1. Бібліогр.: 30 назв.

INFORMATION TECHNOLOGY
ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

UDC 621.372(075)

Integration of cloud services for storage and processing of cryomicroscopic images: practical experience using MINIO and CVAT / *Yu.V. Samokhin, O.G. Avrunin* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2025. No 221. P. 83 – 88.

In modern biomedical science, the efficient processing of large volumes of visual data is critically important for analyzing cellular structures. This abstract describes practical experience integrating the MinIO and CVAT cloud

services to automate the processes of storage, annotation, and analysis of cryo-microscopy images. The application of these tools enhances the accuracy of cell segmentation, ensures scalability, and improves the reproducibility of research.

Cryo-microscopy is a powerful method for visualizing biological samples at the nanoscale. However, processing the resulting images requires significant computational resources and effective tools for data storage and analysis. Integrating cloud services, such as the MinIO for data storage and the CVAT for annotation, optimizes these processes.

Cryo-microscopy images were collected from various sources and stored in the MinIO cloud storage, providing reliable and scalable access to the data. The CVAT tool was used for precise delineation of cellular structures. The annotation process involved manual or semi-automatic marking of regions of interest in the images, which is critically important for training artificial intelligence models. The annotated images were prepared for training deep learning models, such as the U-Net and Mask R-CNN, which have proven effective in image segmentation tasks. The models were trained on the annotated data using the TensorFlow and PyTorch libraries. After training, the models were applied to automatic segmentation of new cryo-microscopy images. The inference results were compared with manual annotations to assess the accuracy and reliability of the models.

Integration with the Jupyter Notebook enabled researchers to interactively analyze inference results and generate analytical reports. Integrating the MinIO and CVAT cloud services into the cryo-microscopy image processing workflow significantly enhances the efficiency and accuracy of cellular structure analysis. The use of modern technologies and tools facilitates the process automation, ensures scalability and reproducibility of research, which is an important step in advancing biomedical research and improving diagnostics.

Key words: cryomicroscopy; image processing; human health; segmentation; cloud services.

2 fig. Ref: 12 items.

УДК 621.372(075)

Інтеграція хмарних сервісів для зберігання та обробки кріомікроскопічних зображень: практичний досвід використання MINIO та CVAT / *Ю.В. Самохін, О.Г Аврунін* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2025. Вип. 221. С. 83– 88.

У сучасній біомедичній науці ефективна обробка великих обсягів візуальних даних є критично важливою для аналізу клітинних структур. У статті описано практичний досвід інтеграції хмарних сервісів MinIO та CVAT для автоматизації процесів зберігання, анотації та аналізу кріомікроскопічних зображень. Застосування цих інструментів дозволяє підвищити точність сегментації клітин, забезпечити масштабованість та відтворюваність досліджень.

Кріомікроскопія є потужним методом візуалізації біологічних зразків на нанорівні. Однак обробка отриманих зображень вимагає значних обчислювальних ресурсів та ефективних інструментів для зберігання та аналізу даних. Інтеграція хмарних сервісів, таких як MinIO для зберігання даних та CVAT для анотації, дозволяє оптимізувати ці процеси.

Кріомікроскопічні зображення було зібрано з різних джерел та збережено у хмарному сховищі MinIO, що забезпечує надійний та масштабований доступ до даних. Для точного виділення клітинних структур використовувався інструмент CVAT. Процес анотації включав ручне або напівавтоматичне позначення областей інтересу на зображеннях, що є критично важливим для навчання моделей штучного інтелекту. Розмічені зображення були підготовлені для навчання моделей глибокого навчання, таких як U-Net та Mask R-CNN, які зарекомендували себе в задачах сегментації зображень. Моделі навчались на розмічених даних з використанням бібліотек TensorFlow та PyTorch. Після навчання моделі застосовувались для автоматичної сегментації нових кріомікроскопічних зображень. Результати інференсу порівнювались з ручними анотаціями для оцінки точності та надійності моделей. Інтеграція з Jupyter Notebook дозволила дослідникам інтерактивно аналізувати результати інференсу та будувати аналітичні звіти.

Інтеграція хмарних сервісів MinIO та CVAT у процес обробки кріомікроскопічних зображень дозволяє значно підвищити ефективність та точність аналізу клітинних структур. Використання сучасних технологій та інструментів сприяє автоматизації процесів, забезпечує масштабованість та відтворюваність досліджень, що є важливим кроком у розвитку біомедичних досліджень та покращенні діагностики.

Ключові слова: кріомікроскопія; обробка зображень; здоров'я людини; сегментація; хмарні сервіси.

Іл. 2. Бібліогр.: 12 назв.

RADIO ELECTRONIC SYSTEMS
РАДІОЕЛЕКТРОННІ СИСТЕМИ

UDC 007.51

Features of constructing an algorithm for the cycle between stage-by-stage situational control of conflict interaction of the ground-based RES complex with small (light) drones / *V.M. Kantsedal, A.A. Mogyla* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2025. No 221. P. 89 – 106.

An informative description provides the structure and features of the construction of the cycle algorithm between the staged situational control of the ground-based RES complex within the framework of a simplified two-way dynamic model of conflict interaction of the components of multifunctional structures of a small (light) tactical-level UAV and a

single-purpose ground-based RES complex when protecting an important infrastructure facility for scenarios of controlled or autonomous UAV flights in conditions of a shortage of counteraction time.

The algorithm prepares the conditions for coordination for the effective solution of functional tasks of intra-stage situational management with the maximum values of the probabilities of their successful solution in the sequence of stages of conflict resolution in favor of the RES complex, and also optimizes the solution of the tasks of the cycle of coordination of the interaction of these stages in order to achieve the Main goal of management - the maximum probability of protecting an important object. This is achieved by managing the dynamic state of a conflict situation in a preformed sequence of purposeful stages, coordinated by goals, conditions of observation and suppression, synchronized in time of statements and solutions of the tasks of the cycle of coordination of the interaction of the stages of the functioning of the RES complex when they change through the synergy of these processes and their results and quick and flexible reconfiguration of its structure.

The peculiarities of constructing the algorithm lie in the characteristics of the interaction capability during the working time interval of the complex of reconnaissance and suppression means for increasing efforts during stage changes with combinations of various types of point interference for signal and covert information suppression of UAVs as intelligence information about its signatures accumulates and arrives, as well as in the technological features of its implementation.

Despite the significant impact of the above technological features of the algorithm on its controllability and effectiveness, the algorithm has certain limitations. They are due to the physical properties of the RES complex, which lead to a short operating time of the complex and an impact only on the composition of suppression objects in the UAV structure. The structure of the ground-based RES complex needs to be modernized, e.g., by including a tethered balloon in its composition, which leads to achieving potential effectiveness in countering various types of tactical-level UAVs due to a significant expansion of the complex's functional capabilities with an increased duration of its operating time, the emergence of new reconnaissance and suppression objects in new counteraction conditions, where the entire structure of a small unmanned system is used, previously inaccessible to the ground-based RES complex.

Key words: unmanned aircraft system; radio electronic suppression; reconnaissance means; suppression means; situational management; general performance characteristics; coordination; formalization.

1 fig. Ref: 18 items.

УДК 007.51

Особливості побудови алгоритму циклу міжетапного ситуаційного управління конфліктною взаємодією наземного комплексу РЕП з малими (легкими) безпілотниками / *В.М. Канцедал, А.А. Могила* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2025. Вип. 221. С. 89 – 106.

Надано інформаційний опис структури та особливостей побудови алгоритму циклу міжетапного ситуаційного управління наземним комплексом РЕП у рамках спрощеної двосторонньої динамічної моделі конфліктної взаємодії складових частин багатофункціональних структур малого (легкого) БПЛА тактичного рівня та одноцільового наземного комплексу РЕП при захисті важливого інфраструктурного об'єкта для сценаріїв керованого або автономного польотів БПЛА в умовах дефіциту часу протидії.

Алгоритм готує умови узгодження для ефективного вирішення функціональних завдань внутрішньо етапного ситуаційного управління з максимальними значеннями ймовірностей успішного їх вирішення на послідовності етапів вирішення конфлікту на користь комплексу РЕП, а також оптимізує вирішення завдань циклу координації взаємодії цих етапів з метою досягнення Головної мети управління – максимуму ймовірності захисту важливого об'єкта. Це досягається при управлінні динамічним станом конфліктної ситуації на заздалегідь сформованої послідовності цілеспрямованих етапів, узгоджених за цілями, умовами спостереження та придушення, синхронізованих у часі постановок та розв'язань завдань циклу координації взаємодії етапів функціонування комплексу РЕП при їх зміні через синергію цих процесів і їх результатів та швидку і гнучку реконфігурацію його структури.

Особливості побудови алгоритму криються у характеристиках спроможності взаємодії на інтервалі робочого часу комплексу засобів розвідки і придушення для нарощування зусиль за зміни етапів комбінаціями різних видів точкових завад для сигнального і прихованого інформаційного придушення БПЛА у міру накопичення та надходження розвідувальної інформації щодо його сигнатур, а також у технологічних особливостях його реалізації.

Незважаючи на суттєвий вплив наведених технологічних особливостей алгоритму на його керованість і результативність, алгоритм має певні обмеження. Вони зумовлені фізичними властивостями комплексу РЕП, що призводять до малої тривалості робочого часу комплексу та впливу тільки на склад об'єктів придушення в структурі БПЛА. Потрібна модернізація структури наземного комплексу РЕП, наприклад включенням до його складу прив'язного аеростату, що веде до досягнення потенційної результативності протидії різним типам БПЛА тактичного рівня за рахунок суттєвого розширення функціональних можливостей комплексу при збільшеній тривалості його робочого часу, появі нових об'єктів розвідки та придушення в нових умовах протидії, де використовується вся структура малої безпілотної системи, яка раніше була недоступна наземному комплексу РЕП.

Ключові слова: безпілотна авіаційна система; радіоелектронне придушення; засоби розвідки; засоби придушення; ситуаційне управління; загальні ТТХ; координація; формалізація.

Іл. 1. Бібліогр.: 18 назв.

PHYSICS OF DEVICES, ELEMENTS AND SYSTEMS
ФІЗИКА ПРИЛАДІВ, ЕЛЕМЕНТІВ І СИСТЕМ

UDC 621.383.5

Development and analysis of mathematical models for photovoltaic converters of solar batteries for avionics systems / *O.D. Meniailo, O.V. Grigorieva, V.G. Makhonin* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2025. No 221. P. 107 – 112.

The paper considers methods for applying mathematical models of photoconverter parameters to the design and development of technical equipment for receiving, converting and storing solar energy.

Considerable attention is paid to determining the optimal power point, and therefore the optimal operating mode of the photovoltaic converter, which, in turn, requires knowledge of its volt-ampere characteristics. For this purpose, the characteristics of the converters were simulated using both certain empirical data and analytical relationships obtained using the equivalent circuit of the photoelectric converter.

The paper presents both theoretical relationships of the photoelectric converters parameters and the results of experimental studies of the characteristics dependence on temperature and illumination level.

The high correspondence of the mathematical models to the experimental data was confirmed. The developed models demonstrated their adequacy to temperatures of the order of –50 °C. Ways of possible extrapolation of the characteristics to even lower temperatures are shown. In this case, it is recommended to use special measures, the simplest of which may be, for example, the use of a special linear or fragmentary-linear function.

Key words: solar energy; photovoltaic converters; equivalent circuit; voltage-current characteristic; mathematical model.

6 fig. Ref: 12 items.

УДК 621.383.5

Розробка та аналіз математичних моделей фотоелектричних перетворювачів сонячних батарей систем авіоніки / *О.Д. Меняйло, О.В. Григор'єва, В.Г. Махонін* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2025. Вип. 221. С. 107 – 112.

Розглянуто методи застосування математичних моделей параметрів фотоперетворювачів при проєктуванні та розробці технічного обладнання для прийому, перетворення та накопичення енергії сонця.

Значну увагу приділено визначенню точки оптимальної потужності, а значить і оптимального режиму роботи фотоелектричного перетворювача, що, в свою чергу, потребує знання його вольтамперних характеристик. З цією метою проведено моделювання характеристик перетворювачів як з застосуванням певних емпіричних даних, так і аналітичних співвідношень, одержаних з використанням схеми заміщення фотоелектричного перетворювача.

Наведено як теоретичні співвідношення параметрів фотоелектричних перетворювачів, так і результати експериментальних досліджень залежностей характеристик від температури та рівня освітленості.

Підтверджено високу відповідність математичних моделей експериментальним даним. Розроблені моделі продемонстрували свою адекватність до температур порядку –50 °С. Показано шляхи можливої екстраполяції характеристики до ще більш низьких температур. Рекомендовано вживати спеціальні заходи, з яких найбільш простим в реалізації може бути, наприклад, застосування спеціальної лінійної або фрагментарно-лінійної функції.

Ключові слова: сонячна енергія; фотоелектричні перетворювачі; схема заміщення; вольтамперна характеристика; математична модель.

Іл. 6. Бібліогр.: 12 назв.

UDC 621.385

Architecture of the TULIPgm program system for designing vacuum amplifiers and generators of microwave range / *I.M. Bondarenko, O.S. Hnatenko, A.V. Gritsunov, O.G. Pashchenko, V.P. Karnaushenko, M.A. Kopot* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2025. No 221. P. 113 – 126.

The article contains an analysis of the architecture and capabilities of a specialized software system (application package) designed for calculations and optimization of parameters and characteristics of powerful vacuum microwave devices that can be used in countermeasure systems for small and medium-sized unmanned aerial vehicles, as well as in other applications where the generation of high-intensity electromagnetic microwave pulses is required. The TULIPgm software package is designed for non-stationary and spectral modeling of microwave devices using the particle-in-cell (PIC) method. It was developed as a full-format two-dimensional PIC code for studying transient processes in amplitrons. Currently, the set of simulated devices has been expanded to include magnetrons, forward and reverse wave amplifiers with an injected beam and crossed fields. The system implements a spectral approach that allows studying the passage of a signal with an arbitrary spectrum through an amplifier and obtaining continuous spectra of the output parameters of the device. The main architectural, algorithmic, software and interface features of the system are considered. Among them, the most important are the division of the program structure and computational process into logical and physical parts; the mechanism of excitation and event processing; the assembly of the software system using prob-

lem-oriented binary keys, etc. Information connections within the system and with auxiliary and service programs are implemented on the basis of a single global data structure. Examples of the use of the TULIPgm code are given. Among the prospects for the development of the system, the implementation of a three-dimensional model of devices with crossed fields, the implementation of a spectral approach for LBVs and klystrons, as well as the introduction of algorithms based on direct integration of Maxwell's equations by the finite difference method for modeling relativistic magnetrons are noted.

Key words: computer simulations; microwave device; program system architecture; signal spectrum; transient process.

6 fig. Ref: 24 items.

УДК 621.385

Архітектура програмної системи TULIPgm для проєктування вакуумних підсилювачів і генераторів НВЧ-діапазону / *І.М. Бондаренко, О.С. Гнатенко, О.В. Грицунов, О.Г. Пащенко, В.П. Карнаушенко, М.А. Копоть* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2025. Вип. 221. С. 113 – 126.

Міститься аналіз архітектури та можливостей спеціалізованої програмної системи (пакета прикладних програм), призначеної для розрахунків та оптимізації параметрів і характеристик потужних вакуумних НВЧ приладів, що можуть бути використані в системах протидії малим та середнім безпілотним літальним апаратам, а також в інших застосуваннях, де потрібна генерація електромагнітних НВЧ імпульсів великої інтенсивності. Програмний комплекс TULIPgm призначено для нестаціонарного та спектрального моделювання НВЧ приладів методом «частка в комірці» (PIC). Він розроблявся як повноформатний двовимірний PIC-код для дослідження перехідних процесів в амплітронах. На цей час набір приладів, що моделюються, розширено магнетронами, підсилювачами прямої та зворотної хвилі з інжектованим променем та схрещеними полями. У системі реалізовано спектральний підхід, який дозволяє досліджувати проходження сигналу з довільним спектром через підсилювач та отримувати континуальні спектри вихідних параметрів приладу. Розглянуто основні архітектурні, алгоритмічні, програмні та інтерфейсні особливості системи. Серед них найважливішими є поділ структури програми та обчислювального процесу на логічну та фізичну частини; механізм збудження та обробки подій; збірка програмної системи за допомогою проблемно-орієнтованих бінарних ключів та ін. Інформаційні зв’язки всередині системи та з допоміжними і сервісними програмами реалізовано на основі єдиної глобальної структури даних. Наведено приклади застосування коду TULIPgm. Серед перспектив розвитку системи зазначається імплементація тривимірної моделі приладів зі схрещеними полями, реалізація спектрального підходу для ЛБВ і клістронів, а також впровадження алгоритмів, заснованих на безпосередньому інтегруванні рівнянь Максвелла методом скінчених різниць, для моделювання релятивістських магнетронів.

Ключові слова: комп’ютерне моделювання; НВЧ прилад; архітектура програмної системи; спектр сигналу; перехідний процес.

Іл. 6. Бібліогр.: 24 назв.

COLLECTION OF SCIENTIFIC PAPERS
RADIOTEKHNIKA
Issue 221
In English and Ukrainian

ЗБІРНИК НАУКОВИХ ПРАЦЬ
РАДІОТЕХНІКА
Випуск 221
Англійською та українською мовами

Коректор Л.І. Сащенко

.

Підп. до друку 25.06.2025. Формат 60x90/8. Папір офсет. Гарнітура Таймс. Друк. ризограф.
Ум. друк. арк**.** 11,3. Обл.-вид. арк. 10,2 Тираж 300 прим. Зам. № 182. Ціна договір.

Харківський національний університет радіоелектроніки (ХНУРЕ)
Просп. Науки, 14, Харків, 61166.

Оригінал-макет підготовлено і збірник надруковано у ПФ „Колегіум”,
Свідоцтво про внесення суб’єкта видавничої діяльності до Державного реєстру видавців.
Сер. ДК №1722 від 23.03.2004.