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 1 3

Kharkiv
Kharkiv National
University of Radio Electronics
2023

**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: 171 – Electronics; 172 – Telecommunications and Radio Engineering; 173 – Avionics; 125 – Cybersecurity; 151 – Automation and Computer-Integrated Technologies; 152 – Metrology and Information-Measuring Equipment; 153 – Micro- and Nanosystem Technology; 163 – Biomedical Engineering; 105 – Applied Physics and Nanomaterials.

Website: rt.nure.ua

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

The authors are responsible for the content of the article.

## Editorial Team



## Members of the editorial board of foreign scientific institutions and educational institutions



Responsible for the issue: *I.V. Svyd, 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 16.06.2023.

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 1 3

Харків
Харківський національний
університет радіоелектроніки
2023

**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: 171 – Електроніка; 172 – Телекомунікації та радіотехніка; 173 – Авіоніка; 125 – Кібербезпека; 151 – Автоматизація та комп'ютерно-інтегровані технології; 152 – Метрологія та інформаційно-вимірювальна техніка; 153 – Мікро- та наносистемна техніка; 163 – Біомедична інженерія; 105 – Прикладна фізика та наноматеріали.

Сайт: rt.nure.ua

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

За зміст статті відповідальні автори.



Відповідальні за випуск: *І.В. Свид, 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 16.06. 2023.

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

# CONTENT

## SYSTEMS AND METHODS OF INFORMATION PROTECTION



## PHYSICS OF DEVICES, ELEMENTS AND SYSTEMS



## INFORMATION METHODS OF RADIO ENGINEERING, SIGNAL PROCESSING



## RADAR AND RADIONAVIGATION

# ЗМІСТ

## СИСТЕМИ І МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ



## ФІЗИКА ПРИЛАДІВ, ЕЛЕМЕНТІВ І СИСТЕМ



## ІНФОРМАЦІЙНІ МЕТОДИ РАДІОТЕХНІКИ, ОБРОБКА СИГНАЛІВ



## РАДІОЛОКАЦІЯ І РАДІОНАВІГАЦІЯ

**УДК 004.056.5** **DOI:10.30837/rt.2023.2.213.01**

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

# КРИПТОГРАФІЯ НА ОСНОВІ ГЕШУ, ЇЇ ЗАХИЩЕНІСТЬ ТА ДОЦІЛЬНІСТЬ ЗАСТОСУВАННЯ У СУЧАСНИХ КРИПТОСИСТЕМАХ

## Вступ

ЕП на основі гешу є одним із найбільш перспективних класів криптографічних схем, які вважаються квантово стійкими. Стійкість криптографічних геш функцій є одним з найважливіших аспектів забезпечення захищеності схем на основі гешу, тому для таких функцій вимагається наявність стійкості до відновлення першого та другого прообразу, а також стійкість до колізій.

Зазвичай виділяють три категорії цифрових підписів на основі гешу: одноразові підписи (OTS), де будь-який ключ підпису слід використовувати не більше одного разу; багаторазові підписи (MTS), які поєднують кілька екземплярів OTS, щоб забезпечити обмежену кількість підписів; декількаразові підписи (FTS), у яких безпека однієї пари ключів повільно знижується з кількістю використань.

Оскільки класичні ЕП на основі гешу вимагають відстеження кількості використаних підписів, довгий час вони вважалися такими, що мають стан. Це обмеження було подолано схемою SPHINCS, яку згодом було вдосконалено до SPHINCS+.

У роботі наводиться оцінка захищеності ЕП на геш функціях відносно атак бічними каналами. Також у роботі проводиться аналіз рекомендацій щодо використання одного з кандидатів конкурсу NIST, який базується на геш криптографії – SPHINCS+, і робляться висновки щодо доцільності його використання.

## 1. Оцінка захищеності ЕП на основі гешу відносно атак бічними каналами

### 1.1. Припущення при аналізі бічних каналів

Для забезпечення аналізу бічних каналів незалежно від фактичної реалізації робляться наступні припущення [1]:

1. Припускається, що атакована реалізація використовує PRNG для створення ключів підпису W-OTS+ на льоту під час створення підпису та обчислення шляху автентифікації.

2. Припускається, що як реалізація PRNG, так і односпрямована функція взагалі не мають витоку бічним каналом (у наступних пунктах буде розглянуто, де саме застосовуються ВЧ у реалізації геш алгоритму SPHINCS+).

### 1.2. W-OTS+

*Часові бічні канали.*

Єдиними секретними даними, які обробляються в W-OTS+, є частини приватного ключа $x_i$. На рис. 1 показані актуальні для аналізу бічних каналів частини W-OTS+.

$x_i$ використовуються лише як вхідні дані для ланцюгової функції $c_k$. Ланцюгова функція застосовує геш функцію $f_k$ кілька разів до частин приватного ключа $x_i$. Під час генерації ключа кількість геш викликів є фіксованою ($w-1$), а під час генерації підпису кількість геш викликів залежить виключно від блоків повідомлень ($b_i$) [2]. Блоки $b_i$ залежать лише від геш значення, яке не представляє інтересу для потенційного зловмисника. Згідно з припущен-

ням 1, сама геш функція не містить часового бічного каналу, отже, оцінка $c_k(x_i, r)$ не може спричинити витік по часу інформації щодо $x_i$.

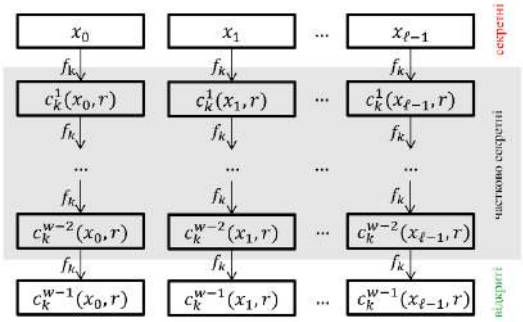


Рис. 1. Частини W-OTS, актуальні для аналізу бічних каналів

Якщо $b_i = 0$, це означає, що зловмисник знає частину приватного ключа, проте навіть якщо все геш значення повідомлення, яке підписується, дорівнюватиме 0, контрольна сума все одно гарантуватиме, що деякі $b_i$ більші за нуль.

Отже, часовий бічний канал в W-OTS+ можна використовувати лише для вилучення інформації про $b_i$-ті, яку зловмисник або вже знає (атака з відомим повідомленням), або обирає сам (атака з обраним повідомленням).

*Бічні канали потужності.*

Цікавою функцією в W-OTS+ є ланцюгова функція:

$$00 \tag{1}$$

Така функція здається ідеальним варіантом для аналізу потужності, тому що для $i = 1$ підписувач обчислює $x \oplus r$, де $x$ – деякий блок приватного ключа, а $r_i$ – бітова маска рандомізації, відома верифікатору та зловмиснику. Однак ця функція викликається лише двічі: один раз під час генерації ключа та один раз під час генерації підпису. Крім того, $r_i$ є однаковим для обох оцінок. Це запобігає диференціальним атакам, таким як DPA, які покладаються на різні вхідні дані атакованого примітиву. Крім того, атаки SPA можуть у найкращому випадку відновити HW (Вагу Хемінга) оброблених значень. Формула середнього витоку таким чином матиме наступний вигляд [1]:

$$leak_{avg} = \sum_{i=0}^{8} \frac{1}{256} \binom{8}{i} \left( 8 - \log_2 \binom{8}{i} \right) = 2.5 bits \,. \tag{2}$$

Крім того, якщо станеться витік ваги Хеммінга лише 32-розрядних слів, що більш імовірно, витік зменшиться приблизно до 3,5 бітів на слово, тобто 28 бітів на 256-бітний ключ.

### 1.3. XMSS

*Часові бічні канали.*

В попередньому пункті зроблено висновок, що W-OTS+ не спричиняє витоку жодної інформації про частини приватного ключа через часові бічні канали. Оскільки XMSS побудовано з використанням багатьох ключів W-OTS+, XMSS також забезпечує цю стійкість.

Актуальні для аналізу частини показано на рис. 2, до них відносяться початкове значення (seed), яке використовується для псевдовипадкової генерації приватного ключа W-OTS+, і сам приватний ключ W-OTS+.

Таким чином, приватний ключ у XMSS або складається з багатьох приватних ключів W-OTS+, або з випадкового початкового числа, яке використовується для їх створення [3]. При використанні першого варіанту стійкість часового каналу XMSS безпосередньо випли-

ває зі стійкості W-OTS+. При використанні останнього варіанту також потрібно зробити припущення, що PRNG не спричиняє витоку про випадкове початкове число [1]. Це гарантує, що принаймні W-OTS+ частина генерації підпису і обчислення відкритого ключа XMSS не має часового бічного каналу, який можна використовувати.

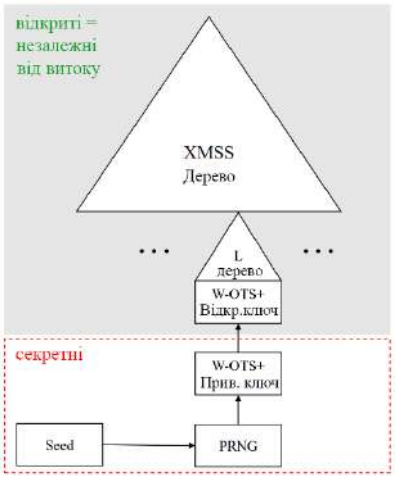


Рис. 2. Частини XMSS, які підходять для аналізу бічних каналів

*Бічні канали потужності.*

Стійкість W-OTS+ до бічних каналів потужності не означає стійкість XMSS, оскільки у XMSS генерація ключа W-OTS+ викликається набагато частіше під час обчислення шляху автентифікації.

Нехай дерево XMSS має висоту $H$, тобто має $2^H$ листів. Для підпису з використанням приватного ключа W-OTS+ з індексом $s$ підписувачу потрібно спочатку обчислити підпис W-OTS+ за допомогою $sk_{OTS,s}$, а потім – шлях автентифікації для $v_0[s]$. Якщо припустити, що підписувач взагалі не використовує вузли повторно, знаємо, що під час генерації підпису для індексу $s$, $sk_{OTS,s}$ вже витікав кілька разів раніше. Витік відбувся один раз під час початкової генерації ключа та один раз для кожного підпису, який був створений раніше, що означає, що включно з поточним витоком він витік $s+2$ рази, а також витік буде відбуватися для всіх генерацій підпису в майбутньому ($2^H+1$ разів, якщо використовуються всі ключі).

У випадку реальної моделі витоку атака стає нездійсненною: під час кожної генерації підпису ланцюгова функція W-OTS+ викликається з абсолютно однаковими вхідними даними для створення однакових відкритих ключів W-OTS+. Зловмисник не може сподіватися відновити більше, ніж вагу Хеммінга кожного проміжного результату [1].

Згідно з представленими припущеннями, W-OTS+ і XMSS забезпечують сильну стійкість щодо атак бічними каналами. Показано, що W-OTS+ стійкий до більшості атак через його одноразовий характер, що обмежує кількість слідів, які можна отримати. Ця стійкість послаблюється генерацією ключів на льоту в XMSS. Отже алгоритми є стійкими, якщо використовувана геш функція та PRNG є стійкими до витоку [4].

### 1.4. LD-OTS, W-OTS і MSS

*Часові бічні канали.*

Обчислення відкритого ключа як LD-OTS, так і W-OTS мають постійну кількість обчислень геш функції. Тому часовий бічний канал у даному випадку відсутній. Генерація підпису для LD-OTS має фіксовану кількість геш викликів (половина обчислення відкритого ключа), що також означає, що жодна атака за часом не може бути проведена [1]. Час виконання генерації підпису W-OTS залежить лише від повідомлення, яке потрібно підписати, і тому не

призводить до витоку будь-якої цінної інформації для зловмисника. Для MSS можна використовувати ті ж міркування, що й для XMSS.

*Бічні канали потужності.*

LD-OTS і W-OTS не роблять нічого, крім застосування геш функції до частин приватного ключа. Бітові маски в W-OTS+, які спричиняють незначний бічний канал потужності, відсутні в попередніх схемах. Таким чином, геш функція стійка до бічних каналів, є достатньою для гарантування стійкості щодо атак бічними каналами LD-OTS і W-OTS. MSS не виконує жодних обчислень із секретними даними, крім базового OTS. Генерація ключа на льоту може бути корисною для зловмисника, щоб зменшити шум, однак атака виглядає так само малоймовірною, як і для XMSS [1]. Очевидно, що якщо використовується PRNG, він має бути стійким до атак бічними каналами.

Таким чином, можна зробити висновок, що представлені схеми також природним чином протистоять розглянутим атакам бічними каналами.

### 1.5. LMS

*Часові бічні канали.*

Дивлячись на ланцюгову функцію $c^j(S,x,i)$, бачимо, що вона застосовує лише геш функцію $H$. Очевидно, що час цієї ланцюгової функції не спричиняє витоку цінної інформації, оскільки він залежить лише від значення, яке не є секретним. Конструкція LMS подібна до XMSS лише з невеликими варіаціями у використанні констант і елементів рандомізації. Оскільки всі вони загальнодоступні, додаткові часові бічні канали не можуть виникати [1].

*Бічні канали потужності.*

Включені $S$ (постійний рядок рандомізації), $i$ (індекс геш ланцюжка), $j$ (індекс у геш ланцюжку) і D_IT ER (константа 0x00), на перший погляд, надають додатковий бічний канал потужності, коли відкриті ключі LM-OTS обчислюються на льоту та кілька разів. Однак значення є фіксованими і тому не підходять для атаки з аналізом потужності [1]. Крім того, вони передаються лише як вхідні дані для геш функції, яка в представленому аналізі вважається стійкою до витоку. Те саме міркування стосується LMS: усі проміжні значення в деревах Merkle є загальнодоступними і, таким чином, не залежать від витоку.

Можна зробити висновок, що LMS за своєю суттю захищена від атак бічними каналами за часом та атак аналізу потужності, якщо реалізації PRNG і геш функції є стійкими до атак бічними каналами.

### 1.6. SPHINCS

*Часові бічні канали.*

Кількість обчислень геш функції як для генерації ключа HORST, так і для генерації підпису HORST не залежить від приватного ключа. Таким чином, якщо геш функція не містить часового бічного каналу, можна з упевненістю зробити висновок, що HORST стійкий до часового бічного каналу. Решта конструкції SPHINCS використовує лише W-OTS+ і XMSS і, таким чином, не може містити часовий бічний канал [1].

*Бічні канали потужності.*

Листя дерева HORST будуються з випадково згенерованих частин секретного ключа $sk_i$ шляхом застосування геш функції $F$. Тому HORST є стійким до бічних каналів, якщо $F$ є стійкою до бічних каналів, оскільки все інше можна вважати відкритим. Поєднуючи цю стійкість із міркуваннями щодо W-OTS+ і XMSS, можна бути впевненим, що SPHINCS має лише незначний витік бічними каналами, якщо використано стійкі геш функції та PRNG [1].

## 2. Атаки бічними каналами та оцінка захищеності SPHINCS+

SPHINCS+ – це схема електронного підпису на основі гешу, обрана NIST у процесі стандартизації постквантової криптографії. У даному пункті буде проаналізовано можливі атаки бічними каналами на даний алгоритм, а також надано оцінку контрзаходів від таких атак.

### 2.1. Захист SPHINCS+ від атак помилками

Перша подібна атака на SPHINCS+ розглядається у роботі Castelnovi та ін. [5]. У ній пропонується атака помилками на фреймворк, що лежить в основі SPHINCS, GRAVITY_SPHINCS та SPHINCS+. Представлена атака дозволяє підробити будь-який підпис повідомлення ціною одного помилкового повідомлення. Атака є загальною в тому сенсі, що вона не залежить від використовуваних геш функцій.

Автори стверджують, що атака дозволяє підробити підписи для будь-якого одного помилкового повідомлення за вартістю $2^{34}$ гешу за повідомлення. А для будь-якої цільової схеми можна підробити будь-яке повідомлення вартістю приблизно $2^{20}$ гешів, знаючи лише три помилкові повідомлення. Як показано в цій роботі, детермінована природа підписів на основі гешу та їхнє внутрішнє використання OTS може бути слабкою стороною проти атак помилками.

У роботі [5] представлено атаку помилками, яка змушує пару ключів W-OTS+ підписати пошкоджене повідомлення шляхом введення помилки під час побудови будь-якого неверхнього піддерева. Разом із дійсним (тобто безпомилковим) підписом піддерева, отриманий помилковий підпис W-OTS+ використовується для компрометації відповідної пари ключів W-OTS+ під час атаки з двома повідомленнями та надання дійсного підпису для іншого піддерева, для якого секрети відомі. Цей процес, подібний до щеплення дерева (живцювання), дає змогу підробити загальний підпис для будь-якого повідомлення.

Представлена у роботі атака має такі кроки:

1. Збирання підписів. На першому етапі зловмиснику необхідно зібрати як дійсні, так і помилкові підписи SPHINCS+ з цільового пристрою:

2. Обробка помилкових підписів. Наступним кроком є обробка помилкових підписів SPHINCS+, щоб отримати інформацію, яка уможливлює універсальну підробку.

3. «Щеплення» (живцювання) дерев. Після того, як найбільш секретні значення скомпрометованої пари ключів W-OTS+ були успішно вилучені з помилкових підписів, зловмисник прагне «прищепити» піддерево (або «ліс») до вилученої верхньої частини, тобто знайти інший XMSS (або FORS), для якого дійсний підпис W-OTS+ можна підробити, щоб підмінити скомпрометований екземпляр за його власною адресою.

4. Пошук шляху. Процедура підпису SPHINCS+ слідує шляху в гіпердереві залежно від повідомлення та значення $R$. У результаті зловмиснику необхідно знайти адекватне значення $R$, яке змусило б підроблений підпис відвідувати скомпрометоване піддерево.

Отримані у роботі результати вказують на те, що атака помилками можлива в усіх сценаріях, хоча кількість необхідних гешів значно змінюється залежно від конкретного рівня, на який спрямована атака. Однак, незважаючи на те, що надані цифри здаються високими, загальна кількість необхідних гешів може бути досягнута на практиці. Цей результат особливо важливий, оскільки атака помилками може бути успішною, навіть якщо помилка неконтрольована.

Робота Castelnovi та ін. [5] була додатково покращена та допрацьована Aymeric Genêt [6]. У цій роботі надано адаптовану оригінальну атаку на SPHINCS+, посилену рандомізованим підписом, і розширено застосовність атаки до будь-якої комбінації помилкових і дійсних підписів [6].

Припустимо, що помилка може вразити будь-який виклик геш функції рівномірно випадковим чином. Наведені вище перерахування призводять до наступних ймовірностей:

можливість використання помилки:

$$P(Expl.) = \frac{\#Total^F + (d-1)\cdot \#Total^X}{\#Total} = \frac{k(3t-1)+1+(d-1)(2^{h'}(lW+2)-1)}{3+k(3t-1)+d(2^{h'}(lW+2)-1)}; \quad (3)$$

можливість перевірки помилки:

$$P(Verif.) = \frac{1+\#Verif^F + (d-1)\cdot \#Verif^X}{\#Total} = \frac{1+k(3t-a-3)+(d-1)((2^{h'}-1)(lW-1)+2^{h'}-h'-1)}{3+k(3t-1)+d(2^{h'}(lW+2)-1)} \quad (4)$$

Влучання в шар:

$$P(L=l^*) = \begin{cases} \dfrac{\#Total^F}{\#Total} = \dfrac{k(3t-1)+1}{3+k(3t-1)+d(2^{h'}(lW+2)-1)} & \text{if } l^*=0 \\ \dfrac{\#Total^X}{\#Total} = \dfrac{2^{h'}(lW+2)-1}{3+k(3t-1)+d(2^{h'}(lW+2)-1)} & \text{if } 1\le l^*\le d \end{cases} \quad (5)$$

У табл. 1 надано ймовірності з урахуванням усіх наборів параметрів SPHINCS+. Ця таблиця показує високу ймовірність того, що випадкова помилка призведе до помилкового підпису, який можна використовувати та підтвердити:

Таблиця 1

Результати аналізу помилок для всіх параметрів SPHINCS+

| | $P(Expl.)$ | $P(Verif.)$ | $P(L=l^*)$ | | | | |
|---|---|---|---|---|---|---|---|
| Набір | | | $l^*=0$ | 1 | … | $d-1$ | $d$ |
| 128s | 0.9326 | 0.9306 | 0.4607 | 0.0674 | … | 0.0674 | 0.0674 |
| 128f | 0.9669 | 0.8857 | 0.3387 | 0.0331 | … | 0.0331 | 0.0331 |
| 192s | 0.9527 | 0.9513 | 0.6216 | 0.0473 | … | 0.0473 | 0.0473 |
| 192f | 0.9613 | 0.8576 | 0.1495 | 0.0387 | … | 0.0387 | 0.0387 |
| 256s | 0.9162 | 0.9138 | 0.3296 | 0.0838 | … | 0.0838 | 0.0838 |
| 256f | 0.9553 | 0.9095 | 0.2398 | 0.0447 | … | 0.0447 | 0.0447 |

### 2.2. Контрзаходи проти атаки помилками

*Кешування шарів.*

Ця стратегія, спочатку запропонована в Gravity-SPHINCS [7], полягає в кешуванні всіх W-OTS+ в межах одного або кількох рівнів (шарів) (починаючи з верхнього рівня). Оскільки кеш не оновлюється новими запитами на підпис, кеш є статичним і тому його можна додати до відкритого ключа.

У табл. 2 показано, як імовірність того, що одна випадкова помилка є придатною для використання, зменшується зі збільшенням $c$ (кількість рівнів, що кешується) для всіх наборів параметрів SPHINCS+ [6]:

Таблиця 2

Аналіз контрзаходу кешування шарів

| Набір | $P(Expl.)$ | | | | | | |
|---|---|---|---|---|---|---|---|
| | $c=1$ | 2 | 3 | 4 | … | $d-1$ | $d$ |
| 128s | 0.8972 | 0.8591 | 0.8179 | 0.7733 | … | 0.6141 | 0.0000 |
| 128f | 0.9505 | 0.9335 | 0.9158 | 0.8975 | … | 0.5076 | 0.0000 |
| 192s | 0.9287 | 0.9034 | 0.8767 | 0.8486 | … | 0.7539 | 0.0000 |
| 192f | 0.9420 | 0.9218 | 0.9007 | 0.8787 | … | 0.2625 | 0.0000 |
| 256s | 0.8711 | 0.8216 | 0.7670 | 0.7066 | … | 0.4784 | 0.0000 |
| 256f | 0.9327 | 0.9090 | 0.8840 | 0.8578 | … | 0.3864 | 0.0000 |

*Кешування гілок.*

Ця стратегія полягає в кешуванні всіх підписів W-OTS+ і відкритих ключів у шляху під час процедури підписання [6]. Кеш є динамічним і може вимагати оновлення для кожного нового підпису.

У табл. 3 показано, як імовірність того, що випадкову помилку можна використати, зменшується з $b$ для всіх наборів параметрів SPHINCS+, припускаючи, що всі кеші заповнені до необхідної ємності:

Таблиця 3

Аналіз контрзаходу кешування гілок

| Набір | $P(Expl.)$ | | | | | |
|---|---|---|---|---|---|---|
| | $b = (2/3)2^{h'}$ | $(2/3)2^{2h'}$ | $(2/3)2^{3h'}$ | $(2/3)2^{4h'}$ | … | $(2/3)2^{dh'}$ |
| 128s | 0.9292 | 0.9238 | 0.9174 | 0.9098 | … | 0.3172 |
| 128f | 0.9647 | 0.9634 | 0.9620 | 0.9605 | … | 0.3219 |
| 192s | 0.9511 | 0.9485 | 0.9457 | 0.9425 | … | 0.3249 |
| 192f | 0.9585 | 0.9568 | 0.9549 | 0.9528 | … | 0.3052 |
| 256s | 0.9111 | 0.9023 | 0.8917 | 0.8785 | … | 0.3068 |
| 256f | 0.9530 | 0.9507 | 0.9481 | 0.9453 | … | 0.3130 |

Результати експериментів показали, що, не зважаючи на контрзаход, лише $2^9$ запитів підпису з імовірністю помилки $\approx 1/3$ достатньо, щоб скомпрометувати принаймні один W-OTS+ і, отже, виконати універсальну підробку SPHINCS+ [6].

Основний висновок аналізу полягає в тому, що SPHINCS+ є надзвичайно вразливим до помилок. Єдине необмежене пошкодження майже будь-якого обчислення має катастрофічний вплив на гарантії безпеки всіх наборів параметрів SPHINCS+.

### 2.3. Аналіз атаки Антонова на DM-SPR

У 2022 р. Сідней Антонов на форумі NIST PQC описав атаку на властивість DM-SPR геш функцій на основі SHA-256, які використовуються в SPHINCS+ [8]. Атака використовує конструкцію Merkle-Damgard SHA-256, використовуючи серію колізійних атак проти основної функції стиснення, щоб перетворити різнофункціональну багатоцільову атаку другого прообразу в однофункціональну багатоцільову атаку другого прообразу. На рис. 3 показано приклад того, як працює атака:

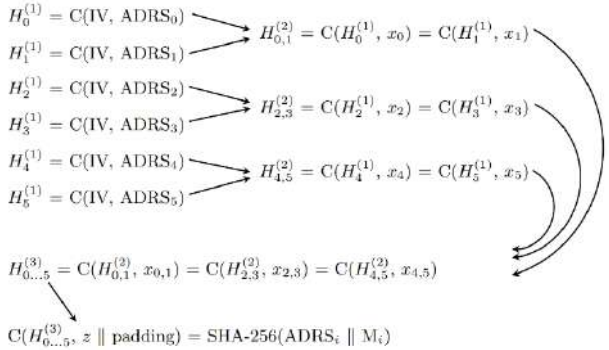


Рис. 3. Приклад роботи атаки Антонова

У відповіді йдеться про те, що автори вирішили замінити функцію SHA-256 на SHA-512 для рівнів безпеки NIST 3 та 5.

Автори не вважають, що ця атака ставить під сумнів загальну надійність конструкції SPHINCS+. У поєднанні з попередніми спостереженнями на форумі PQC щодо слабких місць у безпеці 5 рівня в гешуванні повідомлень [9] стає очевидним, що і атака Антонова, і атака з

роботи [10] стали можливими завдяки спробі дизайнерів SPHINCS+ використати 256-бітний Merkle-Damgard геш, як-от SHA-256, щоб загалом отримати 256 біт безпеки.

Оскільки після реагування на зауваження щодо безпеки для 3 та 5 рівнів безпеки ця функція тепер використовує SHA-512 замість SHA-256. Ця зміна означає, що подібна атака тепер потребує щонайменше $2^{256}$ обчислень геш функції, що ефективно блокує як атаку Антонова, так і атаку з роботи [10].

### 3. Аналіз рекомендацій щодо геш криптографії

Як описано раніше, у більшості випадків використання електронних підписів OTS не підходить, оскільки потрібно підписати та перевірити багато різних повідомлень. Для подолання цього недоліку були запропоновані схеми для створення багаторазових підписів з використанням OTS як будівельного блоку. Далі буде надано аналіз існуючих рекомендацій NIST, аналіз алгоритму, що пропонується до реалізації – SPHINCS+ – на основі відповідності до вимог NIST, а також аналіз швидкодії та захищеності різних варіантів SPHINCS+ [11]. На основі проведеного аналізу будуть представлені рекомендації щодо вибору реалізації.

#### 3.1. Аналіз існуючих рекомендації NIST

Рекомендація NIST (SP 800-208) [12] визначає 2 алгоритми, що можуть застосовуватися для створення ЕП:

- the Leighton-Micali Signature (LMS);
- the eXtended Merkle Signature Scheme (XMSS).

Фактично стандарт встановлює значення параметрів і які геш функції можна застосовувати.

Дослідження NIST 800-208 [11] показало наступне:

1. Публікація виступає у ролі рекомендації з реалізації алгоритмів ЕП «зі станом», серед яких LMS та XMSS разом з їх варіантами з кількома деревами.

2. У публікації описується застосування WOTS+ та дерев Меркла, які використовуються у реалізації SPHINCS+, що робить SPHINCS сумісним та таким, що відповідає усім критеріям даної публікації.

3. У публікації разом з XMSS та $XMSS^{MT}$ схвалюється застосування 4 різних геш функцій SHA-256, SHA-256/192, SHAKE256/256 та SHAKE256/192. В той час SHA-256 та SHAKE256 застосовуються у SPHINCS+, що робить його сумісним.

4. Для SPHINCS+ (sphincs-sha256-256f) ці параметри мають наступні значення: $n=32$, $w=16$, $len=67$, $h=68$ та $d=17$. Отже такий набір параметрів буде відповідати вимогам NIST (SP 800-208).

5. 192-розрядні геш функції, описані в цій рекомендації, SHA-256/192 та SHAKE256/192, пропонують значно меншу стійкість до загальних пошуків колізій, ніж їх 256-розрядні аналоги. Тому, реалізація SPHINCS+ із застосуванням SHA-256 є виправданою.

#### 3.2. Порівняння варіантів оптимізації ЕП

Далі буде надано порівняння різних варіантів оптимізації (закінчується на «s» – варіант з оптимізацією за пам'яттю, закінчується на «f» – варіант з оптимізацією за часом) [13]. Оцінка буде проводитися шляхом порівняння спочатку розмірів ЕП обох реалізацій, а потім швидкістю виконання підписання та перевірки, тобто всіх необхідних процедур алгоритму. У таблиці 4 предсталено порівняння розмірів ЕП для sphincs-256f та sphincs-256s:

Таблиця 4

Порівняння розмірів ЕП для 5 рівня безпеки NIST

| Варіант реалізації | Розмір PK | Розмір SK | Розмір підпису |
|---|---|---|---|
| sphincs-256f | 64 | 128 | 49856 |
| sphincs-256s | 64 | 128 | 29792 |

У табл. 5 надається порівняння швидкодії виконання різних варіантів. Тестування проводилося на процесорі i5-13600KF [14] із частотою 5.1ГГц і 32ГБ ОЗП.

Таблиця 5

Порівняння швидкодії для 5 рівня безпеки NIST

| Процес | Підпроцес | Кількість циклів на одне виконання | Кількість виконань | Загальна кількість циклів |
|---|---|---|---|---|
| sphincs-sha256-256f-robust | | | | |
| Генерація ключової пари | | 29,311,292 | 1x | 29,311,292 |
| - | Генерація WOTS pk | 1,612,542 | 16x | 25,800,672 |
| Підписання | | 701,347,571 | 1x | 701,347,571 |
| - | Підписання FORS | 108,020,496 | 1x | 108,020,496 |
| - | Підписання WOTS | 58,969 | 17x | 1,002,473 |
| - | Генерація WOTS pk | 1,594,614 | 272x | 433,735,008 |
| Перевірка | | 17,030,357 | 1x | 17,030,357 |
| sphincs-sha256-256s-robust | | | | |
| Генерація ключової пари | | 522,514,794 | 1x | 522,514,794 |
| - | Генерація WOTS pk | 1,626,626 | 256x | 416,416,256 |
| Підписання | | 6,736,001,820 | 1x | 6,736,001,820 |
| - | Підписання FORS | 2,282,116,657 | 1x | 2,282,116,657 |
| - | Підписання WOTS | 56,918 | 8x | 455,344 |
| - | Генерація WOTS pk | 1,611,667 | 2048x | 3,300,694,016 |
| Перевірка | | 9,143,489 | 1x | 9,143,489 |

З результатів, наведених у таблицях та на рисунках, видно, що хоча і варіант sphincs-256s має майже вдвічі менший розмір ЕП, проте різниця у швидкості роботи алгоритмів є дуже значною. Це вказує на те, що покращення розміру є не дуже доцільним, оскільки, зважаючи на сучасний стан розвитку технологій, час є більш цінним ресурсом ніж обсяг пам’яті.

### 3.3. Порівняння режимів роботи з різними параметрами

Варіант robust застосовує бітову маску, в той час як simple не застосовує. Оскільки представлені у NIST 800-208 алгоритми (LMS та XMSS) її застосовують, то з точки зору узгодження режим robust є більш підходящим.

### 3.4. Застосування псевдовипадкових чисел у реалізації

Детальний аналіз програмних реалізацій та документації різних версії SPHINCS+ показав, що (псевдо)випадкові числа застосовуються для SPHINCS+:

1. При початковій ініціалізації (заповненні) генератора псевдовипадкових чисел, що застосовується у реалізації (AES256_CTR_DRBG), за допомогою функції randombytes_init(entropy_input, NULL, 256). Тут до функції передається початкова ентропія (в даному випадку масив entropy_input, заповнений числами від 0 до 47). У самій функції, якщо присутній рядок персоналізація (у даному випадку рядок персоналізації = NULL), то цей рядок поелементно поєднується з seed_material (який і буде вхідною ентропією) шляхом XOR. Далі з використання функції AES256_CTR_DRBG_Update оновлюються (або ініціалізуються при початковому використанні) значення Key та V для DRBG_ctx.

2. При генерації початкового значення seed, а також при генерації повідомлення для підписання з використанням функції randombytes. Функція генерує seed довжини 48 байтів і

повідомлення довжини mlen. Також у функції AES256_CTR_DRBG_Update оновлюються значення Key та V для DRBG_ctx.

3. При оновленні (повторному заповненні) генератора псевдовипадкових чисел з використанням функції randombytes_init та згенерованого раніше seed. Всередині функції з використанням переданого seed оновлюються значення Key та V для DRBG_ctx із застосуванням AES256_CTR_DRBG_Update для подальшої генерації seed для застосування в процесі створення ключової пари.

4. Всередині функції crypto_sign_keypair при генерації seed із застосуванням функції randombytes для використання в процесі створення ключової пари. На цьому кроці генерується seed довжини CRYPTO_SEEDBYTES, яка залежить від вихідної довжини гешу у байтах SPX_N. SPX_N в свою чергу залежить від криптостійкості обраного варіанту реалізації алгоритму. Згенерований seed застосовується для формування ключів (до складу ключів входять частини seed, а також обчислений корінь геш дерева).

5. У процедурі підписання при ініціалізації випадкового значення optrand з використанням randombytes, якщо необхідно зробити процедуру підписання недетерміністичною. Довжина optrand дорівнює SPX_N і залежить від криптостійкості обраного варіанту реалізації SK_SEED, SK_PRF та PUB_SEED у процедурі генерації підпису не генеруються повторно.

Переглядаючи .req файли реалізацій, де генерується початкове значення seed, можна бачити, що для різних варіантів оптимізації генеруються однакові значення seed на однакових кроках. Це означає, що, з точки зору випадковості, дані реалізації є абсолютно ідентичними.

Таким чином, можна переконатися що за однакової ініціалізації (початкового заповнення) генератор буде поводитися ідентичним чином, а отже реалізація PRNG є однаковою для різних версій і варіантів оптимізації.

**Висновки**

Розглянуто атаки бічними каналами і атаки помилками на криптографію на основі гешу, а також проаналізовано рекомендації щодо застосування одного з кандидатів конкурсу NIST– SPHINCS+.

Згідно з представленими припущеннями W-OTS+ і XMSS забезпечують сильну стійкість щодо атак бічними каналами. Показано, що W-OTS+ стійкий до більшості атак через його одноразовий характер, що обмежує кількість слідів, які можна отримати. Ця стійкість послаблюється генерацією ключів на льоту в XMSS. Алгоритми є стійкими, якщо використовувана геш функція та PRNG є стійкими до витоку.

Не зважаючи на це, SPHINCS+ є надзвичайно вразливим до помилок. Єдине необмежене пошкодження майже будь-якого обчислення має катастрофічний вплив на гарантії безпеки всіх наборів параметрів SPHINCS+.

До такої вразливості слід ставитися серйозно, оскільки помилки природно трапляються у звичайному обладнанні, наприклад у DRAM. Оскільки загрозу помилки не можна повністю усунути, найкращим рішенням для захисту схеми ЕП від випадкових і навмисних помилок є надлишковість. Результати, надані у роботі, показують, що усі реальні застосування SPHINCS+ необхідно виконувати з перевірками шляхом надмірності, навіть якщо сценарій використання не є схильним до помилок.

Для відповідності вимогам NIST 800-208 слід застосовувати SPHINCS+ з параметром розміру вихідного гешу у 32 байти – 256 біт разом із функцією SHA-256 або SHAKE256 для кращого забезпечення стійкості до колізій.

Гарним рішенням було б використання середовища виконання з мінімально можливою ймовірність помилки.

Щодо варіанту реалізації SPHINCS+, з точки зору інших параметрів, найкращими варіантами для реалізації будуть: для 1 рівня захисту NIST: sphincs-128f-robust та sphincs-128s-robust. Для 3 рівня захисту NIST: sphincs-192f-robust та sphincs-192s-robust. Для 5 рівня захи-

сту NIST: sphincs-256f-robust та sphincs-256s-robust. Також доцільним є забезпечення переходу від одного варіанту до іншого за допомогою файлу параметрів.

**Список літератури:**


1. Denis Butin Physical Attack Vulnerability of Hash-Based Signature Schemes. 2017. URL: https://kannwischer.eu/theses/MasterThesisMatthiasKannwischerFINAL.pdf.
2. A. Hülsing W-OTS+ – Shorter Signatures for Hash-Based Signature Schemes. 2013. URL: https://eprint.iacr.org/2017/965.pdf.
3. A. Hülsing, D. Butin, S.-L. Gazdag, A. Mohaisen XMSS: Extended Hash-based Signatures. 2020. URL: https://datatracker.ietf.org/doc/rfc8391
4. T. Eisenbarth, I. von Maurich, and X. Ye. Faster Hash-Based Signatures with Bounded Leakage. 2014. URL: https://www.researchgate.net/publication/290110020_Faster_Hash-Based_Signatures_with_Bounded_Leakage.
5. Laurent Castelnovi, Ange Martinelli, Thomas Prest Grafting trees: A fault attack against the SPHINCS framework. 2018. URL: https://eprint.iacr.org/2018/102.pdf.
6. Aymeric Genêt On Protecting SPHINCS+ Against Fault Attacks. 2023. URL: https://eprint.iacr.org/2023/042.pdf.
7. Jean-Phillippe Aumasson and Guillaume Endignoux. Gravity-SPHINCS. 2017. URL: https://github.com/gravity-postquantum/gravity-sphincs
8. Antonov S. Round 3 official comment: SPHINCS+. 2022. URL: https://groups.google.com/a/list.nist.gov/g/pqc-forum/c/FVItvyRea28/m/mGaRi5iZBwAJ
9. Stern M. Diversity of signature schemes. 2021. URL: https://groups.google.com/a/list.nist.gov/g/pqc-forum/c/2LEoSpskELs/m/LkUdQ5mKAwA
10. Ray Perlner, John Kelsey, David Cooper Breaking Category Five SPHINCS+ with SHA-256. 2022. URL: https://eprint.iacr.org/2022/1061.pdf
11. J. Aumasson, D. J. Bernstein, et al. SPHINCS+. Submission to the NIST post-quantum project, v.3.1. 2022. URL: https://sphincs.org/data/sphincs+-r3.1-specification.pdf
12. NIST SP 800-208. Recommendation for Stateful Hash-Based Signature Schemes. 2020. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-208.pdf
13. SPHINCS+ official web-site. NIST 3-rd Round Package. URL: https://sphincs.org/data/sphincs+-round3-submission-nist.zip
14. Офіційний сайт Intel. Процессор Intel® Core™ i5-13600KF. URL: https://www.intel.com/content/www/us/en/products/sku/230494/intel-core-i513600kf-processor-24m-cache-up-to-5-10-ghz/specifications.html


*Надійшла до редколегії 04.06.2023*


*Відомості про авторів:*

**Дерев'янко Ярослав Андрійович** - науковий співробітник-консультант АТ «Інститут інформаційних технологій», Україна; e-mail: yarik0009258@gmail.com; ORCID: https://orcid.org/0000-0002-3290-3373

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

**Горбенко Іван Дмитрович** – д-р техн. наук, професор, Харківський національний університет імені В. Н. Каразіна, професор кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук, АТ "Інститут Інформаційних Технологій", головний конструктор, Україна; e-mail: gorbenkoi@iit.kharkov.ua; ORCID: https://orcid.org/0000-0003-4616-3449

**УДК 004.056.5** **DOI:10.30837/rt.2023.2.213.02**

*С.О. КАНДІЙ*

# АНАЛІЗ ПРОЦЕСІВ ГЕНЕРАЦІЇ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ В ЕП CRYSTALS-DILITHIUM

## Вступ

Здебільшого під час аналізу електронних підписів (ЕП) у літературі вважається, що є певне ідеалізоване джерело випадковості і не існує атак, що використовують властивості цього джерела [13]. Проте на практиці джерело випадковості може бути неідеальним та містити вразливості.

ЕП Crystals-Dilithium є фіналістом у конкурсу NIST PQC з постквантової криптографії [8]. Ця робота присвячена аналізу процесів генерації випадкових чисел у еталонній реалізації ЕП Crystals-Dilithium.

ЕП Crystals-Dilithium використовує для генерації випадкових змінних shake128/256 [9] та (варіативно) генератор псевдовипадкових чисел (DRNG) на основі AES в режимі лічильника (CTR) [1, 8]. Останній є варіацією стандартизованого CTR_DRBG. Оскільки PRNG на основі AES у режимі лічильника (CTR) є популярним вибором для багатьох практичних застосувань, то для повноти картини у цій роботі проведено аналіз стандартизованої версії – генератора CTR_DRBG [1] з AES-256 у якості блочного шифру (надалі – AES_CTR_PRNG). Аналіз виконано відповідно до останньої версії стандарту AIS 31 [2], що регламентує вимоги до генераторів ПВП.

Додатково проведено аналіз безпеки shake128/256 для генерації випадкових поліномів у ЕП Crystals-Dilithium. Отримано практичні рекомендації щодо параметрів компіляції в залежності від умов використання.

Роботу організовано наступним чином. В розд. 1 наведено необхідні відомості з криптографії, наведено опис генераторів. В розд. 2 побудовано та в розд. 3 проаналізовано формальну модель для AES_CTR_PRNG. В розд. 4,5 наведено аналіз використання shake128/256 в ЕП Crystals-Dilithium.

## 1. Попередні відомості

### 1.1. Стандарт AIS 31

Стандарт AIS 31 класифікує генератори випадкових чисел наступним чином [2]:

- генератори псевдовипадкових чисел (PRNG). Усі безпечні PRNG діляться на три функціональні класи: DRG.2, DRG.3, DRG.4;
- фізичні генератори випадкових чисел (PTRNG). Усі безпечні PTRNG діляться на два функціональні класи: PTG.2, PTG.3;
- нефізичні генератори випадкових чисел (NPTRNG). Для NPTRNG стандарт визначає тільки один функціональний клас – NTG.1.

Кожен PRNG, згідно з AIS 31, може бути описано за допомогою кортежу параметрів $(S, S_{req}, R, A, I, \phi, \phi_{req}, \phi_0, \psi)$, де

- $S$ – множина допустимих внутрішніх станів;
- $S_{req}$ – множина допустимих (тимчасових) станів запитів;
- $R$ – множина допустимих вихідних значень;
- $A$ – множина допустимих додаткових вхідних значень;
- $I$ – множина допустимих розмірів запитів;
- $\phi : S \times A \to S$ – функція переходу станів;
- $\phi_{req} : S \times A \to S_{req}$ – функція генерації стану запиту;

- $\phi_0 : S_{req} \times A \to S_{req}$ – функція переходу стану запиту;
- $\psi : S_{req} \to R$ – вихідна функція.

Вважається, що для обробки запиту на $p \in I$ біт генерується $m$ внутрішніх випадкових чисел. Причому, виконується наступний псевдокод для кожного запиту з додатковими вхідними даними $a$ та внутрішнім станом $s$:

$$
\begin{aligned}
& s_{req} = \phi_{req}(s, a) \\
& for(j = 1; m;\ j{+}{+}) \\
& \quad r_j = \psi(s_{req}) \\
& \quad s_{req} = \phi_0(s_{req}) \\
& s = \phi(s, a)
\end{aligned}
\quad .
$$

Процес ініціалізації PRNG описується кортежем $(SM, PS, S, \phi_{seed}, \phi_{reseed})$, де $SM$ – множина допустимих строк ініціалізації; $PS$ – множина допустимих строк персоналізації; $S$ – множина допустимих внутрішніх станів; $\phi_{seed}$ – функція ініціалізації; $\phi_{reseed}$ – функція повторної ініціалізації.

Повний опис функціональних класів виходить за межі даної роботи, проте для подальшого аналізу необхідно описати вимоги до класу DRG.3.

Генератор псевдовипадкових чисел належить до класу DRG.3 у разі виконання наступних вимог:

DRG.3.1 – строка ініціалізації (seed), повинен бути отриманий з DRG.3 або DRG.4 сумісного PRNG або безпечного TRNG;

DRG.3.2 – між викликами процедури ініціалізації та повторної ініціалізації повинно відбутися не більше $2^{48}$ запитів на генерацію ПВП. Кожен запит повинен бути не більше $2^{19}$ біт;

DRG.3.3 – ефективний внутрішній стан (критична для безпеки частина внутрішнього стану) повинен мати не менше 252 біт ентропії;

DRG.3.4 – початковий ефективний внутрішній стан повинен мати не менше 250 біт ентропії (або 240 біт мінімальної ентропії);

DRG.3.5 – має бути обчислювально важко дізнатися наступне випадкове число, знаючи деяку кількість попередніх (forward secrecy);

DRG.3.6 – має бути обчислювально важко дізнатися попереднє випадкове число, знаючи деяку кількість наступних (backward secrecy);

DRG.3.7 – якщо поточний внутрішній стан дізнається зловмисник, то в нього не має бути змоги дізнатися попередній внутрішній стан (enhanced backward secrecy);

DRG.3.8– додаткові вхідні дані не повинні зменшувати безпеку;

DRG.3.9 – функція переходу станів $\phi$ та вихідна функція $\psi$ мають бути криптографічними;

DRG.3.10 – мають бути свідчення того, що статистичні тести не зможуть відрізнити на практиці псевдовипадкову послідовність від випадкової.

### 1.2. Генератор ПВП CTR_DRBG

На рис. 1 наведено псевдокод генератора CTR_DRBG, що є частиною стандарту SP800-90A [1]. Зауважимо, що у межах цієї роботи розглядається варіант CTR_DRBG без функції виведення. Втім, аналіз може бути легко адаптований для цього варіанта за необхідності.

**CTR-DRBG update**

Require: $provided\_data, K, V$
Ensure: $K, V$
$temp \leftarrow \varepsilon\ ; m \leftarrow \lceil (\kappa + \ell)/\ell \rceil$
For $j = 1, \ldots, m$
  $V \leftarrow (V + 1) \bmod 2^{\ell}\ ; Z \leftarrow \mathsf{E}(K, V)$
  $temp \leftarrow temp \,\|\, Z$
$temp \leftarrow \text{left}(temp, (\kappa + \ell))$
$temp \leftarrow temp \oplus provided\_data$
$K \leftarrow \text{left}(temp, \kappa)$
$V \leftarrow \text{right}(temp, \ell)$
Return $K, V$

**CTR-DRBG next**

Require: $S = (K, V, cnt), \beta, addin$
Ensure: $R, S' = (K', V', cnt')$
1. If $cnt > reseed\_interval$
2.  Return reseed_required
3. If $addin \neq \varepsilon$
4.  If derivation function used then
5.  $addin \leftarrow \mathsf{CTR\text{-}DRBG\_df}(addin, (\kappa + \ell))$
6.  Else if $len(addin) < (\kappa + \ell)$ then
7.  $addin \leftarrow addin \,\|\, 0^{(\kappa+\ell-len(addin))}$
8.  $(K, V) \leftarrow \mathsf{update}(addin, K, V)$
9. Else $addin \leftarrow 0^{\kappa+\ell}$
10. $temp \leftarrow \varepsilon\ ; n \leftarrow \lceil \beta/\ell \rceil$
11. For $j = 1, \ldots, n$
12.  $V \leftarrow (V + 1) \bmod 2^{\ell}\ ; r \leftarrow \mathsf{E}(K, V)$
13.  $temp \leftarrow temp \,\|\, r$
14. $R \leftarrow \text{left}(temp, \beta)$
15. $(K', V') \leftarrow \mathsf{update}(addin, K, V)$
16. $cnt' \leftarrow cnt + 1$
17. Return $R, (K', V', cnt')$

Рис. 1. Генератор ПВП CTR_DRBG

У межах роботи розглядається варіант цього генератора для AES256 [3] (хоча більша частина аналізу підходить до довільного блочного шифру). Позначимо як $c = AES256(m, key)$ шифротекст AES-256 повідомлення $m$ на ключі $key$. Режим роботи лічильника (CTR) для AES-256 наведено на рис. 2.

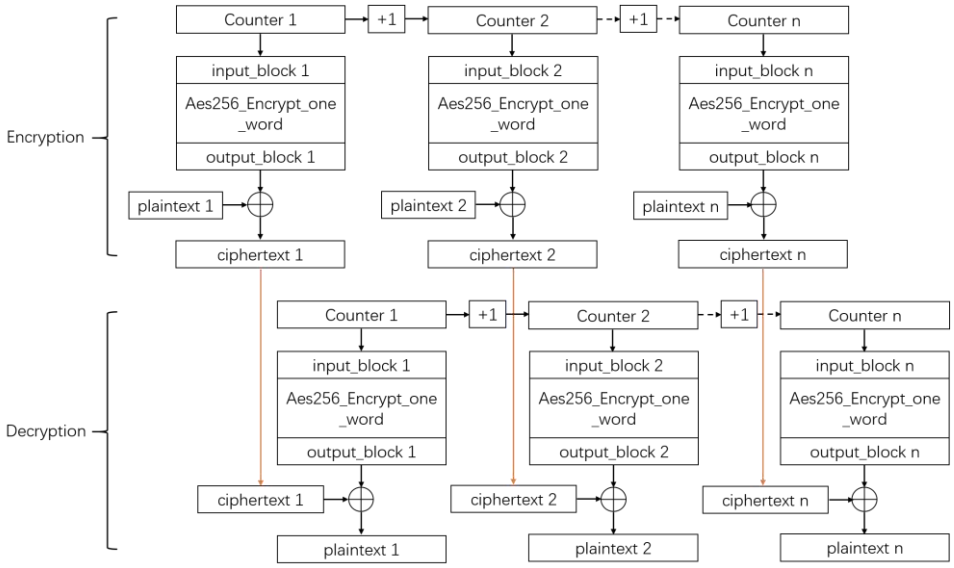


Рис. 2. Режим лічильника (CTR)

Для режиму лічильника введемо позначення $c = AES_{CTR}^{IV}(m, key)$. Передбачається, що поточний стан $v$ при шифруванні має форму $v = v_{info} \,\|\, ctr$, де $v_{info}$ – довільна інформаційна частина, $ctr$ – лічильник.

### 1.3. shake128/256

shake128 та shake256, за визначенням, є XOF (eXtendable output function). XOF є узагальненням геш функцій [9]. Криптографічна геш функція, за визначенням, є стискаючим відображенням, що відображає строки довільного розміру у множину строк (меншого) фіксова-

ного розміру. XOF робить відображення строк довільного розміру у множину строк довільного розміру, що заданий аргументом функції. При цьому зберігаються властивості криптографічних геш функцій. Це дає змогу використовувати XOF у якості геш функції, потокового шифру, DRNG, MAC-коду та інших симетричних криптопримітивів!

В основі XOF shake128/256 лежить sponge-конструкція, що зображена на рис. 3.

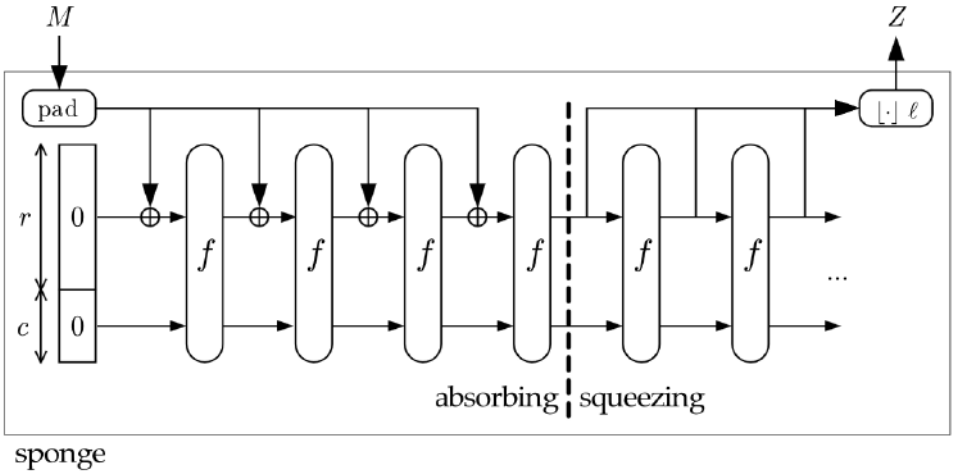


Рис. 3. Sponge-конструкція

Sponge-конструкція використовує випадкову перестановку $f:\{0,1\}^{b=r+c}\to\{0,1\}^b$, де $b$ – довжина входу, $r$ – бітрейт, $c$ – ємність. Робота Sponge-конструкції складається з двох фаз – поглинання (absorbing) та стиснення (squeezing).

На фазі поглинання Sponge-конструкція застосовує до повідомлення $M$ схему відступу $pad$, розбиває повідомлення на $r$-бітні блоки та побітово складає останні з поточним станом.

На фазі стиснення Sponge-конструкція ітераційно повертає перші $r$ біт внутрішнього стану та обрізає отриману послідовність до $\ell$ біт, як зображено на рис. 3.

Введемо позначення $Z = SPONGE[f, pad, r](M, \ell)$ для Sponge-конструкції, що використовує випадкову перестановку $f$, схему відступу $pad$, має бітрейт $r$ та повертає $\ell$-бітну бітову строку $Z$ для повідомлення $M$.

XOF shake128/256 є Sponge-конструкціями. Їх параметри зведено у табл. 1.

Таблиця 1

Параметри shake128/256

| | $f$ | $pad$ | $r$ | $c$ |
|---|---|---|---|---|
| shake128 | KECCAK-p[1600, 24] | pad10*1 | 1344 | 256 |
| shake256 | | | 1088 | 512 |

Повна специфікація KECCAK-p[1600, 24] та pad10*1 наведена в стандарті FIPS 202 [2]. Стандарт FIPS 202 доволі добре проаналізований міжнародною спільнотою, тож надалі вважається, що не існує ефективних атак, що використовують властивості $f$ чи pad10*1.

На Sponge-конструкцію існують загальні атаки, що використовують саме її властивості. Надалі останні $c$ біт стану називатимемо внутрішнім станом. Загальні атаки можна класифікувати як атаки:

на пошук внутрішніх колізій (колізій внутрішнього стану);

пошук шляху до внутрішнього стану;

пошук циклів;

відновлення внутрішнього стану.

Загальні атаки детально проаналізовано у [11]. Спираючись на [11], розглянемо кожен клас загальних атак більш детально.

Відповідно до визначень, внутрішній стан $s$ є бітовою строкою довжини $b=r+c$. Його можливо представити як конкатенацію бітових строк $s_{outer}$ та $s_{inner}$ довжини $r$ та $c$ біт відповідно.

Сутність атак на пошук внутрішніх колізій полягає у тому, щоб знайти два повідомлення $M_1, M_2$, для яких стани (після фази поглинання) $s^1, s^2$ матимуть $s^1_{inner} = s^2_{inner}$. Позначимо цю подію як $W_{IC}$. Нехай $N$ – кількість звернень до перестановки $f$. Якщо $f$ обчислювально складно відрізнити від випадкової перестановки, то з простого комбінаторного аналізу [4, розд.5.4] випливає оцінка атаки

$$\Pr(W_{IC}) \approx \frac{N(N+1)}{2^{c+1}} - \frac{N(N-1)}{2^{r+c+1}}. \quad (1)$$

Атаки на пошук шляху до внутрішнього стану фактично полягають у знаходженні повідомлення $M$ для відомого внутрішнього стану $s^1 = s^1_{outer} \| s^1_{inner}$, для якого $s^2 = s^2_{outer} \| (s^2_{inner} = s^1_{inner}) = absorb(M)$. Позначимо цю подію як $W_{Path}$. Якщо $f$ обчислювально складно відрізнити від випадкової перестановки, то з простого комбінаторного аналізу [4, розд. 5.5] випливає оцінка

$$\Pr(W_{Path}) \approx \frac{N(N+4)}{2^{c+2}} - \frac{N^2}{2^{r+c+2}}. \quad (2)$$

Атака на пошук циклів полягає у знаходженні повідомлення $M$, для якого у послідовності проміжних станів $s^1, s^2, \ldots$ існують такі $i, j$, що $s^i = s^j$. Позначимо цю подію як $W_{Cycle}$. Якщо $f$ обчислювально складно відрізнити від випадкової перестановки, то ймовірність такої події становить

$$\Pr(W_{Cycle}) \approx \frac{N}{2^{r+c}}. \quad (3)$$

Атаки на відновлення внутрішнього стану є найбільш актуальними для аналізу генерації випадкових чисел у реалізаціях ЕП. Сутність атак на відновлення стану полягає для заданої бітової строки $Z$ у знаходженні $s$, для якого виконується $Z = squeeze(s, |Z|)$. Позначимо цю подію як $W_{SR}$.

Аналіз цієї атаки є дещо складнішим за раніше розглянуті атаки. Оцінки безпеки отримано в роботах [11, 12]. Введемо необхідну термінологію.

Нехай $|Z| = mr$. Строку $Z$, за визначенням, можливо розбити на послідовність блоків $Z_0, Z_1, \ldots, Z_{m-1}$. Прямим розбиттям блоків $B_f(Z)$ є множина підмножин індексів $i, 0 \le i < m-1$. В одну підмножину входять індекси $i_1, i_2, \ldots$, для яких значення блоків є однаковими $Z_{i_1} = Z_{i_2} = \ldots$. Прямою кратністю $m_f(Z,r)$ є потужність найбільшої підмножини у $B_f(Z)$. Зворотне розбиття блоків $B_b(Z)$ і зворотна кратність $m_b(Z,r)$ визначені аналогічно, тільки для індексів у діапазоні $0 < i \le m-1$. Повна кратність визначена як

$$m(Z,r) = \max\{m_f(Z,r), m_b(Z,r)\}. \quad (4)$$

Згідно з [4, 5] для заданого $Z = squeeze(s, |Z|)$ ймовірність знаходження $s$ складає

$$\Pr(W_{SR} \mid \mathrm{Z}) \approx \Pr(W_{SR}) \approx \frac{m(Z,r)\,\mathrm{N}}{2^c}. \quad (5)$$

### 1.4. Відомості з теоретичної криптографії

Псевдовипадкові функції (PRF) є функціями, які обчислювально важко відрізнити від випадкових функцій. Псевдовипадкові перестановки (PRP), відповідно, є перестановками, які важко відрізнити від дійсно випадкових перестановок. Точні формальні визначення можливо знайти, наприклад, у [4]. PRNG, PRF, PRP тісно пов'язані між собою. У межах роботи нас цікавлять два результати, що отримані у [5, 6].

Т е о р е м а 1 . Для всіх алгоритмів, що роблять не більше $M$ запитів на обчислення функції в точці та працюють за час, не більший за $t$, для будь-якої родини перестановок $P$ довжини $L$ має місце твердження

$$Adv^{P}_{PRF}(t,M) \le Adv^{P}_{PRP}(t,M) + M^2 2^{-L-1}.$$

Тут і надалі $Adv$ позначає перевагу у відрізненні відповідного псевдовипадкового об'єкта від випадкового. З теореми видно, що будь-яка псевдовипадкова перестановка може бути розглянута як псевдовипадкова функція.

Сімейство бієктивних псевдовипадкових перестановок (функцій) може бути розглянуто як блочний шифр. Наступна теорема встановлює зв'язок між захищеністю шифру (у режимі лічильника) від атак з підібраним відкритим текстом (CPA).

Т е о р е м а 2 . Припустимо, що $E$ є сімейством псевдовипадкових функцій з розміром образів $L$. Тоді, для будь-яких $t$ та $M$ має місце

$$Adv^{CPA}_{CTR[E]}(t,M) \le 2 \cdot Adv^{PRF}_{E}(t,M).$$

Тут $CTR[E]$ позначає блочний шифр $E$ у режимі лічильника.

### 2. Побудова формальної моделі

У цьому розділі будуть використовуватися дві допоміжні функції - $rm(str, bitlen)$ та $lm(str, bitlen)$, які обрізають бітову строку до довжини $bitlen$ справа та зліва. Функція $len(\cdot)$ повертає довжину строки в бітах. $seedlen$ – довжина строки ініціалізації.

Для аналізу AES_CTR_PRNG побудуємо формальний опис у вигляді кортежу $(S, S_{req}, R, A, I, \phi, \phi_{req}, \phi_0, \psi)$. Нехай $S_K = \{0,1\}^{256}$ – множина усіх допустимих ключів та $S_B = \{0,1\}^{128}$ – множина усіх допустимих шифротекстів/відкритих текстів. Тоді, множину усіх допустимих внутрішніх станів можливо описати як

$$S = S_B \times S_K \times \square_{2^{48}}. \quad (6)$$

Кожен допустимий внутрішній стан задається трійкою $(v, key, rc)$, де $v$ – значення лічильника, $key$ – ключ шифрування, $rc$ – кількість зроблених запитів до генератора ПВП.

Ефективним внутрішнім станом є друга компонента внутрішнього стану – ключ шифрування $key$. Внутрішній стан запиту можливо визначити як

$$S_{req} = S_B \times S_K. \quad (7)$$

Відповідно до попередніх домовленостей маємо визначення множини додаткових входів та допустимих вихідних значень:

$$A = \{0,1\}^{\le seedlen}, \quad (8)$$

$$R = S_B . \tag{9}$$

Для завершення опису наведемо декомпозицію генератору ПВП на функції $\phi, \phi_{req}, \phi_0, \psi$. Вихідна функція $\psi : S_{req} \to R$ задається як

$$\psi(s_{req} = (v, key)) = AES256(v, key) . \tag{10}$$

Функція генерації внутрішнього стану запиту $\phi_{req} : S \times A \to S_{req}$ задається як

$$\begin{aligned} &\phi_{req}(s = (v, key, rc), a) = \\ &rm(f(a, key, v), 256), lm(f(a, key, v), 128) = (v_{req}, key_{req}) \end{aligned}, \tag{11}$$

де $f$ визначена наступним чином:

$$f(a, key, v) = AES^{v}_{CTR}(a \,||\, 0^{seedlen - len(a)}, key) . \tag{12}$$

Функція оновлення внутрішнього стану запиту $\phi_0 : S_{req} \times A \to S_{req}$ визначена наступним чином:

$$\phi_0(v = v_{info} \,||\, ctr, key, a) = (v_{info} \,||\, ctr + 1, key) . \tag{13}$$

Для опису функції оновлення внутрішнього стану $\phi : S \times A \to S$ зробимо наступну декомпозицію:

$$\phi = \phi_A \circ (\phi_B \times id) , \tag{14}$$

де функція $\phi_A : S \times A \to S$ визначена як

$$\begin{aligned} &\phi_A(s = (v, key, rc), a) = \\ &rm(f(a, key), 256), lm(f(a, key), 128), rc = (v_{new}, key_{new}, rc) \end{aligned}. \tag{15}$$

І функція $\phi_B : S \times A \to S$ визначена як

$$\begin{aligned} &\phi_B(s = (v, key, rc), a) = \\ &rm(f(a, key), 256), lm(f(a, key), 128), rc = (v_{new}, key_{new}, rc + 1) \end{aligned}. \tag{16}$$

Також, для аналізу процесів ініціалізації наведемо формальний опис у термінах кортежу $(SM, PS, S, \phi_{seed}, \phi_{reseed})$. Множина допустимих внутрішніх станів була визначена раніше (формула (1)). Множини допустимих строк ініціалізації ($SM$) та персоналізуючих строк ($PS$) задані наступним чином:

$$SM = \{0,1\}^{seedlen} , \tag{17}$$

$$PS = \{0,1\}^{\le seedlen} . \tag{18}$$

Функції $\phi_{seed} : SM \times PS \to S$ та $\phi_{reseed} : S \times SM \times PS \to S$ задані наступним чином:

$$\begin{aligned} &\phi_{seed}(seed, personal) = \\ &rm(f(seed \oplus personal, 0^{256}), 256), \\ &lm(f(seed \oplus personal, 0^{256}), 128), 1 = (v, key, rc) \end{aligned} \tag{19}$$

$$\begin{aligned}&\phi_{reseed}(s=(v,key),seed,personal)=\\&rm(f(seed\oplus personal,key,v),256),\\&lm(f(seed\oplus personal,key,v),128),1=(v,key,rc)\end{aligned}. \quad (20)$$

**3. Аналіз формальної моделі**

Покажемо, що AES_CTR_PRNG задовільняє вимогам класу безпеки DRG.3.

Властивість DRG.3.2 (обмеження на кількість біт за один запит та кількість біт між ініціалізаціями) виконується за визначенням AES_CTR_PRNG.

Властивість DRG3.3 (ефективний внутрішній стан повинен мати щонайменше 252 біта ентропії) виконується, оскільки ефективним внутрішнім станом є секретний ключ *key* та вектор ініціалізації $v$, які отримані як результат застосування CTR[AES256] до строки ініціалізації. З властивостей AES256 випливає, що отримані бітові строки будуть мати достатньо велику ентропію. Властивість DRG3.4 (початковий ефективний внутрішній стан повинен мати щонайменше 250 біт ентропії) виконується з тих самих причин.

Доведемо, що AES_CTR_PRNG задовільняє властивості DRG.3.5 – знання випадкових чисел $r_i,...,r_j$, що отримані за допомогою AES_CTR_PRNG, не дозволяє визначити $r_{j+1}$. Для DRNG це твердження є еквівалентним наступному твердженню: послідовність $r_i,...,r_j,r_{j+1}$ неможливо відрізнити від послідовності дійсно випадкових чисел.

Припустимо, що задано деякий алгоритм $D$, що робить не більше $q$ запитів на генерацію випадкових чисел та може відрізнити послідовність $r_i,...,r_j,r_{j+1}$ від послідовності дійсно випадкових чисел. Розглянемо гру $Game^b_{RNG}(D,q)$ між тестувальником та супротивником $D$, яка для параметра $b\in\{0,1\}$ визначена наступним чином. Тестувальник на початку гри володіє станом AES_CTR_PRNG - $S_0=(v,key,rc)$. Тестувальник генерує бітові послідовності $r^0_0,r^0_1,...,r^1_M$ та $r^1_0,r^1_1,...,r^1_M$ для деякого $M$, де послідовність $r^0_0,r^0_1,...,r^1_M$ отримана за допомогою AES_CTR_PRNG, а $r^1_0,r^1_1,...,r^1_M$ є дійсно випадковою послідовністю Результатом гри є рішення супротивника $d\leftarrow D(r^b_0,r^b_1,...,r^b_M)$. Якщо супротивник вважає, що послідовність є дійсно випадковою, то повертає 1, інакше повертає 0. Перевага супротивника $D$ у $Game^b_{RNG}(D)$ визначена наступним чином:

$$\begin{aligned}&Adv_{AES\_CTR\_PRNG}(D,q)=\\&|\Pr(Game^1_{PRG}(D,q)=1)-\Pr(Game^0_{PRG}(D,q)=1)|\end{aligned}. \quad (21)$$

Ця нотація узагальнюється для довільного алгоритму, що працює не довше за заданий час $t$, наступним чином:

$$Adv_{AES\_CTR\_PRNG}(t,q)=\max_D\{Adv_{AES\_CTR\_PRNG}(D,q)\}, \quad (22)$$

де $D$ береться з множини усіх алгоритмів, що працюють менше за заданий час $t$.

З визначення функцій $\psi,\phi_0$ випливає, що послідовність $r_i,...,r_j$ має вигляд $AES256(v_{info}\,||\,ctr+i,key)$, $AES256(v_{info}\,||\,ctr+i+1,key)$,..., $AES256(v_{info}\,||\,ctr+j,key)$, що є визначенням режиму лічильника для AES. Отже, за теореми 2 випливає:

$$\begin{aligned}&Adv^{CTR[AES256]}_{CPA}(t,M)\le Adv^{AES256}_{PRF}(t,M)\\&\le 2\cdot(Adv^{AES256}_{PRP}(t,M)+M^2 2^{-L-1})\end{aligned}. \quad (23)$$

Відповідно маємо оцінку безпеки для одного запита:

$$Adv_{AES\_CTR\_PRNG}(t,1) \le Adv_{ROR-CPA}^{CTR[AES256]}(t,M). \quad (24)$$

Оскільки AES256 є добре вивченим шифром, то можемо вважати, що $Adv_{PRP}^{AES256}(t,M)=0$, звідки випливає оцінка

$$Adv_{AES\_CTR\_PRNG}(t,1) \le \frac{M^2}{2^{L+1}}. \quad (25)$$

Припустимо, що супротивник є обчислювально необмеженим. Верхню оцінку для $Adv_{AES\_CTR\_PRNG}(q)$ можливо отримати, якщо припустити, що ймовірність перемогти у грі $Game_{RNG}^{b}(D,q)$ не залежить від кількості спроб, тоді маємо:

$$\begin{aligned} &Adv_{AES\_CTR\_PRNG}(\cdot,q) \le 1-(1-Adv_{AES\_CTR\_PRNG}(\cdot,1))^q \\ &\approx q \cdot Adv_{AES\_CTR\_PRNG}(\cdot,1) \end{aligned} \quad (26)$$

Звідки випливає верхня оцінка

$$Adv_{AES\_CTR\_PRNG}(\cdot,q) \le \frac{qM^2}{2^{L+1}}. \quad (27)$$

Оскільки максимальна кількість блоків за один запит складає $2^{19}/2^7 = 2^{12}$, то ймовірність знаходження $r_{j+1}$ з $r_i,...,r_j$ є меншою за $q \cdot 2^{-104}$. Враховуючи те, що після кожного запиту ключ шифрування змінюється, то можливо вважати $q=1$, оскільки ефективних багатоключових атак на AES256 невідомо.

Властивість DRG.3.6 (з $r_i,...,r_j$ важко отримати $r_{j-1}$) аналогічно доводиться для AES_CTR_PRNG. Оскільки послідовність псевдовипадкових бітів важко відрізнити від дійсно випадкових бітів, то важко отримати $r_{j-1}$.

Властивість DRG.3.7 полягає у тому, що якщо супротивник дізнався поточний стан $S_i$, то він не зможе дізнатися попередній стан $S_{i-1}$. Ця властивість випливає з визначення функції $\phi_B$. Оскільки у кінці кожного запиту новий ключ шифрування отримується як результат криптографічної операції на старому ключі шифрування, то, якщо супротивник дізнається $S_{i-1}$, він порушить безпеку AES256, оскільки зможе розшифрувати шифротекст, не знаючи ключа шифрування, на якому останній був отриманий.

Властивість DRG.3.8 полягає у тому, що додаткові вхідні дані не мають зменшувати безпеку генератора, якщо зловмисник може контролювати їх. У AES_CTR_PRNG додаткові вхідні дані фактично зашифровуються AES256 у режимі лічильника. Якщо супротивник може за допомогою зміни вхідних даних впливати на безпеку генератора, то це означало б вдалу атаку з підібраними відкритими текстами на AES256 у режимі лічильника, що вважається неможливим згідно з модельними припущеннями безпеки AES256.

Властивість DRG.3.9 вимагає, щоб функції $\phi,\psi$ були криптографічними. Причому, функція $\phi$ має бути односторонньою. З визначень функцій $\phi,\psi$ видно, що це виконується, оскільки результатом роботи обох функцій є застосування AES256 до вхідних аргументів.

Властивість DRG.3.10 вимагає, щоб були сильні свідчення того, що статистичні тести не можуть відрізнити псевдовипадкові біти від дійсно випадкових. Вище було показано, що

ймовірність цього складає не більше $q \cdot 2^{-104}$, де $q$ – кількість запитів на вироблення випадкових бітів.

Остання вимога, яку необхідно розглянути є DRG.3.1, вимагає, щоб матеріал для ініціалізації генератора був отриманий за допомогою TRNG (допустимі класи безпеки PTG.2,PTG.3,NTG.1) або іншого PRNG класу DRG.3. Виконання цієї вимоги залежить від конкретної реалізації. Наприклад, генератор випадкових чисел /dev/random у ядрах Linux версії 5.6–5.17 задовільняє вимогам DRG.3 і може бути використаний для отримання матеріалу для ініціалізації.

Тож, усі вимоги виконано.

## 4. Генерація ПВП у Crystals-Dilithium

Розглянемо детально процеси генерації випадкових об'єктів в реалізації ЕП Crystals-Dilithium. Для зручності наведемо псевдовод Crystals-Dilithium з специфікації [8] на рис. 4.

**Gen**

$\rho \leftarrow \{0,1\}^{256}$
$K \leftarrow \{0,1\}^{256}$
$(\mathbf{s}_1, \mathbf{s}_2) \leftarrow S_\eta^\ell \times S_\eta^k$
$\mathbf{A} \in R_q^{k \times \ell} := \mathsf{ExpandA}(\rho)$ // $\mathbf{A}$ is stored in NTT Domain Representation
$\mathbf{t} := \mathbf{A}\mathbf{s}_1 + \mathbf{s}_2$
$(\mathbf{t}_1, \mathbf{t}_0) := \mathsf{Power2Round}_q(\mathbf{t}, d)$
$tr \in \{0,1\}^{384} := \mathsf{CRH}(\rho \parallel \mathbf{t}_1)$
**return** $(pk = (\rho, \mathbf{t}_1), sk = (\rho, K, tr, \mathbf{s}_1, \mathbf{s}_2, \mathbf{t}_0))$

**Sign**$(sk, M)$

$\mathbf{A} \in R_q^{k \times \ell} := \mathsf{ExpandA}(\rho)$ // $\mathbf{A}$ is stored in NTT Domain Representation
$\mu \in \{0,1\}^{384} := \mathsf{CRH}(tr \parallel M)$
$\kappa := 0$, $(\mathbf{z}, \mathbf{h}) := \perp$
**while** $(\mathbf{z}, \mathbf{h}) = \perp$ **do**
  $\mathbf{y} \in S_{\gamma_1 - 1}^\ell := \mathsf{ExpandMask}(K \parallel \mu \parallel \kappa)$
  $\mathbf{w} := \mathbf{A}\mathbf{y}$
  $\mathbf{w}_1 := \mathsf{HighBits}_q(\mathbf{w}, 2\gamma_2)$
  $c \in B_{60} := \mathsf{H}(\mu \parallel \mathbf{w}_1)$
  $\mathbf{z} := \mathbf{y} + c\mathbf{s}_1$
  $(\mathbf{r}_1, \mathbf{r}_0) := \mathsf{Decompose}_q(\mathbf{w} - c\mathbf{s}_2, 2\gamma_2)$
  **if** $\|\mathbf{z}\|_\infty \geq \gamma_1 - \beta$ or $\|\mathbf{r}_0\|_\infty \geq \gamma_2 - \beta$ or $\mathbf{r}_1 \neq \mathbf{w}_1$, then $(\mathbf{z}, \mathbf{h}) := \perp$
  **else**
    $\mathbf{h} := \mathsf{MakeHint}_q(-c\mathbf{t}_0, \mathbf{w} - c\mathbf{s}_2 + c\mathbf{t}_0, 2\gamma_2)$
    **if** $\|c\mathbf{t}_0\|_\infty \geq \gamma_2$ **or** the # of 1's in $\mathbf{h}$ is greater than $\omega$, then $(\mathbf{z}, \mathbf{h}) := \perp$
  $\kappa := \kappa + 1$
**return** $\sigma = (\mathbf{z}, \mathbf{h}, c)$

**Verify**$(pk, M, \sigma = (\mathbf{z}, \mathbf{h}, c))$

$\mathbf{A} \in R_q^{k \times \ell} := \mathsf{ExpandA}(\rho)$ // $\mathbf{A}$ is stored in NTT Domain Representation
$\mu \in \{0,1\}^{384} := \mathsf{CRH}(\mathsf{CRH}(\rho \parallel \mathbf{t}_1) \parallel M)$
$\mathbf{w}_1' := \mathsf{UseHint}_q(\mathbf{h}, \mathbf{A}\mathbf{z} - c\mathbf{t}_1 \cdot 2^d, 2\gamma_2)$
**return** $[\![\|\mathbf{z}\|_\infty < \gamma_1 - \beta]\!]$ **and** $[\![c = \mathsf{H}(\mu \parallel \mathbf{w}_1')]\!]$ **and** $[\![\#$ of 1's in $\mathbf{h}$ is $\leq \omega]\!]$

Рис. 4. Псевдокод ЕП Crystals-Dilithium

### 4.1. Генерація ключової пари

Відповідно до специфікації виконується наступна послідовність викликів до засобів генерації псевдовипадкових послідовностей:

- генерується випадкова строка seed за допомогою функції randombytes, що робить запит до криптографічного API Windows або до Linux RNG (в залежності від операційної системи). Надалі вважатимемо, що криптографічне API задовольняє необхідному рівню безпеки;
- обчислюється rho||rhoprime||key = shake256(seed);

- за допомогою генератора ПВП stream128 (буде розглянуто далі) та rho генерується матриця поліномів A. Кожен поліном генерується з унікальним nounce, який є його індексом у матриці;
- За допомогою генератора ПВП stream256 (буде розглянуто далі) генеруються вектори поліномів $s_1, s_2$. На відміну від поліномів у матриці, до поліномів додатково застосовується вибірка з відхиленням;
- shake256 в кінці генерації використовується як криптографічна геш функція: tr=shake256(rho||t1).

### 4.2. Вироблення підпису

Відповідно до специфікації виконується наступна послідовність викликів до засобів генерації псевдовипадкових послідовностей:

- shake256 використовується як криптографічна геш функція: mu=shake256(m||tr);
- shake256 використовується як криптографічна геш функція: rhoprime=shake256(key||mu), як і при генерації ключів;
- за допомогою генератора ПВП stream256 та rho генерується матриця поліномів A, як і при генерації ключів;
- за допомогою генератора ПВП stream256 генерується вектор поліномів y. Зауважимо, що в реалізації також підтримується режим, коли вектор генерується на основі випадкового значення з функції randombytes, що робить запит до криптографічного API. Ввімкнути цей режим можливо параметром компіляції DILITHIUM_RANDOMIZED_SIGNING;
- обчислюється c_seed для полінома c як shake256(mu||w1) та безпосередньо поліном c з shake256(c_seed).

### 4.3. Перевірка підпису

Відповідно до специфікації виконується наступна послідовність викликів до засобів генерації псевдовипадкових послідовностей:

- обчислення shake256(shake256(rho|| t), M);
- обчислення c2 з відновленого вектора поліномів w, аналогічно до обчислення оригінального полінома.

Для реалізації stream128/256 в залежності від параметрів компіляції існує два варіанти:

- використання shake128/256. Генерація гамми відбувається аналогічно до попередніх використань;
- використання AES128/256 в режимі лічильника. Генерація відбувається згідно з [3]. Цей генератор ПВП вже був проаналізований в [1]. Щоб ввімкнути використання цього варіанта, необхідно встановити параметр компіляції DILITHIUM_USE_AES.

## 5. Аналіз генерації випадкових чисел в ЕП Crystals-Dilithium

З опису можна зробити декілька висновків:

- в ЕП основним засобом генерації є shake256, проте для генерації матриці A використовується shake128. Це пов’язано з оптимізацією часу виконання. Матриця A є публічною, і оскільки Module-LWE є безпечним «у середньому» для випадкових матриць A, то для безпеки необхідно лише щоб у матриці A не було явно заданої алгебраїчної структури, що може зменшити складність Module-LWE. Тому використання shake128 не зменшує безпеки;
- усю роботу з випадковими числами можливо представити у вигляді графа. На рис. 5 зображено граф обчислень. Публічно відомі змінні позначено зеленим кольором, таємні змінні позначено червоним кольором. Цікавим є те, що у ЕП Crystals-Dilithium вироблення підпису є детермінованим. Випадковий вектор $y$ генерується з випадковості у секретному ключі. У класичному випадку вектор $y$ повинен генеруватися з незалежного джерела випадковості.

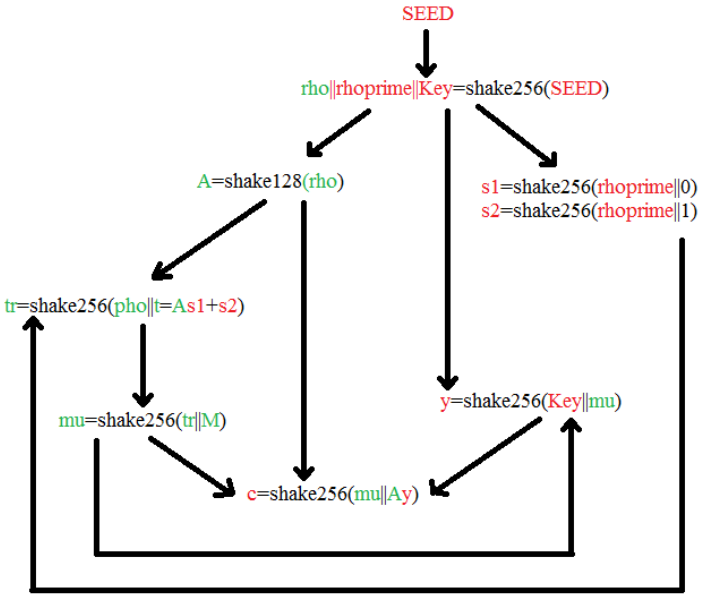


Рис. 5. Граф обчислень

Для змінних tr та mu shake256 виступає у якості криптографічної геш функції. Для shake256 вартість пошуку колізії складає $\min(d/2, 256)$, де $d$ – довжина вихідної послідовності. Для обох випадків для параметрів Crystals-Dilithium маємо $\min(384/2, 256) = 192$ для всіх рівнів безпеки в специфікації ЕП.

У всіх інших випадках shake256 можливо розглядати як PRNG. Для $s_1, s_2, y$ є невідомими як аргумент shake256, так і вихідне значення. Їх аргументи залежать від результату роботи shake256(seed), для якого частково є відомим значення вихідних даних (rho), отже, у цьому випадку задача криптоаналізу зводиться до атаки та пошуку внутрішнього стану. Стійкість до цієї атаки описується формулою (6). Оскільки $r$ є доволі великим, то $m(Z, r) \approx 1$ і маємо оцінку:

$$\Pr(seed \mid rho) \approx \frac{\mathrm{N}}{2^{256}}, \tag{28}$$

де $N$ – кількість запитів супротивника до функції стискання shake256. Тож, складність такої атаки фактично близька до перебору. Важливо також зауважити, що в результаті обчислень маємо послідовність

$$\text{Shake256(shake256(…shake(256(…)…)))}$$

У загальному випадку можуть існувати атаки саме на таку конструкцію, проте аналіз таких атак виходить за межі даної роботи.

**Висновки**

У роботі показано, що AES_CTR_PRNG задовільняє вимогам функціонального класу DRG.3. Проте, варто зауважити, останні дослідження [7] показують, що AES_CTR_PRNG є вразливим до атак на реалізацію у багатьох випадках. Тому, перед використанням AES_CTR_PRNG необхідно детально дослідити середовище виконання.

Окремо варто підкреслити, що модель безпеки AIS 31 передбачає використання незалежних та рівномірно розподілених випадкових змінних для ініціалізації генератора. У випадку AES_CTR_PRNG це є особливо критичним, оскільки це дає змогу зловмиснику за певних умов реалізовувати атаки на зв'язаних ключах.

Використання XOF shake256 є загальноприйнятим прийомом для реалізації асиметричної криптографії через її гнучкість та гарну безпеку.

Оскільки генератор на основі AES більш вразливий до атак по побічним каналам, то не рекомендовано використовувати флаг DILITHIUM_USE_AES, якщо немає додаткових гарантій захисту машини від атак по побічним каналам.

Якщо є довіра до криптографічного API операційної системи, то рекомендовано використовувати флаг компіляції DILITHIUM_RANDOMIZED_SIGNING. У системах з низькою довірою до криптографічного API операційної системи можна використовувати варіант з детермінованим виробленням підпису.

**Список літератури:**


1. NIST SP 800-90A. Recomendation for Random Number Generation Using Deterministic Random Bit Generation, June 2015.
2. BSI AIS 31. A Proposal for Functionality Classes for Random Number Generators, September 2022
3. FIPS 197. Advanced Encryption Standart, 2001.
4. Introduction to Modern Cryptography: Principles and Protocols / Katz, Jonathan; Lindell, Yehuda // Chapman & Hall/CRC Cryptography and Network Security Series, CRC Press, 2014.
5. Bellare M, Desai A., Jokipii E., Rogaway P. A concrete security treatment of symmetric encryption. FOCS, 1997.
6. M. Campagna. Security bounds for the NIST codebook-based deterministic random bit generator. Cryptology ePrint Archive. URL: https://eprint.iacr.org/2006/379
7. Hoang V., Shen Y. Security Analysis of NIST CTR-DRBG. Cryptology ePrint Archive. URL: https://eprint.iacr.org/2020/619
8. Lyubachevsky V., Ducas L., Kiltz E. CRYSTALS-Dilithium Techn. rep. NIST, 2017. [Electronic resource]. – Access mode: https://pq-crystals.org/dilithium/index.shtml
9. FIPS 202. SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, 2015.
10. Goldreich O. Foundations of Cryptography: Volume 2. Cambridge University Press, 2000. 392 p.
11. Bertoni G., Daemen J., Peeters M., Van Assche G. Cryptographic sponge functions. URL: https://keccak.team/files/CSF-0.1.pdf
12. Sponge-based pseudo-random number generators, CHES (S. Mangard and F.-X. Standaert, eds.), Lecture Notes in Computer Science, vol. 6225, Springer, 2010, pp. 33–47.
13. Горбенко І. Д., Горбенко Ю. І. Прикладна криптологія. Теорія. Практика. Застосування: монографія. Харків : Форт, 2012. 880 с.



*Надійшла до редколегії 10.06.2023*



*Відомості про автора:*

**Кандій Сергій Олегович** – Харківський національний університет імені В. Н. Каразіна, аспірант кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук; АТ «Інститут Інформаційних Технологій», технік-конструктор, Україна; e-mail: sergeykandy@gmail.com; ORCID: https://orcid.org/0000-0003-0552-8341

**УДК 004.056.5** **DOI:10.30837/rt.2023.2.213.03**

*О.О. КУЗНЕЦОВ, д-р техн. наук, Д.О. ЗАХАРОВ*

# ЗАСТОСУВАННЯ МОДЕЛЕЙ ГЛИБОКОГО НАВЧАННЯ ДЛЯ ГЕНЕРАЦІЇ КРИПТОГРАФІЧНОГО КЛЮЧА ІЗ ЗОБРАЖЕННЯ ОБЛИЧЧЯ

## Вступ

Біометрія традиційно вважається важливою сферою сучасної кібербезпеки [1 – 3]. Наприклад, біометричні методи автентифікації широко використовуються в різних додатках: криміналістика, електронна комерція, захист авторських прав, електронний документообіг, системи контролю доступу та багато іншого [1, 4, 5].

В останні роки інтерес до біометричних методів різко зріс. Від традиційних біометричних систем, заснованих на порівнянні отриманих біометричних зображень із збереженими еталонними копіями, сучасні технології перейшли до формування криптографічних ключів «на льоту» [5 – 7]. Цю проблему вирішують так звані нечіткі екстрактори, які дозволяють однозначно відновити секретний ключ з неточно відтворених біометричних даних за участю допоміжних даних (допоміжного рядка), які є публічними.

Традиційно нечіткі екстрактори, як і попередні їм нечіткі контейнери [4], будуються з використанням методів кодування з виправленням помилок. На початковому етапі біометричні дані в певному сенсі «зливаються» з елементами кодів, що виправляють помилки (наприклад, з кодовими словами або синдромальними послідовностями). Для нечітких екстракторів додатково формується відкритий допоміжний рядок (допоміжний рядок), який «допомагає» у вилученні секретного параметра з нечіткої біометрії. На етапі безпосереднього використання використовується завадостійке декодування, яке усуває можливу невизначеність (спричинену спотвореннями, стираннями тощо) у наданих користувачем біометричних зображеннях. Якщо відмінності в наборах характеристик невеликі (не перевищують коригуючу здатність кодів), то нечіткі екстрактори (сховища) дозволяють однозначно відновити секретний параметр (біометричний ключ).

Наступним кроком у розвитку таких технологій стане побудова повноцінних біометричних криптографічних систем, в яких біометричні персональні дані повинні використовуватися як джерело унікальних секретних параметрів. У цьому випадку користувачеві не потрібно буде запам’ятовувати криптографічні ключі (паролі) та/або використовувати додаткові пристрої для їх зберігання, передачі тощо. Біометрична криптосистема ініціалізується у будь-який час і в будь-якому місці шляхом вилучення необхідних параметрів “на льоту” з наданих біометричних зображень (з можливими неточностями, стираннями тощо) без шкоди для цих зображень. При цьому необхідно забезпечити максимальний набір послуг і гарантій безпеки з урахуванням особливостей побудови біометричних криптосистем.

У статті [8] запропоновано нову схему нечіткого екстрактора, яка використовує криптосистему коду McEliece [9]. Криптографія на основі коду є важливим напрямком у розвитку постквантових методів захисту інформації [10 – 14]. В роботах [10, 15, 16] показано, що використання методів на основі коду дозволяє забезпечити високу стійкість як до класичного, так і до квантового криптоаналізу. Незважаючи на численні спроби криптоаналізу [10, 12, 17 – 19], схема МакЕліса на основі кодів Гоппи [9, 18, 20] є надійною альтернативою сучасним криптосистемам з відкритим ключем. Зокрема, варіант класичної схеми McElice був представлений серед фіналістів третього етапу NIST PQC [21].

Екстрактор, запропонований у [8], оперує біометричними даними, представленими у вигляді наборів бінарних векторів. Передбачається, що різні набори одного користувача відрізняються один від одного не більше ніж на 25 % (цей поріг відповідає граничним можливостям виправлення помилок кодів). Проте в роботі [8] не запропоновано методів отримання таких бінарних наборів з будь-яких біометричних зображень (обличчя, пальці, сітківка та райдужка, вени, вушні раковини чи щось інше).

Метою цієї статті є розробка нечіткого екстрактора для генерації криптографічно надійних ключів із біометричних зображень людських облич.

**Методи глибинного навчання для отримання набору біометричних характеристик**

Більшість раніше реалізованих алгоритмів діставання фіч за певним зображенням $I$ повертає вектор фіч з дійсних чисел $f(I) \in R^{n_f \times 1}$ фіксованого розміру $n_f$.

У дослідженні будемо використовувати попередньо навчені екстрактори [22, 23]. Обидва алгоритми використовують підхід глибокого навчання: спочатку формується набір триплетів, де кожен елемент має форму $\left\{A^{(t)}, P^{(t)}, N^{(t)}\right\}$, де $A^{(t)}$ та $P^{(t)}$ – зображення однієї людини, а $A^{(t)}$ та $N^{(t)}$ – двох різних (тут $A, P, N$ відповідають термінам *anchor*, *positive* та *negative*, що відображають вищезгадані відносини) [22, 23]. Потім алгоритм намагається знайти такі параметри нейронної мережі, щоб мінімізувати функцію втрат $L(T)$ на цій множині триплетів.

**Датасет для оцінки екстрактора фіч**

Для оцінки екстрактора фіч використаємо датасети [25, 26].

Спочатку розбиваємо зображення людей на $n_b$ груп, де в кожній групі зберігаються зображення лише однієї людини. Припустимо, що кожна група складається з $n_i$ зображень. Таким чином, якщо візьмемо два зображення з однієї групи – матимемо зображення однієї людини; якщо два зображення взято з двох різних груп – матимемо зображення різних людей. Позначимо *j* зображення в *i* групі як $I_{i,j}$

Окрім поділу зображень на групи, для подальшої оцінки точності також потрібно буде розділити зображення на пари. Позначимо набір пар як $P$, кожен елемент $p$ якого визначається чотирма елементами $\{p(n_1), p(i_1), p(n_2), p(i_2)\}$, де $p(n_1), p(i_1)$ відповідають першому зображенню в групі $p(n_1)$ з порядковим номером $p(i_1)$. Так само для $p(n_2), p(i_2)$. Відповідно, якщо $p(n_1) = p(n_2)$, то маємо зображення однієї людини, в той час якщо ці два числа різні – то двох різних людей.

**Тюнінг порогового гіперпараметра**

Для подальшого аналізу також важливо знайти такий пороговий гіперпараметр $\tau$, який максимізував би точність класифікації «це два зображення однієї людини» і «двох різних людей» (назвемо це двійковою точністю). Припустимо, що маємо сформований набір пар $P$ і запускаємо наш класифікатор на цьому наборі пар із певним значенням порогу $\tau$. Визначимо двійкову точність $\alpha_{bin}$ на цій множині як

$$\alpha_{bin}(P,\tau) = \frac{N_+(P,\tau)}{|P|},$$

де $N_+(P,\tau)$ – кількість правильно ідентифікованих пар на множині $P$, використовується поріг $\tau$. Тепер спробуємо підібрати $\tilde{\tau}$ таке, що максимізує $\alpha_{bin}(P,\tau)$. Іншими словами,

$$\tilde{\tau} = \arg\max_{\tau} \alpha_{bin}(P,\tau) = \arg\max_{\tau} N_+(P,\tau).$$

Зробимо це наступним чином: беремо інтервал $(\tau_{\min}, \tau_{\max})$, на якому є шукане $\tilde{\tau}$ і рухаємось з $\tau_{\min}$ до $\tau_{\max}$ маленьким шагом $\Delta\tau$ ($\Delta\tau \in \tau_{\min}, \tau_{\max}$), обчислюючи значення $\alpha_{bin}(\tau)$ для кожного $\tau$. Присвоїмо $\tilde{\tau}$ значення $\tau$, яке дало найбільше значення $\alpha_{bin}(\tau)$.

Важливе зауваження: такий алгоритм потрібно робити окремо для кожного алгоритму, оскільки різні моделі виводять вектор $f(I)$ по-різному. Наприклад, для моделі *Face Recognition* маємо $\tilde{\tau} \approx 0.365$, в той час як для моделі *Keras Facenet* маємо $\tilde{\tau} \approx 155$, тому різниця в значеннях є значною.

На рис. 1 та 2 можна побачити залежність $\alpha_{bin}(\tau)$ для різних значень $\tau$ для моделей *Keras Facenet* та *Face Recognition* відповідно.

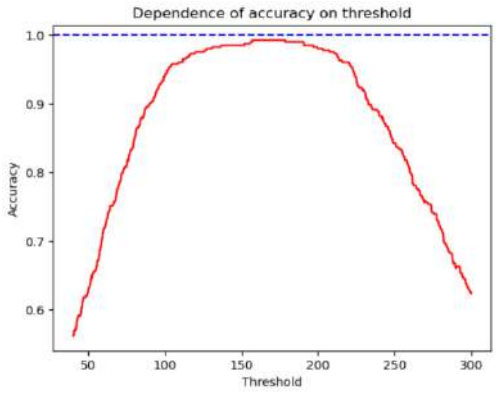


Рис. 1. Залежність $\alpha_{bin}(\tau)$ для моделі *Keras Facenet*

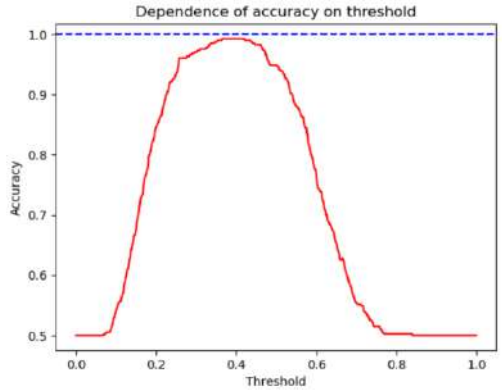


Рис. 2. Залежність $\alpha_{bin}(\tau)$ для моделі *Face Recognition*

**Оцінка екстрактора фіч**

Існує багато методів оцінки точності цих нейронних мереж. На перший погляд, можна застосувати оцінку $F_1$ [27] або просто використати значення $\alpha_{bin}(\tilde{\tau})$. Однак нам потрібно оцінити не те, наскільки точно модель класифікує бінарно, а наскільки схожі два вектори, коли вони відповідають зображенням однієї людини, і наскільки вони відрізняються, коли відповідають зображенням різних людей. Таким чином, пропонуємо використовувати деяку неперервну функцію точності від двох зображень $\alpha_{\text{cont}}(I,J)$, яку будемо називати *неперервною точністю*. Насправді, побачимо, що $\alpha_{\text{cont}}$ та $\alpha_{\text{bin}}$ сильно відрізняються.

Наприклад, застосуємо наступну функцію:

$$\alpha_{cont}(I,J)=\begin{cases}\left[1-\left(\dfrac{d(I,J)}{\tilde{\tau}}\right)^{\eta_1}\right]_+, I\equiv J,\\ \left[1-\left(\dfrac{\tilde{\tau}}{d(I,J)}\right)^{\eta_2}\right]_+, I\not\equiv J.\end{cases}$$

де $[z]_+ := \max\{0,z\}$.

Ця функція зображена на рис. 3. Інтуїтивне пояснення таке: коли нейронна мережа виводить відстань, близьку до $\tilde{\tau}$, вона дуже невпевнена щодо свого вибору, тому точність нижча порівняно з випадком, коли вона виводить значення, яке далі від $\tilde{\tau}$ (звичайно, у

правильному напрямку). Зауважимо, що функція також має два гіперпараметри $\eta_1$ та $\eta_2$, які використовуються для створення великого нахилу поблизу $\tilde{\tau}$ та меншого нахилу далі від $\tilde{\tau}$.

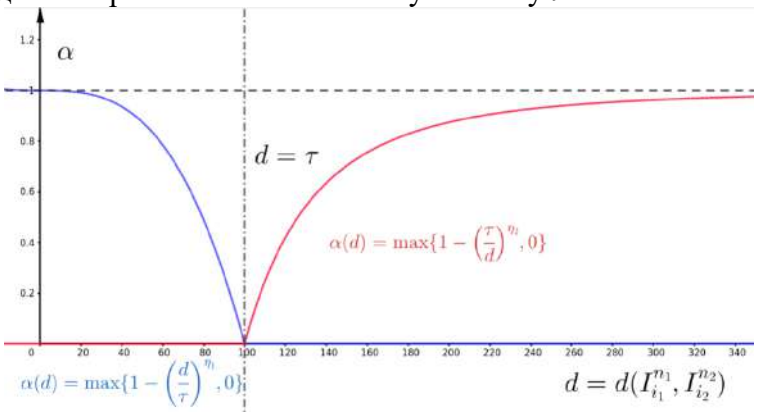


Рис. 3. Залежність $\alpha_{\text{cont}}(d)$ для $\eta_1 = \eta_2 = 3, \tilde{\tau} = 100$.
Синім відмічено випадок $I \equiv J$, червоним – $I \not\equiv J$

*Зауваження*: ця функція буде мати зміст лише для $\tilde{\tau}$, що максимізує двійкову точність. Дійсно, якщо, наприклад, покласти $\tau = 0$, то функція взагалі не буде визначена для випадку $I \equiv J$. Проте, якщо значення $\tilde{\tau}$ обрано таким чином, що двійкова точність вища за, скажімо, 90 % (хоча реальне значення близько 99 %), функція дає точне представлення ефективності екстрактора.

Визначимо кумулятивну точність за допомогою сформованого набору пар $P$. У цьому випадку визначимо загальну кумулятивну точність на наборі пар $A_{\text{cont}}$ як середньоквадратичне значення набору безперервних точностей, застосованих до кожної пари в цьому наборі:

$$A_{\text{cont}}^2 = \frac{1}{|P|} \sum_{p \in P} \alpha_{\text{cont}}^2 (I_{p(n_1),p(i_1)}, I_{p(n_2),p(i_2)}).$$

Також визначимо загальну кумулятивну двійкову точність $A_{\text{bin}}$ як просто бінарну точність при порозі $\tilde{\tau}$, тобто

$$A_{\text{bin}}(P) = \alpha_{\text{bin}}(P, \tilde{\tau}).$$

**Конвертер вектора фіч**

Як казали раніше, конвектор вектора фіч повинен, враховуючи дійсний вектор фіч $f(I)$, сформувати бінарну строку $s(I)$ довжини $n_s$, де $I$ – це зображення. Оскільки у нашому випадку $n_f = n_s = k = 128$, це суттєво спрощує задачу. Нехай маємо вектор

$$f(I) = \begin{bmatrix} f(I)_1 \\ f(I)_2 \\ \vdots \\ f(I)_k \end{bmatrix} \in \mathbb{R}^k$$

і нам потрібно сформувати

$$s(I) = \begin{bmatrix} s(I)_1 \\ s(I)_2 \\ \vdots \\ s(I)_k \end{bmatrix} \in \{0,1\}^k$$

згідно з деяким правилом $\phi: \square^k \to \{0,1\}^k$. В цьому випадку визначимо $\phi$ наступним чином:

$$s(I)_j = \begin{cases} 1, f(I)_j > 0 \\ 0, f(I)_j \le 0 \end{cases}.$$

Також визначимо бінарну відстань $\delta(I,J)$ між зображеннями $I$ та $J$ як

$$\delta(I,J) = \frac{1}{k}\sum_{j=1}^{k} \left| s(I)_j - s(J)_j \right|.$$

Аналогічно можемо визначити схожість зображень $\sigma(I,J)$ як $\sigma(I,J) = 1 - \delta(I,J)$.

Подивимося, який результат отримаємо, застосовуючи $\phi$ до деяких зображень із нашого набору даних. Як можна побачити з рис. 4, два двійкові рядки однієї особи майже збігаються. Згідно з нашим визначенням подібність між цими двома зображеннями становить приблизно 86 %, що є відносно хорошим результатом. Але для двох різних людей, наприклад як показано на рис. 5, двійкові рядки суттєво відрізняються, і в наведеному прикладі подібність дорівнює 50 %, що є відносно невеликим значенням, як і очікувалося.


Рис. 4. Бінарна строка для пари зображень однієї особи.
Зеленим позначено однакові символи, а червоним – різні.
Для демонстрації включено лише 36 рядкових символів


Рис. 5. Бінарна строка для пари зображень двох різних людей.
Зеленим позначено однакові символи, а червоним – різні.
Для демонстрації включено лише 36 рядкових символів

Оцінимо точність такого конвертера на більшому наборі даних. По-перше, пропонуємо розділити множину пар $P$ на дві інші множини: $P_{same}$ – набір пар зображень однієї особи та $P_{diff}$ – набір пар зображень різних людей, згідно з тим, як ми формували набір пар $P$, $|P_{same}| = |P_{diff}| = |P|/2$.

Для оцінки точності будемо використовувати два значення: $\sigma_{same}$ – середня схожість між бінарними строками, сформованими для множини пар однієї людини, і $\sigma_{diff}$ – для множини пар різних людей. Визначимо їх наступним чином:

$$\sigma_{same} = \frac{1}{\left|P_{same}\right|} \sum_{p \in P_{same}} \sigma\left(I_{p(n_1),p(i_1)}, I_{p(n_2),p(i_2)}\right),$$

$$\sigma_{diff} = \frac{1}{\left|P_{diff}\right|} \sum_{p \in P_{diff}} \sigma\left(I_{p(n_1),p(i_1)}, I_{p(n_2),p(i_2)}\right).$$

**Результати експериментів**

У табл. 1 – 4 включено всі базові параметри, описані раніше для двох наборів даних (*lfw* і *CelebA*) і двох моделей (*Keras Facenet* і *Face Recognition*). Для обох наборів даних використано приблизно 1 тисячу зображень (тобто майже однакову кількість пар).

Таблиця 1

Бінарна точність

| Набір даних | Keras Facenet | Face Recognition |
|---|---|---|
| Lfw | 99.3% | 98.2% |
| CelebA | 94.8% | 93.2% |

Таблиця 2

Неперервна точність

| Набір даних | Keras Facenet | Face Recognition |
|---|---|---|
| Lfw | 84.0% | 81.9% |
| CelebA | 75.8% | 74.8% |

Таблиця 3

Схожість пар зображень однієї людини

| Набір даних | Keras Facenet | Face Recognition |
|---|---|---|
| Lfw | 77.3% | 88.8% |
| CelebA | 73.7% | 88.5% |

Таблиця 4

Схожість пар зображень двох різних людей

| Набір даних | Keras Facenet | Face Recognition |
|---|---|---|
| Lfw | 50.8% | 79.7% |
| CelebA | 51.7% | 80.9% |

Як бачимо, для всіх наборів даних двійкова точність обох моделей перевищує 93 %. Однак безперервна точність нижча, і це логічний результат, оскільки безперервна точність завжди повинна мати менше значення. Це досягається завдяки тому, що ми визначили двійкову відстань як середнє значення одиниць і нулів, тоді як при застосуванні формули безперервної точності всі нулі залишаються нулями, але всі одиниці відображаються на інтервал (0,1), який завжди не перевищує 1. Ця точність завжди відносно висока для обох моделей, але в наборі даних *CelebA* маємо значення близько 75 %.

Щодо значень $\sigma$, модель *Keras* має значну перевагу над моделлю *Face Recognition*: за нашим правилом $\phi$, ця модель видає найбільше значення $\sigma_{\text{same}} - \sigma_{\text{diff}}$, що перевищує 20 %. В свою чергу, модель *Face Recognition* має значну меншу різницю, яка навіть менша за 10 %. Можливо, інший спосіб визначення $\phi$ може зробити модель *Face Recognition* більш точною, оскільки її бінарна точність більша за модель *Keras,* і це є чудовою темою для майбутніх публікацій.

Для збільшення значення різниці для подальших досліджень потрібно визначити $\phi$ більш складним способом, а саме – створити нейронну мережу, яка навчиться максимізувати точність перетворювача.

Реалізацію функцій і методів, згаданих у попередніх розділах, можна знайти у [28].

**Code based нечіткий екстрактор**

У статті [8] запропоновано новий нечіткий екстрактор криптографічно надійних ключів із біометричних даних. Цей екстрактор використовує криптосистему на основі коду McEliece [9].

Кожен сформований біометричний двійковий вектор інтерпретуємо як слово [8]:

$$B^* = I \cdot G_X + e^* . \quad (1)$$

Якщо ми використовуємо допоміжну строку, ми припускаємо, що слово $B^*$ складається з спотвореної вектором $e^*$ частини $B_k^*$ та несекретної допоміжної строки $P_{n-k} = I \cdot G_{X_2} = B_k \cdot G_{X_1}^{-1} \cdot G_{X_2}$, де [8]:

- матриця $G_{X_1}$ сформована $k$ рядками матриці $G_X$, номери стовпців відповідають довільно обраними $k$ позиціями вектору $B$;
- матриця $G_{X_2}$ сформована $n-k$ колонками, що залишились від матриці (1);
- матриця $G_X$ це публічний ключ в криптосистемі McEliece.

**Показники ефективності біометричного екстрактора**

Важливими характеристиками біометричної автентифікації є частота помилкових відхилень (FRR) і частота помилкових прийомів (FAR):

- FRR – характеризує рівень помилкових відмов, тобто це ймовірність того, що біометрична система помилково відхилить спробу доступу авторизованого користувача;
- FAR – характеризує рівень помилкових акцептів, тобто це ймовірність того, що біометрична система помилково прийме спробу доступу неавторизованого користувача.

Для оцінки цих ймовірностей розглянемо два випадки.

Припустимо, що в результаті сканування та обробки біометричних даних сформовано двійковий рядок (1), де вага Хеммінга (кількість ненульових позицій) вектора помилок $e^*$ характеризує можливі відмінності $B^*$ з еталонним біометричним набором $B$.

Кількість ненульових позицій вектору $e^*$ визначається ймовірністю появи ненульового символу в $e^*$, тобто ймовірність спотворення одного символу кодового слова $c_X = I \cdot G_X$. Для авторизованого та неавторизованого користувача ці ймовірності різні.

В и п а д о к 1. Нехай вектор (5) належить авторизованому користувачу. Позначимо ймовірність спотворення одного символу в $c_X$ як $p_0$. Тоді значення FRR можна оцінити за формулою [8]

$$FRR = 1 - \sum_{i=0}^{t} C_k^i p_0^{\,i} (1 - p_0)^{k-i} . \quad (2)$$

Табл. 3 надає емпіричну оцінку цієї ймовірності, отриману на наборах даних *Lfw* і *CelebA* з використанням моделей глибокого навчання *Keras Facenet* і *Face Recognition*. Бачимо, що для різних варіантів обробки біометричних ознак оцінка ймовірності $p_0$ дещо відрізняється. Приймаємо оцінку ймовірності $p_0$ за критерієм мінімального ризику, тобто розглядаємо найгірший сценарій (з найбільшою ймовірністю):

- $p_0 \approx 0,263$ для моделі *Keras Facenet*;
- $p_0 \approx 0,125$ для моделі *Face Recognition*.

В и п а д о к 2 . Нехай вектор (1) належить неавторизованому користувачу. Позначимо ймовірність спотворення одного символу як $p_1$. Тоді значення FAR можна оцінити за формулою [8]

$$FAR = \sum_{i=0}^{t} C_k^i p_1^{\,i} (1-p_1)^{k-i} \ . \qquad (3)$$

Емпірична оцінка ймовірності $p_1$ наведена в табл. 4. Приймаємо оцінку ймовірності $p_1$ за критерієм мінімального ризику, тобто розглядаємо найгірший сценарій (найменшої ймовірності):

- $p_1 \approx 0,483$ для моделі *Keras Facenet*;
- $p_1 \approx 0,191$ для моделі *Face Recognition*.

Завдання екстрактора полягає в мінімізації FRR і FAR для різної довжини згенерованих паролів і різних ймовірностей $p_0$ та $p_1$.

**Оцінка та порівняння FRR та FAR**

Розглянутий екстрактор заснований на використанні кодових криптосистем, які використовують лінійний блок $(n, k, d = 2t+1)$ із швидким (поліноміальної складності) декодуванням. Найбезпечнішим варіантом вважається використання двійкового коду Goppa з параметрами

$$(n, k, d) = (2^m, 2^m - mt, 2t+1)$$

для деякого додатного цілого $m$.

У експериментах ми сформували бінарні строки довжини $n = 128$, тобто для $m = 7$. У табл. 5 показано параметри $k, d$ кодів Гоппи для різних значень $t$. У таблиці також наведено розрахункові значення FRR і FAR для різних випадків. У таблиці виділено випадок із FRR ≈ FAR.

Таблиця 5

Оцінки FRR та FAR для різних кодів Гоппи довжини 128

| *t* | *k* | *d* | Keras Facenet | | Face Recognition | |
|---|---|---|---|---|---|---|
| | | | FRR | FAR | FRR | FAR |
| 8 | 72 | 17 | 0.9987 | 1.88E-11 | 0.5532 | 0.0512 |
| 9 | 65 | 19 | 0.9877 | 4.94E-09 | **0.2912** | **0.1800** |
| 10 | 58 | 21 | 0.9262 | 8.09E-07 | 0.1026 | 0.4368 |
| 11 | 51 | 23 | 0.7229 | 7.60E-05 | 0.0212 | 0.7417 |
| 12 | 44 | 25 | 0.3663 | 0.0036 | 0.0022 | 0.9366 |
| 13 | 37 | 27 | **0.0830** | **0.0744** | 8.18E-05 | 0.9939 |
| 14 | 30 | 29 | 4.66E-03 | 0.5023 | 6.85E-07 | 0.9999 |
| 15 | 23 | 31 | 1.77E-05 | 0.9673 | 3.63E-10 | 1.0000 |

**Висновки**

У статті розглянуто застосування моделей глибокого навчання *Keras Facenet* і *Face Recognition* для генерації криптографічно надійних послідовностей (ключів, пін-кодів, паролів). У експериментах використовувались набори даних *Lfw* і *CelebA* з нечітким екстрактором на основі криптосистем на основі коду з [8]. Досягнуті результати демонструють перспективність даної теми та можливість використання в різних криптографічних додатках. Наприклад, вдосконалення систем авторизації доступу за паролем, генерування первинної ентропії в криптографічних алгоритмах тощо.

Розглянуто різні варіанти побудови нечіткого екстрактора з кодами Гоппи довжиною 128 біт. Найефективнішими виявилися: за співвідношенням FRR і FAR – модель глибокого навчання *Keras Facenet* і криптосистеми на основі коду з використанням допоміжного рядка

– (128, 37, 27) коду Гоппи з формуванням 37-бітного пароля. Це забезпечує можливість помилок FRR ≈ FAR < 10%.

Перспективним напрямком подальших досліджень є використання криптосистем із кодами Гоппи значно більшої довжини. Це значно зменшить ймовірність FRR і FAR. Крім того, цікавим напрямком досліджень є алгоритми багатофакторної автентифікації з формуванням криптографічно надійних ключів.

**Список літератури:**


1. S. Chakraborty and D. Das. An Overview of Face Liveness Detection // arXiv:1405.2227 [cs], May 2014, Accessed: Feb. 12, 2021. [Online]. Available: http://arxiv.org/abs/1405.2227
2. C. Rathgeb and A. Uhl. A survey on biometric cryptosystems and cancelable biometrics // EURASIP Journal on Information Security, vol. 2011, no. 1, p. 3, Sep. 2011, doi: 10.1186/1687-417X-2011-3.
3. U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain. Biometric cryptosystems: issues and challenges // Proceedings of the IEEE, vol. 92, no. 6, pp. 948–960, Jun. 2004, doi: 10.1109/JPROC.2004.827372.
4. M. Lutsenko, A. Kuznetsov, A. Kiian, O. Smirnov, and T. Kuznetsova. Biometric Cryptosystems: Overview, State-of-the-Art and Perspective Directions // Advances in Information and Communication Technology and Systems, Cham, 2021, pp. 66–84. doi: 10.1007/978-3-030-58359-0_5.
5. Z. Jin, A. B. J. Teoh, B.-M. Goi, and Y.-H. Tay. Biometric cryptosystems: A new biometric key binding and its implementation for fingerprint minutiae-based representation // Pattern Recognition, vol. 56, pp. 50–62, Aug. 2016, doi: 10.1016/j.patcog.2016.02.024.
6. M. Lutsenko, A. Kuznetsov, Y. Gorbenko, I. Oleshko, Y. Pronchakov, and Y. Kotukh. Key Generation from Biometric Data of Iris // 2019 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo), Sep. 2019, pp. 1–6. doi: 10.1109/UkrMiCo47782.2019.9165457.
7. A. Kuznetsov, I. Oleshko, K. Chernov, M. Bagmut, and T. Smirnova. Biometric Authentication Using Convolutional Neural Networks // Advances in Information and Communication Technology and Systems, Cham, 2021, pp. 85–98. doi: 10.1007/978-3-030-58359-0_6.
8. A. Kuznetsov, A. Kiyan, A. Uvarova, R. Serhiienko, and V. Smirnov. New Code Based Fuzzy Extractor for Biometric Cryptography // 2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S T), Oct. 2018, pp. 119–124. doi: 10.1109/INFOCOMMST.2018.8632040.
9. R. J. McEliece. A Public-Key Cryptosystem Based On Algebraic Coding Theory // Deep Space Network Progress Report, vol. 44, pp. 114–116, Jan. 1978.
10. R. Overbeck and N. Sendrier. Code-based cryptography // Post-Quantum Cryptography. D. Bernstein, J. Buchmann and E. Dahmen, Eds. Berlin, Heidelberg: Springer, 2009, pp. 95–145. doi: 10.1007/978-3-540-88702-7_4.
11. W. Wang, J. Szefer, and R. Niederhagen. FPGA-Based Niederreiter Cryptosystem Using Binary Goppa Codes // Post-Quantum Cryptography, Cham, 2018, pp. 77–98. doi: 10.1007/978-3-319-79063-3_4.
12. M. Bardet, J. Chaulet, V. Dragoi, A. Otmani and J.-P. Tillich. Cryptanalysis of the McEliece Public Key Cryptosystem Based on Polar Codes // Post-Quantum Cryptography, Cham, 2016, pp. 118–143. doi: 10.1007/978-3-319-29360-8_9.
13. I. von Maurich, L. Heberle, and T. Güneysu. IND-CCA Secure Hybrid Encryption from QC-MDPC Niederreiter // Post-Quantum Cryptography, Cham, 2016, pp. 1–17. doi: 10.1007/978-3-319-29360-8_1.
14. D. Moody and R. Perlner. Vulnerabilities of 'McEliece in the World of Escher // Post-Quantum Cryptography, Cham, 2016, pp. 104–117. doi: 10.1007/978-3-319-29360-8_8.
15. D. J. Bernstein, J. Buchmann, and E. Dahmen, Eds. Post-Quantum Cryptography. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009. doi: 10.1007/978-3-540-88702-7.
16. T. Takagi, Ed., Post-Quantum Cryptography, vol. 9606. Cham: Springer International Publishing, 2016. doi: 10.1007/978-3-319-29360-8.
17. V. M. Sidelnikov and S. O. Shestakov. On insecurity of cryptosystems based on generalized Reed-Solomon codes // Discrete Mathematics and Applications, vol. 2, no. 4, pp. 439–444, Jan. 1992, doi: 10.1515/dma.1992.2.4.439.
18. N. Sendrier. Niederreiter Encryption Scheme // Encyclopedia of Cryptography and Security, H. C. A. van Tilborg and S. Jajodia, Eds. Boston, MA: Springer US, 2011, pp. 842–843. doi: 10.1007/978-1-4419-5906-5_385.
19. R. Canto Torres and N. Sendrier. Analysis of Information Set Decoding for a Sub-linear Error Weight // Post-Quantum Cryptography, Cham, 2016, pp. 144–161. doi: 10.1007/978-3-319-29360-8_10.
20. Classic McEliece: Intro. https://classic.mceliece.org/index.html (accessed Feb. 12, 2021).
21. Classic McEliece: NIST submission. https://classic.mceliece.org/nist.html (accessed Feb. 12, 2021).
22. F. Schroff, D. Kalenichenko, and J. Philbin. FaceNet: A unified embedding for face recognition and clustering // 2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Jun. 2015, pp. 815–823. doi: 10.1109/CVPR.2015.7298682.
23. Machine Learning is Fun! Part 4: Modern Face Recognition with Deep Learning ; by Adam Geitgey ; Medium https://medium.com/@ageitgey/machine-learning-is-fun-part-4-modern-face-recognition-with-deep-learning-c3cffc121d78 (accessed Sep. 02, 2022).

24. Y. Taigman, M. Yang, M. Ranzato, and L. Wolf. DeepFace: Closing the Gap to Human-Level Performance in Face Verification // 2014 IEEE Conference on Computer Vision and Pattern Recognition, Jun. 2014, pp. 1701–1708. doi: 10.1109/CVPR.2014.220.

25. G. B. Huang, M. Mattar, T. Berg, and E. Learned-Miller. Labeled Faces in the Wild: A Database forStudying Face Recognition in Unconstrained Environments // presented at the Workshop on Faces in "Real-Life" Images: Detection, Alignment, and Recognition, Oct. 2008. Accessed: Sep. 02, 2022. [Online]. Available: https://hal.inria.fr/inria-00321923

26. Z. Liu, P. Luo, X. Wang, and X. Tang. Deep Learning Face Attributes in the Wild // arXiv, Sep. 24, 2015. doi: 10.48550/arXiv.1411.7766.

27. A. A. Taha and A. Hanbury. Metrics for evaluating 3D medical image segmentation: analysis, selection, and tool // BMC Medical Imaging, vol. 1, no. 15, pp. 1–28, 2015, doi: 10.1186/s12880-015-0068-x.

28. D. Zakharov. Binary Encoder // Sep. 02, 2022. Accessed: Sep. 04, 2022. [Online]. Available: https://github.com/ZamDimon/Binary-Encoder

29. J. H. van Lint and G. van der Geer. Classical Goppa codes // Introduction to Coding Theory and Algebraic Geometry, J. H. van Lint and G. van der Geer, Eds. Basel: Birkhäuser, 1988, pp. 22–24. doi: 10.1007/978-3-0348-9286-5_5.

30. A. Kuznetsov, A. Kiian, V. Babenko, I. Perevozova, I. Chepurko, and O. Smirnov. New Approach to the Implementation of Post-Quantum Digital Signature Scheme // 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), May 2020, pp. 166–171. doi: 10.1109/DESSERT50317.2020.9125053.

31. G. Hua. Facial Recognition Technologies // Encyclopedia of Big Data, L. A. Schintler and C. L. McNeely, Eds. Cham: Springer International Publishing, 2022, pp. 475–479. doi: 10.1007/978-3-319-32010-6_93.

32. C. Libby and J. Ehrenfeld. Facial Recognition Technology in 2021: Masks, Bias, and the Future of Healthcare // J Med Syst, vol. 45, no. 4, p. 39, Feb. 2021, doi: 10.1007/s10916-021-01723-w.

33. K. A. Gates. Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance. NYU Press, 2011.

34. P. J. Grother, M. L. Ngan, and K. K. Hanaoka. Ongoing Face Recognition Vendor Test (FRVT. Part 2: Identification // NIST, Nov. 2018, Accessed: Aug. 26, 2022. [Online]. Available: https://www.nist.gov/publications/ongoing-face-recognition-vendor-test-frvt-part-2-identification.

*Надійшла до редколегії 11.05.2023*

*Відомості про авторів:*

**Кузнецов Олександр Олександрович** – д-р техн. наук, професор, Харківський національний університет імені В.Н. Каразіна, професор кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук; Україна; e-mail: kuznetsov@karazin.ua, ORCID: https://orcid.org/0000-0003-2331-6326

**Захаров Дмитро Олегович –** Харківський національний університет імені В.Н. Каразіна, студент 2-го курсу, кафедра прикладної математики; Україна; e-mail: zamdmytro@gmail.com, ORCID: https://orcid.org/my-orcid?orcid=0000-0001-9519-2444

**УДК 004.056.5** **DOI:10.30837/rt.2023.2.213.04**

*О.І. ПЕЛЮХ, М.В. ЄСІНА, канд. техн. наук, Д.Ю. ГОЛУБНИЧИЙ, канд. техн. наук*

# ОЦІНКА CERT-UA НА ОСНОВІ МОДЕЛІ ЗРІЛОСТІ CSIRT ENISA

## Вступ

Відкритість та підключеність до глобальної мережі стали невід'ємною частиною сучасного світу, але разом з цим зростають і загрози, пов'язані з кібербезпекою. Кіберінциденти, такі як: хакерські атаки, витоки даних та викрадення конфіденційної інформації, стають все поширенішими й складнішими. У боротьбі з цими загрозами вирішальну роль відіграє ефективне реагування на кіберінциденти.

У цьому контексті оцінка команди з реагування на кіберінциденти набуває все більшої важливості. Команда з реагування складається з експертів з кібербезпеки, інженерів з мережі, аналітиків та інших фахівців, які працюють разом для виявлення, аналізу та врегулювання кіберінцидентів. Ефективна команда з реагування може швидко усунути загрозу, зменшуючи шкоду та відновлюючи нормальне функціонування систем.

Метою статті є розгляд важливості оцінки команди з реагування на кіберінциденти. Розглянемо ключові аспекти, які необхідно враховувати при оцінці команди, такі як навички, досвід, комунікація та співпраця за допомогою оновленої Моделі зрілості CSIRT ENISA [1]. Розглянуто інструменти та методики, що допомагають оцінити ефективність команди з реагування та виявити слабкі місця, які можна вдосконалити, що спрямовані на предмет статті – CERT-UA та урядова команда реагування на комп’ютерні надзвичайні події України, яка функціонує в складі Державної служби спеціального зв’язку та захисту інформації України [2].

Оцінка команди з реагування на кіберінциденти є необхідним етапом для будь-якої організації, яка прагне забезпечити свою безпеку та захистити свої цінності в кіберпросторі. Вона сприяє постійному вдосконаленню та зміцненню необхідних навичок та зусиль для готовності до реагування на небезпеки. Розуміння важливості оцінки команди з реагування допоможе організаціям стати більш впевненими в здатності захистити свою інформацію та протистояти кіберзагрозам у сучасному цифровому світі.

## 1. Модель зрілості CSIRT ENISA

### 1.1. Загальні відомості про Модель зрілості ENISA CSIRT

Модель зрілості ENISA CSIRT сприяє зміцненню глобальної спроможності управляти кіберінцидентами з фокусом на CSIRT (Команди реагування на кіберінциденти) [1]. Вона базується на стандарті OCF SIM [3] і пропонує трирівнений підхід до зрілості, разом з методологією оцінки ENISA. Ця модель не є нормативною або стандартизованою, але надає орієнтири для підвищення зрілості CSIRT та є цінним джерелом рекомендацій. Вона поєднує в собі попередні моделі, що мають широке визнання й вжиток.

Модель, що розглядається у цій роботі, містить у своїй основі три визначні складові:

- стандарт Моделі зрілості управління безпековими інцидентами SIM3 [3];
- трирівневий підхід до оцінки зрілості команди [4];
- унікальна методологія оцінювання [5].

Розглянемо суть кожного із наведених пунктів для повного розуміння Моделі й подальшого її використання для оцінки рівня зрілості CERT-UA.

### 1.2. Модель зрілості управління безпековими інцидентами SIM3

SIM3, або Модель зрілості управління інцидентами безпеки, є основою для оцінки зрілості можливостей організації щодо реагування на інциденти. Це широко прийнята модель, яку використовують організації всіх розмірів, від малого бізнесу до великих підприємств [1, 3]. SIM3 базується на чотирьох квадрантах (категоріях):

- Організаційний («O»).

Цей квадрант оцінює загальний підхід організації до управління інцидентами, включаючи її політики, процедури та ресурси.

- Людський фактор («Н»).

У цьому квадранті оцінюються навички та знання людей, залучених до реагування на інциденти, включаючи їхню підготовку, досвід і здатність до спільної роботи.

- Інструменти («Т»).

У цьому квадранті оцінюються інструменти та технології, які організація використовує для підтримки реагування на інциденти, включаючи їх можливості, зручність використання та інтеграцію з іншими системами.

- Процеси («Р»).

Цей квадрант оцінює процеси реагування на інциденти в організації, включаючи їх ефективність, результативність і масштабованість.

Слід зазначити, що оновлена Модель зрілості ENISA CSIRT використовує SIM3v2i – модернізовану версію SIM3, що має додатковий параметр (О–6). Загалом стандарт складається із 45 параметрів, що охоплюють усі чотири зазначені квадранти. Нижче наведений повний перелік параметрів SIMv2i [1] – табл.1.

Таблиця 1

Параметри SIMv2i

| Номер параметра | Опис параметра | Номер параметра | Опис параметра |
|---|---|---|---|
| О–1 | Повноваження | Т–6 | Стійкість обміну повідомленнями |
| О–2 | Виборчий округ | Т–7 | Стійкість доступу в Інтернет |
| О–3 | Управління | Т–8 | Інструментарій для запобігання інцидентам |
| О–4 | Обов’язки | Т–9 | Інструментарій для виявлення інцидентів |
| О–5 | Опис послуги | Т–10 | Інструментарій для усунення інцидентів |
| О–6 | Публічна медіаполітика | Р–1 | Перехід на рівень управління |
| О–7 | Опис рівня обслуговування | Р–2 | Перехід до служби ЗМІ |
| О–8 | Класифікація інциденту | Р–3 | Перехід до юридичної служби |
| О–9 | Участь в системах CSIRT | Р–4 | Процес запобігання інцидентам |
| О–10 | Організаційна модель | Р–5 | Процес виявлення інцидентів |
| О–11 | Політика безпеки | Р–6 | Процес усунення інцидентів |
| Н–1 | Кодекс поведінки/практики/етики | Р–7 | Конкретні процеси обробки інцидентів |
| Н–2 | Стійкість персоналу | Р–8 | Процес аудиту та зворотного зв'язку |
| Н–3 | Опис набору навичок | Р–9 | Процес забезпечення доступності в надзвичайних ситуаціях |
| Н–4 | Розвиток персоналу | Р–10 | Найкращі методи забезпечення присутності в Інтернеті |
| Н–5 | Технічна підготовка | Р–11 | Безпечний процес обробки інформації |
| Н–6 | Розвиток соціально-комунікативних навичок | Р–12 | Процес пошуку джерел інформації |
| Н–7 | Зовнішні зв’язки | Р–13 | Процес інформаційно-просвітницької роботи |
| Т–1 | ІТ-ресурси та конфігурація | Р–14 | Процес звітування з питань управління |
| Т–2 | Список джерел інформації | Р–15 | Процес звітування виборчих округів |
| Т–3 | Консолідована система (–и) обміну повідомленнями | Р–16 | Процес проведення зустрічей |
| Т–4 | Система відслідковування інцидентів | Р–17 | Процес співпраці за принципом «рівний–рівному» |
| Т–5 | Надійність голосових дзвінків | | |

Кожен параметр квадранту поділяється на рівні від 0 до 4, де 0 – найнижчий рівень зрілості, а 4 – найвищий [1, 3 – 5]. Загальний рівень зрілості організації визначається як середнє арифметичне балів за всіма чотирма квадрантами. Шкала вимірювання наведена у табл. 2.

Таблиця 2

Шкала вимірювання рівня параметрів SIMv2i

| Рівень | Статус | Основні критерії |
|---|---|---|
| 0 | Недоступний / невизначений / невідомий | Відсутнє будь-яке розуміння параметра і його важливості в цілому. |
| 1 | Неявний | Наявне розуміння важливості, але жодним чином не задокументоване. |
| 2 | Явний, внутрішній | Наявність будь-якого документа, що не був формально погоджений із CSIRT. |
| 3 | Явний, формалізований на підставі повноважень керівника CSIRT | Наявність будь-якого документу, офіційно затвердженого керівництвом CSIRT. Якщо документ був офіційно затверджений на організаційному рівні, який є ієрархічно вищим, але в тій самій гілці організаційної структури організації, цей документ автоматично є дійсним і для CSIRT та її керівництва – проте, якщо він має безпосереднє відношення до справи, бажано, щоб керівництво CSIRT в будь-якому випадку схвалило цей документ і, наприклад, розмістило його на вікі-сторінці команди. |
| 4 | Чіткий, активно оцінюваний на регулярній основі авторитет рівнів управління над керівництвом CSIRT | Аналогічно рівню 3, але документ регулярно оцінюється на рівні керівництва вище за керівництво CSIRT. |

SIM3 можна використовувати для оцінки спроможності організації реагувати на інциденти в будь-який час, але найчастіше її застосовують для порівняння прогресу з плином часу. Регулярно оцінюючи свій рівень зрілості, організації можуть визначити сфери, які потребують вдосконалення, і зробити цільові інвестиції, щоб поліпшити свої загальні можливості реагування на інциденти, зокрема у кіберпросторі.

### 1.3. Трирівневий підхід у визначенні етапів зрілості CSIRT

Стадії зрілості CSIRT – це спосіб вимірювання зрілості команди реагування на інциденти комп'ютерної безпеки. Трирівневий підхід до етапів зрілості CSIRT базується на моделі зрілості SIM3 [1, 3 – 5], яка є результатом зусиль спільноти з вимірювання зрілості CSIRT. Існує три стадії зрілості, кожна з яких має свою характеристику, що наведена у табл. 3.

Таблиця 3

Етапи зрілості у Моделі зрілості ENISA CSIRT

| Рівень | Опис |
|---|---|
| Базовий | Команда має обмежене розуміння у реагуванні на інциденти та не здатна ефективно на них реагувати. На цьому рівні розпочато роботу над усіма параметрами з чітким фокусом на завдання та інших формальних аспектах ролі команди. Приблизно 80% організаційних параметрів уже опрацьовано до такої міри, що їх можна вважати "просунутими". |
| Проміжний | Команда має краще розуміння ніж на «Базовому» етапі й краще реагує на інциденти. На основі виконаної роботи було досягнуто прогресу за всіма параметрами, окрім тих, що вже знаходяться на "просунутому" рівні. Загалом, приблизно 50 % «H», «P» і «T» параметрів можна вважати "просунутими". |
| Просунутий | Команда має глибоке розуміння процедури реагування на інциденти та здатна максимально ефективно на них реагувати. Більшість з параметрів SIM3 має найвищий, 4-й рівень, однак деякі вкраплення 3-го рівня допускаються. |

Кожна стадія зрілості визначається набором параметрів, яким повинна відповідати CSIRT. Ці параметри для кожної стадії зрілості ґрунтуються на моделі зрілості SIM3 і охоплюють цілий ряд, зазначений у п. 1.2. У [1] наведено таблицю, що показує необхідний рівень кожного із параметрів SIM3v2i, залежно від етапу зрілості команди реагування на інциденти. Детальні критерії для оцінки кожного з параметрів наведені у [4, 5].

Використання трирівневого підходу до етапів зрілості CSIRT у комбінації із параметрами SIM3 має наступні значні переваги:

- забезпечення структурованої основи для оцінки можливостей реагування на інциденти;
- допомога організаціям та командам з реагування визначити сфери для вдосконалення;

- потенційне використання у якості індикатора прогресу команди через певний проміжок часу.

### 1.4. Методологія оцінки Моделі зрілості ENISA CSIRT

Наведена система зрілості CSIRT у контексті оцінки використовує збалансований симбіоз самооцінки й експертної думки [1, 4]. Автори заявляють, що така методологія є доволі збалансованою та правильною, адже шляхом самооцінки команда рефлексує, у той час як експертний погляд допомагає більш критично оцінити загальну ситуацію в команді, що оцінюється. Пропоновані складові методології оцінки виглядають наступним чином:

- Система зрілості CSIRT надає можливість оцінити зрілість CSIRT шляхом самооцінки, що є першим кроком.

Самооцінка корисна для встановлення базової, але більш суб'єктивної оцінки для внутрішнього аналізу. Вона також може слугувати відправною точкою для підвищення рівня зрілості. Результати самооцінки використовуються для розробки плану дій з визначеними часовими рамками для досягнення вищого рівня зрілості. Також можна порівняти результати оцінки з іншими CSIRT, використовуючи Модель зрілості як орієнтир. Етапи зрілості, визначені в Моделі зрілості CSIRT, є прикладом належних практик, що слугують орієнтиром для національних CSIRT. Деякі параметри можуть мати меншу вагу для конкретної команди, в той час як інші є основою для стратегії.

- У якості другого кроку в оцінці, що передбачено Моделлю зрілості CSIRT, є експертна оцінка.

Національні CSIRT можуть звернутися до інших команд з проханням провести експертну оцінку їхньої самооцінки. Це можна зробити, запрошуючи групу колег, серед яких є досвідчені співробітники, які мають знання та досвід в оцінці зрілості CSIRT. Експертна оцінка проходить більш ефективно, якщо представники команди та експертів обох сторін ознайомлені з Моделлю зрілості CSIRT. Тому рекомендується активно брати участь у формальному та неформальному навчанні, що стосується використання цих оцінок.

По-перше, самооцінка часто буває упередженою. Люди схильні переоцінювати власні можливості, і це може призвести до неточної оцінки зрілості. З іншого боку, експертна оцінка забезпечує зовнішній і критичний погляд, який може допомогти пом'якшити цю упередженість.

По-друге, експертна оцінка може допомогти виявити "сліпі зони". Коли CSIRT проводить самооцінку, вона може не знати про всі свої слабкі сторони. Експертна оцінка може допомогти виявити ці слабкі сторони, які потім можуть бути усунені для підвищення зрілості CSIRT.

Додатково необхідно визначити наступне:

- Вагомість двох форм оцінки може змінюватися залежно від конкретних обставин.

Наприклад, якщо CSIRT є новою і має обмежений досвід, може бути важливіше покладатися на самооцінку, щоб отримати уявлення про власні можливості. Однак, у міру того, як CSIRT стає більш зрілою, може виявитися більш важливим покладатися на експертну оцінку для отримання об'єктивної оцінки рівня її зрілості.

- Вагомість цих двох форм оцінювання також може змінюватися залежно від конкретної мети оцінювання.

Наприклад, якщо оцінка проводиться для того, щоб визначити, чи відповідає CSIRT певним вимогам відповідності, слід більше покладатися на самооцінку. Якщо оцінка проводиться для визначення сфер, в яких CSIRT може покращити свою роботу, краще покластися на експертну оцінку.

Зрештою, рішення про те, як зважити ці дві форми оцінки, є складним і повинно прийматися в кожному конкретному випадку окремо.

Отже, Модель, наведена у [1], є динамічною структурою, що активно використовується не лише приватними компаніями, а й урядовими організаціями.

## 2. Оцінка CERT-UA

### 2.1. Загальні відомості про CERT-UA

CERT-UA, або Команда реагування на комп'ютерні надзвичайні події України, – це організація, що підтримується урядом і надає консультації з реагування на інциденти та безпеки організаціям в Україні. CERT-UA була заснована у 2007 р. і з 2009 р. є членом Форуму команд реагування на інциденти та безпеки (FIRST) [2, 7]. Послуги CERT–UA включають:

- реагування на інциденти: CERT-UA може допомогти організаціям розслідувати та реагувати на кіберінциденти;
- консультування з питань безпеки: CERT-UA може надати організаціям поради щодо покращення їхньої системи безпеки;
- навчання: CERT-UA пропонує навчальні курси з різних тем безпеки;
- публікації: CERT-UA публікує різноманітні матеріали, пов'язані з безпекою, включаючи інформаційні бюлетені, звіти та технічні документи;
- CERT-UA є цінним ресурсом для організацій в Україні, які шукають допомоги з реагування на інциденти та забезпечення безпеки. Послуги організації доступні як державним, так і приватним організаціям.

Отже, можна стверджувати, що CERT-UA є певним аналогом національної CSIRT, а значить, не лише можливо, а й важливо оцінити рівень зрілості CERT-UA за допомогою запропонованої моделі від ENISA. Однак, через певний ступінь конфіденційності внутрішніх документів організації, неможливо надати вичерпну й точну оцінку. Тому нижче наводиться приблизна оцінка етапу зрілості команди CERT-UA, заснована на інформації, що доступна на офіційному сайті організації [2].

### 2.2. Оцінка CERT-UA за допомогою SIM3v2i

Для спрощеної процедури оцінки команда SIM3 розробила сайт [6], що допомагає швидко та якісно пройти оцінювання й отримати діаграму.

Таблиця 4

Оцінка CERT-UA за допомогою параметрів SIM3v2i

| Параметр | Рівень | Обґрунтування |
|---|---|---|
| O-1 | 4 | Організація підпорядковується Державній службі спеціального зв’язку та захисту інформації України та має чітко визначені завдання. |
| O-2 | 4 | Згідно з нормативно-правовою базою організації чітко визначено цільову групу розповсюдження послуг CERT-UA. |
| O-3 | 3 | Наявне письмове затвердження повноважень на сайті, але у жодному із документів чітко не зазначено про дозволені дії. |
| O-4 | 4 | Існують чітко сформовані й задокументовані визначення від органу, вищого за рангом (Державна служба спеціального зв’язку та захисту України). |
| O-5 | 4 | Наявний офіційний сайт із зазначенням послуг, контактів для зв’язку, тощо. |
| O-6 | 3 | Простежується наявність медіа-політики, але існує значна відмінність у висвітленні різних інцидентів/новин. |
| O-7 | 4 | Наявні контакти, графіки роботи й можливість отримання цілодобової допомоги. |
| O-8 | 4 | Класифікація зазначена серед нормативно-правових документів, в межах яких організація здійснює свою діяльність. |
| O-9 | 4 | CERT-UA є акредитованим членом FIRST протягом останніх 14 років. |
| O-10 | – | Відсутній загальний доступ до документу, що визначає внутрішню організаційну структуру. |
| O-11 | 4 | Політика безпеки зазначена у нормативно-правових документах. |
| H-1 | 3 | Кодекс поведінки базується на засадах FIRST. |
| H-2 | – | Відсутній загальний доступ до документу, що визначає внутрішню організаційну структуру. |

Продовження табл. 4

| Параметр | Рівень | Обґрунтування |
|---|---|---|
| Н-3 | 3 | Опис навичок можливо сформувати на основі деяких організаційних параметрів. |
| Н-4 | 4 | Розвиток забезпечений основними положеннями членства у FIRST й нормативно-правовою базою діяльності організації. |
| Н-5 | 4 | Розвиток забезпечений основними положеннями членства у FIRST й нормативно-правовою базою діяльності організації. |
| Н-6 | 2 | Розвиток забезпечений основними положеннями членства у FIRST, але чітко не є визначеним |
| Н-7 | 4 | CERT-UA є акредитованим членом FIRST протягом останніх 14 років й активно співпрацює із Форумом. |
| Т-1 | 4 | Визначено нормативно-правовою базою діяльності організації. |
| Т-2 | 4 | Джерела інформації окреслені нормативно-правовими документами. |
| Т-3 | – | Відсутня загальнодоступна інформація з цього приводу. |
| Т-4 | 4 | Послужний список реагування на інциденти в кіберпросторі дає впевненість у наявності чіткої, постійно обновлюваної системи. |
| Т-5 | – | Відсутня загальнодоступна інформація з цього приводу. |
| Т-6 | – | Відсутня загальнодоступна інформація з цього приводу. |
| Т-7 | – | Відсутня загальнодоступна інформація з цього приводу. |
| Т-8 | 3 | Послужний список реагування на інциденти в кіберпросторі дає впевненість у наявності певного набору інструментів для запобігання інцидентам. |
| Т-9 | 3 | Послужний список реагування на інциденти в кіберпросторі дає впевненість у наявності певного набору інструментів для виявлення інцидентів. |
| Т-10 | 3 | Послужний список реагування на інциденти в кіберпросторі дає впевненість у наявності певного набору інструментів для вирішення інцидентів. |
| Р-1 | 4 | Визначено нормативно-правовою базою діяльності організації. |
| Р-2 | 3 | Наявна велика кількість прикладів взаємодії зі ЗМІ, що вказує на існування письмового процесу. |
| Р-3 | 4 | Визначено нормативно-правовою базою діяльності організації. |
| Р-4 | 3 | Наявні інструкції із запобігання деяким інцидентам. |
| Р-5 | 3 | Реальні приклади дозволяють засвідчити наявність певного письмового процесу з виявлення інцидентів. |
| Р-6 | 4 | Визначено нормативно-правовою базою діяльності організації. |
| Р-7 | 3 | Доступні офіційні процеси реагування на інциденти. |
| Р-8 | 4 | Наявний регулярний і прогресуючий процес зворотного зв’язку через контактні джерела й ЗМІ. |
| Р-9 | 3 | Існує джерело для надання цілодобової консультації та підтримки. |
| Р-10 | 3 | Аналіз соціальних мереж CERT-UA надає розуміння наявності певного формального процесу для формування процесу присутності в Інтернеті. |
| Р-11 | 4 | Наявні оновлюванні бібліотеки процесів шифрування та підпису повідомлень. |
| Р-12 | 3 | Аналіз прикладів реагування на інциденти показує існування таких процесів. |
| Р-13 | 2 | Складно стверджувати про ефективність чи наявність процесу масового охоплення. |
| Р-14 | -- | Відсутня загальнодоступна інформація з цього приводу. |
| Р-15 | 3 | Наявне часткове інформування громадян про інциденти та шляхи їх усунення. |
| Р-16 | -- | Відсутня загальнодоступна інформація з цього приводу. |
| Р-17 | 4 | CERT-UA є акредитованим членом FIRST протягом останніх 14 років. |

Отже, через деякі обмеження в доступі та наявності, частина параметрів, а саме: О-10, Н-2, Т-3-5-6-7, Р-14-16 не можуть бути оцінені належним чином. Слід зауважити, що загальний відсоток параметрів, що були оцінені на основі сайту організації, нормативно-правових документів, тощо, складає 82 %.

### 2.3. Узагальнення отриманих результатів

Наведена нижче кругова діаграма показує визначені рівні параметрів CERT-UA. Діаграма була створена на основі даних, отриманих у табл. 4.

Слід зазначити, що діаграма не містить параметрів, оцінка яких відсутня. Наступним кроком для узагальнення є визначення рівнів кожного із квадрантів за допомогою середнього арифметичного значення та медіани. Ця інформація систематизована у табл. 5.

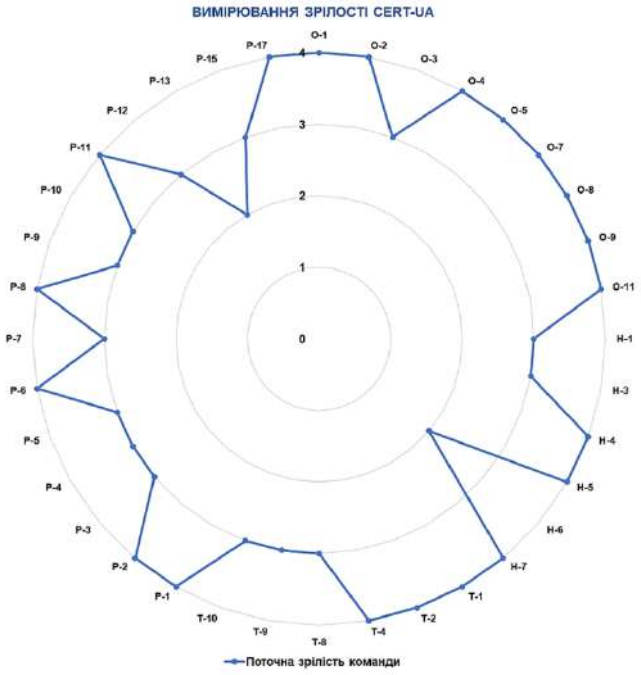


Рис. 1. Отримана діаграма рівнів параметрів CERT–UA

Таблиця 5

Рівні квадрантів параметрів CERT-UA

| Квадрант параметрів | Середнє арифметичне | Медіана вибірки | Рівень-відповідник |
|---|---|---|---|
| Організаційний («О») | 3,9 | 4 | «Просунутий» |
| Людський фактор («Н») | 3,3 | 3 | «Просунутий» |
| Інструменти («Т») | 3,5 | 3 | «Просунутий» |
| Процеси («Р») | 3,3 | 3 | «Проміжний» |

Отже, згідно з отриманими результатами оцінки й критеріями, висунутими у [1, 3 – 5], спостерігається «Просунутий» рівень 3 з 4 категорій CERT-UA. Квадрант, що відповідає за процеси, відповідає рівню «Проміжний» й потребує покращень процедур або їх часткового висвітлення для ознайомлення широкого загалу. Загалом, зрілість CERT-UA знаходиться на межі «Просунутого» рівня, однак потребує деяких покращень параметрів у категорії «Р».

**Висновки**

1. Модель зрілості CSIRT ENISA є цінним інструментом для покращення зрілості CSIRT. Це комплексна та гнучка модель, яка може бути використана CSIRT будь-якого розміру. Модель також підкріплена методологією оцінки, яка допомагає оцінити поточний рівень команди.

2. SIM3 є цінним інструментом для організацій, які прагнуть поліпшити свої можливості реагування на інциденти. Модель є комплексною, гнучкою та простою у використанні. Використовуючи SIM3, організації можуть визначити області для вдосконалення і зробити відповідні кроки для поліпшення своїх загальних можливостей реагування на інциденти.

3. Трирівневий підхід до етапів зрілості CSIRT в поєднанні з параметрами SIM3 є цінним інструментом для вимірювання зрілості команди реагування на інциденти комп'ютерної безпеки. Модель є структурованою, комплексною та простою у використанні.

4. Вага самооцінки та експертної оцінки у методології має бути різною, із наданням переваги експертній оцінці. Однак вагомість цих двох форм оцінювання може змінюватися залежно від конкретних обставин і мети оцінювання.

5. CERT-UA є цінним ресурсом в Україні, націленим на допомогу в реагуванні на інциденти та забезпеченні безпеки. Послуги організації доступні як державним, так і приватним організаціям, вона має широкий спектр можливостей, включаючи реагування на інциденти, консультування з питань безпеки, навчання та сповіщення про актуальні новини.

6. Через обмежений доступ до певної документації вдалося оцінити лише 82 % параметрів для CERT-UA. Параметри, які не вдалося оцінити, були такими: O-10, H-2, T-3, T-5, T-6, T-7, P-14, P-16.

7. Попри обмеженість оцінювання можна зробити деякі висновки щодо рівня зрілості CERT-UA. Організація має чітке розуміння своєї ролі та обов'язків, а також чітко визначений процес реагування на інциденти. Однак є деякі сфери, в яких CERT-UA може покращити свій рівень зрілості. Наприклад, організація могла б покращити свою документацію та зробити її більш доступною.

8. Систематизовані результати показують, що рівень зрілості CERT-UA знаходиться на рівні "Просунутий" у трьох з чотирьох квадрантів: «O», «H» та «T». Рівень зрілості у квадранті «P» знаходиться на "Проміжному" рівні. Це свідчить про те, що CERT-UA має міцну основу з точки зору організаційної структури, людських ресурсів та інструментів. Однак слід покращити свій рівень зрілості шляхом подальшого розвитку ефективності деяких процесів.

**Список літератури:**


1. ENISA CSIRT Maturity Framework – Updated and improved, ENISA, Feb. 23, 2022. [Електронний ресурс]. Режим доступу: https://www.enisa.europa.eu/publications/enisa–csirt–maturity–framework.
2. CERT–UA, cert.gov.ua. [Електронний ресурс]. Режим доступу: https://cert.gov.ua/.
3. SIM3 : Security Incident Management Maturity Model – Open CSIRT Foundation. Mar. 30, 2015. [Електронний ресурс]. Режим доступу: https://opencsirt.org/csirt–maturity/sim3–and–references/.
4. ENISA CSIRT maturity assessment model. ENISA, Apr. 30, 2019. [Електронний ресурс]. Режим доступу: https://www.enisa.europa.eu/publications/study–on–csirt–maturity.
5. ENISA Maturity Evaluation Methodology for CSIRTs. ENISA, Apr. 09, 2019. [Електронний ресурс]. – Режим доступу: https://www.enisa.europa.eu/publications/study–on–csirt–maturity–evaluation–process.
6. SIM3v2i self–assessment tool. ENISA. [Електронний ресурс]. Режим доступу: https://www.enisa.europa.eu/topics/incident–response/csirt–capabilities/csirt–maturity/sim3–v2i.
7. FIRST – Improving Security Together. FIRST – Forum of Incident Response and Security Teams. [Електронний ресурс]. Режим доступу: https://www.first.org/.



*Надійшла до редколегії 25.05.2023*



*Відомості про авторів:*

**Пелюх Олександр Іванович** – Харківський національний університет імені В. Н. Каразіна, студент факультету комп'ютерних наук; Україна; e-mail: oleksandrpelyukh@gmail.com; ORCID: https://orcid.org/0000-0003-0507-0262.

**Єсіна Марина Віталіївна** – канд. техн. наук, Харківський національний університет імені В.Н. Каразіна, доцент кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук; науковий співробітник-консультант АТ «Інститут Інформаційних технологій»; Україна; e-mail: m.v.yesina@karazin.ua; ORCID: https://orcid.org/0000-0002-1252-7606

**Голубничий Дмитро Юрійович** – канд. техн. наук, доцент, начальник наукового відділу АТ "Інститут Інформаційних Технологій"; Україна; e-mail: goldim1971@gmail.com; ORCID: https://orcid.org/0000-0002-6873-7004

**УДК 621.391:519.2** **DOI:10.30837/rt.2023.2.213.05**

*Є.В. КОТУХ, канд. техн. наук, Г.З. ХАЛІМОВ, д-р техн. наук,*
*М.В. КОРОБЧИНСЬКИЙ, д-р техн. наук*

# ПОБУДОВА ТРЬОХПАРАМЕТРИЧНОЇ СХЕМИ ШИФРУВАННЯ НА ГРУПАХ ЕРМІТА В КРИПТОСИСТЕМІ MST3

## Вступ

У статті пропонується метод побудови трьохпараметричної схеми шифрування на групах Ерміта, що вдосконалює параметри безпеки існуючої криптосистеми MST3. Завдання вдосконалення існуючих підходів до побудови криптосистем зумовлено успіхами в побудові квантового комп'ютера з достатньою обчислювальною потужністю, що зробить багато криптосистем із відкритим ключем незахищеними. Зокрема мова йде про ті криптосистеми, що базуються на складності факторизації або проблемі дискретного логарифмування, такі як RSA, ECC тощо. Існує кілька пропозицій, які стали класичними за останні майже 20 років, щодо використання некомутативних груп для побудови квантовостійких криптосистем [1 – 4]. Нерозв'язна проблема слова є цікавою областю дослідження для побудови криптосистеми. Вона була сформульована Вагнером і Магьяриком, досліджена у [5, 6] і лежить у площині застосування груп перестановок. Вперше логарифмічні сигнатури (LS) були запропоновані Магліверасом. У цьому контексті логарифмічна сигнатура є особливим типом факторизації, вона застосовується до кінцевих груп. Покращення оригінальної версії криптосистеми запропоновано в [7, 8]. Остання версія цієї реалізації відома як MST3 [9] і базується на групі Сузукі.

У 2008 р. Магліверас продемонстрував обмеження транзитивного використання LS для криптосистеми MST3. Пізніше Сваба запропонував криптосистему eMST3 з покращеними параметрами безпеки. Для цього вдосконалення було додано секретне гомоморфне покриття. Потім, у 2018 р., Т. ван Трунг запропонував підхід MST3 з використанням сильних аперіодичних LS для абелевих *p*-груп. Конг з колегами провели широкий аналіз MST3 і відзначили, що, оскільки на даний момент немає публікацій про квантову вразливість алгоритму, його можна вважати кандидатом на постквантовий період.

Оригінальний підхід до побудови криптосистеми MST3 базується на групі Сузукі. В рамках доповідей на конференції було розглянуто результати дослідницької роботи, що демонструє подальше вдосконалення MST3 [10 – 19]. Однією з цінних ідей є підвищення ефективності шифрування шляхом оптимізації накладних витрат на обчислення. Це зроблено зі зменшенням великого розміру ключового простору. Цей підхід можна застосовувати для обчислень LS за межами центру групи. І це було зроблено над кінцевими полями малої розмірності з використанням груп з великим порядком.

Групи Сузукі ізоморфні проєктивній лінійній групі $PGL\left(3,F_q\right)$, $q_0=2^n$, де $q=2q_0^2$ і має порядок $q^2$. Безпека криптосистеми на групах визначається саме груповим порядком. У [13] автори вперше запропонували використання трьохпараметричної групи автоморфізму для вдосконалення параметрів безпеки криптосистеми MST3.

Особливістю пропозиції є те, що $H\left(P_\infty\right)$ має ще $Herm\left|F_{q^2}\right.$ більший порядок $ordH\left(P_\infty\right)=q^3\left(q^2-1\right)$ ніж порядок відповідної групи Сузукі, яка розглядається в оригінальних статтях. Наукова новизна пропозиції полягає в тому, що стаття представляє практичну реалізацію цього нового підходу.

## Використання трьохпараметричної групи автоморфізмів функціонального поля Ерміта

Розглянемо $Herm\left|F_{q^2}\right.$ [14]. Використовуємо $Aut\left(Herm\right)$ у $Herm\left|F_{q^2}\right.$, і це можна представити як $H:=Aut\left(Herm\right)=\left\{\psi:Herm\mapsto Herm\left|\psi\ \text{з}\ Herm\right|F_{q^2}\right\}$. Властивості автоморфізмів обговорювалися

в [14]. Порядок цієї групи $ordA = q^3\left(q^2-1\right)\left(q^3+1\right)$. Група розкладання $H\left(P_\infty\right)$ має всі автоморфізми $Aut\left(Herm\right)$ з $Herm\left|F_{q^2}\right.$ та такі властивості:

$$\begin{cases} \psi(y) = \alpha y + \beta \\ \psi(z) = \alpha^{q+1} z + \alpha\beta^q y + \gamma, \end{cases}$$

де $\alpha \in F_{q^2}^* := F_{q^2} \setminus \{0\}$, $\beta \in F_{q^2}$ і $\gamma^q + \gamma = \beta^{q+1}$.

Порядок групи дорівнює $ordH\left(P_\infty\right) = q^3\left(q^2-1\right)$. Структуру групи представимо виразом

$$[\alpha_1,\beta_1,\gamma_1]\cdot[\alpha_2,\beta_2,\gamma_2] = \left[\alpha_1\alpha_2, \alpha_2\beta_1+\beta_2, \alpha_2^{q+1}\gamma_1 + \alpha_2\beta_2^q\beta_1 + \gamma_2\right].$$

Таким чином, маємо тотожність $[1,0,0]$ та інверсію $[\alpha,\beta,\gamma]$:

$$[\alpha,\beta,\gamma]^{-1} = \left[\alpha^{-1}, -\alpha^{-1}\beta, \alpha^{-(q+1)}\gamma^q\right],$$

$H\left(P_\infty\right)$ можна представити простіше:

$$H\left(P_\infty\right)\left\{\left[\alpha,\beta,\frac{\beta^{q+1}}{2}+\gamma\right]\middle|\alpha\in F_{q^2}^*, \beta\in F_{q^2},\ \gamma^q+\gamma=0\right\}.$$

Унікальна *p*-Sylow підгрупа $H\left(P_\infty\right)$ може бути позначена в $H_1\left(P_\infty\right)$ межах представлення $H_1\left(P_\infty\right) = \left\{\psi \in H\left(P_\infty\right)\middle|\psi(y) = y+\beta \text{ для деяких } b\in F_{q^2}\right\}$.

У такому випадку маємо порядок, що дорівнює $q^3$ для унікальної *p*-Sylow підгрупи:

$$\begin{cases} \psi(y) = y + \beta \\ \psi(z) = z + \beta^q y + \gamma, \end{cases}$$

де $\beta \in F_{q^2}$ і $\gamma^q + \gamma = \beta^{q+1}$, а порядок дорівнює $q^3$, як ми згадували вище. Структура для групи може бути досягнута шляхом представлення підгрупи PGL(3, *k*)*:*

$$H_1 := \left\{\begin{pmatrix} 1 & \beta & \gamma \\ 0 & 1 & \beta^q \\ 0 & 0 & 1 \end{pmatrix},\ \gamma\in F_{q^2}, \gamma^q+\gamma=\beta^{q+1}\right\}.$$

Групова операція визначається як $[1,\beta_1,\gamma_1]\cdot[1,\beta_2,\gamma_2] = \left[1,\beta_1+\beta_2,\gamma_1+\beta_2^q\beta_1+\gamma_2\right]$ та $[\beta_1,\gamma_1]\cdot[\beta_2,\gamma_2] = \left[\beta_1+\beta_2,\gamma_1+\beta_2^q\beta_1+\gamma_2\right]$. Група факторизації $H\left(P_\infty\right)/H_1\left(P_\infty\right)$ є циклічною за порядком $q^2-1$. Крім того, вона була створена за $\varsigma\in H\left(P_\infty\right)$ допомогою $\varsigma(y)=\alpha z,\ \varsigma(z)=\alpha^{q+1}z$. Інший автоморфізм $\zeta\in H$ задано $\zeta(y)=y/z,\ \zeta(z)=1/z$. Група автоморфізмів $H\left(P_\infty\right)$ ермітового функціонального поля $Herm\left|F_{q^2}\right.$, що визначає його $\psi(y),\psi(z)$, має порядок $ordH\left(P_\infty\right) = q^3\left(q^2-1\right)$ більший, ніж порядок групи Сузукі.

**Метод, що пропонується**

Отже, у рамках цієї пропозиції маємо наступні етапи генерації ключів, шифрування та дешифрування.

Маємо велику групу $H\left(P_\infty\right)$. Ця група заснована на автоморфізмі $\psi(y),\psi(z)$. Побудова елементів групи $H\left(P_\infty\right)$ визначається розв'язуванням рівняння $\gamma^q+\gamma=\beta^{q+1}$ відносно $\gamma$. Складність знаходження *c* пропорційна $q$. $H\left(P_\infty\right)$ з $Herm\left|F_{q^2}\right.$ можуть бути представлені так:

$$H\left(P_\infty\right) = \left\{\left[\alpha,\beta,\frac{\beta^{q+1}}{2}+\gamma\right]\middle|\alpha\in F_{q^2}^*, \beta\in F_{q^2},\ \gamma^q+\gamma=0\right\}.$$

І це вірно для непарної характеристики. Якщо $\lambda$ – твірний елемент поля, то рівняння $\gamma^q+\gamma=0$ має розв'язання $\gamma_i = \lambda^{(q+1)/2+k(q+1)}$, $k=\overline{0,q-1}$. Обчислювальні вектори з використанням матриць LS і випадкових покриттів (RC) транскодуються в координати $\beta,\gamma$ підгрупи $H\left(P_\infty\right)$.

Групова операція визначається як

$$S(\alpha_1,\beta_1,\gamma_1)\cdot S(\alpha_2,\beta_2,\gamma_2)=S\left(\alpha_1\alpha_2,\alpha_2\beta_1+\beta_2,\alpha_2^{q+1}\gamma_1+\alpha_2\beta_2^q\beta_1+\gamma_2\right).$$

Інверсія до $S(\alpha,\beta,\gamma)^{-1}=S\left(\alpha^{-1},-\alpha^{-1}\beta,-\alpha^{-(g+1)}\gamma+\alpha^{-(g+1)}\beta^{q+1}\right)$.

Обчислення оберненого елемента $S(\alpha,\beta,\gamma)^{-1}$ в цьому представленні розширює область для $\gamma_1=\frac{\beta_1^{q+1}}{2}+\gamma'_1$ і $\gamma_2=\frac{\beta_2^{q+1}}{2}+\gamma'_2$. Це ключова ідея в побудові LS на групі $H(P_\infty)$ на основі $Herm\left|F_{q^2}\right.$.

В іншому випадку, якщо $\gamma'_1$ і $\gamma'_2$ є розв'язанням рівняння $\gamma^q+\gamma=0$, обернений елемент строго визначається через вираз $S(\alpha,\beta,\gamma)^{-1}=S\left(\alpha^{-1},-\alpha^{-1}\beta,\alpha^{-(q+1)}\gamma^q\right)$.

Як вихід ми маємо $[w,\gamma,f]$ як відкритий ключ із відповідним секретним ключем $\left[v,(\tau_0,...,\tau_s)\right]$. Для генерації ключів застосовуємо наступні кроки:

1. Обираємо першу просту LS: $v_{(1)}=\left[V_{1(1)},...,V_{s(1)}\right]=(v_{kn})_{(1)}=S\left(1,v_{kn(1)},v_{kn(1)}^{q+1}/2\right)$ типу $\left(r_{1(1)},...,r_{s(1)}\right)$, $k=\overline{1,s(1)}$, $n=\overline{1,r_{i(1)}}$, $v_{kn(1)}\in F_{q^2}$.

2. Обираємо другу просту LS: $v_{(2)}=\left[V_{1(1)},...,V_{s(2)}\right]=(v_{kn})_{(2)}=S\left(1,0,v_{kn(2)}\right)$ типу $\left(r_{1(2)},...,r_{s(2)}\right)$, $k=\overline{1,s(2)}$, $n=\overline{1,r_{i(2)}}$, $v_{kn(2)}\in F_q\subset F_{q^2}$.

3. Обираємо перше RC: $w_{(1)}=\left[W_{1(1)},...,W_{s(1)}\right]=(w_{kn})_{(1)}=S\left(w_{kn(1)_1},w_{kn(1)_2},\left(w_{kn(1)_2}\right)^{q+1}/2\right)$ того ж типу, що й $v_{(1)}$, де $w_{kn}\in H(P_\infty)$, $w_{kn(1)_1},w_{kn(1)_2}\in F_{q^2}\setminus\{0\}$.

4. Обираємо друге RC: $w_{(2)}=\left[W_{1(2)},...,W_{s(2)}\right]=(w_{kn})_{(2)}=S\left(w_{kn(2)_1},w_{kn(2)_2},\left(w_{kn(2)_2}\right)^{q+1}/2+w_{kn(2)_3}\right)$ того ж типу, що $v_{(2)}$, де $w_{kn(2)_2},w_{kn(2)_3}\in F_q\setminus\{0\}\subset F_{q^2}$.

5. Обираємо: $\tau_{0(l)},\tau_{1(l)},...,\tau_{s(l)}\in H(P_\infty)\setminus Z$, $\tau_{i(l)}=S\left(\tau_{i(l)_1},\tau_{i(l)_2},(\tau_{i(l)_2})^{q+1}/2\right)$, $t_{i(l)_k}\in F^\times$, $i=\overline{0,s(l)}$, $l=\overline{1,2}$. Домовимося, що $\tau_{s(1)}=\tau_{0(2)}$.

6. Будуємо гомоморфізм $f_1$, що визначається $f_1\left(S\left(w_1,w_2,w_2^{q+1}/2\right)\right)=S\left(1,w_2,w_2^{q+1}/2\right)$.

7. Обчислюємо $g_{(1)}=\left[g_{1(1)},...,g_{s(1)}\right]=(g_{kn})_{(1)}=\tau_{(k-1)(1)}^{-1}f_1\left((w_{kn})_{(1)}\right)(v_{kn})_{(1)}\tau_{k(1)}$, $k=\overline{1,s(1)}$, $n=\overline{1,r_{i(1)}}$, де $f_1\left((w_{kn})_{(1)}\right)(v_{kn})_{(1)}=S\left(1,w_{kn(1)_2}+v_{kn(1)},w_{kn(1)_2}^{q+1}/2+w_{kn(1)_2}v_{kn(1)}^q+v_{kn(1)}^{q+1}/2\right)$.

8. Визначимо гомоморфізм $f_2\left(S\left(w_1,w_2,w_2^{q+1}/2\right)\right)=S\left(1,0,w_2\right)$ та обчислимо

$$g_{(2)}=\left[g_{1(2)},...,g_{s(2)}\right]=(g_{kn})_{(2)}=\tau_{(k-1)(2)}^{-1}f_2\left((w_{kn})_{(2)}\right)(v_{kn})_{(2)}\tau_{k(2)},\ k=\overline{1,s(2)},\ n=\overline{1,r_{i(2)}},$$

де $f_2\left((w_{kn})_{(2)}\right)v(b_{kn})_{(2)}=S\left(1,0,w_{kn(2)_2}+v_{kn(2)}\right)$.

В результаті виконання кроків 1 – 8 маємо відкритий ключ, що дорівнює $[f_1,f_2,(w_l,g_l)]$, та секретний ключ, що дорівнює $\left[v_{(l)},\left(\tau_{0(l)},...,\tau_{s(l)}\right)\right]$, $l=\overline{1,2}$. Генерацію ключів завершено. Розглянемо наступний етап реалізації нашого методу – шифрування.

Отже, як вхідні дані для шифрування маємо текст $x\in H(P_\infty)$ і $x=S(x_1,x_2,x_3)$, відкритий ключ $[f_1,f_2,(w_l,g_l)]$, $l=\overline{1,2}$. Для етапу шифрування необхідно виконати кроки:

1. Оберемо випадково $Q=(Q_1,Q_2)$, $Q_1\in Z_{\left|F_{q^2}\right|}$, $Q_2\in Z_{|\square|}$.

2. Обчислимо $y_1=w'(Q)\cdot x=w_1'(Q_1)\cdot w_2'(Q_2)\cdot x,$

$$y_2=g'(Q)=g_1'(Q_1)\cdot g_2'(Q_2)=S\left(*,w_{(1)_1}(Q_1)+v_{(1)}(Q_1)+*,w_{(2)_2}(Q_2)+v_{(2)}(Q_2)+*\right).$$

Перехресні розрахунки $\tau_{0(l)},...,\tau_{s(l)}$ використовуються для визначених $(*)$ компонентів та для додавання третьої координати в добуток $w_{(1)_1}(Q_1)+v_{(1)}(Q_1)$.

3. Обчислимо $y_3 = f_1\left(w_1'(Q_1)\right) = S\left(1, w_{(1)_2}(Q_1), *\right)$, $y_4 = f_2\left(w_2'(Q_2)\right) = S\left(1, 0, w_{(2)_2}(Q_2)\right)$.

Як результат обчислень маємо зашифрований вектор $(y_1, y_2, y_3, y_4)$ повідомлення $x$.

Перевіримо правильність запропонованого підходу на практиці.

Візьмемо кінцеве поле $F_{q^2}$, $q^2 = 3^6$, $g(z) = z^6 + 2z + 2$ та групу

$$H(P_\infty) = \left\{ \left[ \alpha, \beta, \frac{\beta^{q+1}}{2} + \gamma \right] \middle| \alpha \in F_{q^2}^*, \beta \in F_{q^2}, \ \gamma^q + \gamma = 0 \right\}.$$

Для групової операції використовуємо добуток двох матриць:

$$S(\alpha_1, \beta_1, \gamma_1) \cdot S(\alpha_2, \beta_2, \gamma_2) = S\left(\alpha_1\alpha_2, \alpha_2\beta_1 + \beta_2, \alpha_2^{q+1}\gamma_1 + \alpha_2\beta_2^q\beta_1 + \gamma_2\right).$$

$$S(a_1, b_1, c_1) \cdot S(a_2, b_2, c_2) = S\left(a_1a_2, a_2b_1 + b_2, a_2^{q+1}c_1 + a_2b_2^qb_1 + c_2\right),$$

де $\gamma_1 = \frac{\beta_1^{q+1}}{2} + \gamma'_1$, $\gamma_2 = \frac{\beta_2^{q+1}}{2} + \gamma'_2$.

Обернений елемент визначаємо як $S(\alpha,\beta,\gamma)^{-1} = S\left(\alpha^{-1}, -\alpha^{-1}\beta, \alpha^{-(q+1)}\gamma^q\right)$; $S(1,0,0)$ є трійкою і є тотожністю.

4. Побудуємо прості LS: $v_{(1)} = \left[V_{1(1)}, ..., V_{s(1)}\right] = (v_{kn})_{(1)} = S\left(1, v_{i_{kn}(1)}, v_{kn(1)}^{q+1}/2\right)$ типу $\left(r_{1(1)}, ..., r_{s(1)}\right)$, $k = \overline{1, s(1)}$, $n = \overline{1, r_{i(1)}}$, $v_{kn(1)} \in F_{q^2}$ для координати $\beta$ та $v_{(2)} = (v_{kn})_{(2)} = S\left(1, 0, v_{i_{kn}(2)}\right)$ типу $\left(r_{1(2)}, ..., r_{s(2)}\right)$, $k = \overline{1, s(2)}$, $n = \overline{1, r_{i(2)}}$, $v_{kn(2)} \in F_q \subset F_{q^2}$ для координати $\gamma$. LS $v_1$ і $v_2$ в групових представленнях визначають $v_{kn(1)}$ і $v_{kn(2)}$ координати. Типи $\left(r_{1(l)}, ..., r_{s(l)}\right)$ і LS $v_1$ і $v_2$ обираються самостійно. Нехай LS $v_1$ і $v_2$ мають типи $\left(r_{1(1)}, r_{2(1)}, r_{3(1)}\right) = \left(3^3, 3^2, 3\right)$, $\left(r_{1(2)}, r_{2(2)}\right) = \left(3^2, 3\right)$; масиви $v_{kn(1)}$ складаються з трьох підмасивів і $v_{kn(2)}$ мають два підмасиви з $r_i$ кількістю рядків. Будь-яку фрагментацію масивів можна обрати за умови $\prod_{i=1}^{s(1)} r_i = 3^6$ для $v_{kn(1)}$ і $\prod_{i=1}^{s} r_i = 3^3$ відповідно. Кожен рядок $v_{kn}$ – це $F_{q^2}$ елемент поля. Побудуємо масиви LS методом, який розглянуто у [2]. Для виконання та підвищення вимог безпеки масивів $v_l$ можемо використовувати різні криптографічні перетворення. Можемо просто додати вектори шуму, переставити рядки в підмасивах $V_i$, об'єднати масиви $V_i$ або використати матричні перетворення. Це допомагає створити дві різні LS: $v_1 = \left[V_{1(1)}, V_{2(1)}, V_{3(1)}\right]$ і $v_2 = \left[V_{1(2)}, V_{2(2)}\right]$. Масиви LS $v_1 = S\left(1, v_{kn(1)}, v_{kn(1)}^{q+1}/2\right)$ та $v_2 = S\left(1, 0, v_{kn(2)}\right)$ у груповому представленні визначають координати $v_{kn(1)}$ та $v_{kn(2)}$ відповідно.

5. Побудуємо RC $w_l$ для того самого типу, що і $v_1$ і $v_2$:

$$w_{(1)} = \left[W_{1(1)}, ..., W_{s(1)}\right] = (w_{kn})_{(1)} = S\left(w_{kn(1)_1}, w_{kn(1)_2}, \left(w_{kn(1)_2}\right)^{q+1}/2\right),$$

$$w_{(2)} = \left[W_{1(2)}, ..., W_{s(2)}\right] = (w_{kn})_{(2)} = S\left(w_{kn(2)_1}, w_{kn(2)_2}, \left(w_{kn(2)_2}\right)^{q+1}/2 + w_{kn(2)_3}\right),$$

де $w_{kn(1)_1}, w_{kn(1)_2} \in F_{q^2} \setminus \{0\}$, $w_{kn(2)_3} \in F_q \setminus \{0\} \subset F_{q^2}$, $k = \overline{1, s_{(l)}}$, $n = \overline{1, r_{k(l)}}$, $l = \overline{1, 2}$.

Ці покриття $w_l$ мають бути визначені трьома масивами $\left(w_{kn(l)_1}, w_{kn(l)_2}, w_{kn(l)_3}\right)$ з ненульовими записами.

6. Згенеруємо RC $w_1 = \left[W_{1(1)}, W_{2(1)}, W_{3(1)}\right]$, $w_2 = \left[W_{1(2)}, W_{2(2)}\right]$. У полі представлення $w_1 = S\left(w_{kn(1)_1}, w_{kn(1)_2}, w_{kn(1)_3}\right)$ і $w_2 = S\left(w_{kn(2)_1}, w_{kn(2)_2}, w_{kn(2)_3}\right)$ має вигляд: $\tau_{0(l)}, \tau_{1(l)}, ..., \tau_{s(l)} \in H(P_\infty) \setminus Z$, $\tau_{i(l)} = S\left(\tau_{i(l)_1}, \tau_{i(l)_2}, (\tau_{i(l)_2})^{q+1}/2\right)$, $\tau_{i(l)_k} \in F^\times$, $i = \overline{0, s(l)}$, $l = \overline{1, 2}$ буде обрано випадковим чином.

7. Припустимо, $\tau_{s(1)} = \tau_{0(2)}$. Нехай для 1-*ї* LS $\beta_1$ і для 2-ї LS $\beta_2$.

8. Масиви $g_1$ та, $g_2$, які потрібно обчислити на наступному кроці. Отже, отримуємо

$$g_{(1)} = \left[g_{1(1)}, ..., g_{s(1)}\right] = (g_{kn})_{(1)} = \tau_{(k-1)(1)}^{-1} f_1\left((w_{kn})_{(1)}\right)(v_{kn})_{(1)}\, \tau_{k(1)},$$

$$g_{(2)} = \left[g_{1(2)}, ..., g_{s(2)}\right] = (g_{kn})_{(2)} = \tau_{(k-1)(2)}^{-1} f_2\left((w_{kn})_{(2)}\right)(v_{kn})_{(2)}\, \tau_{k(2)}.$$

за умови наданого прикладу.

9. Побудуємо гомоморфізми $f_1$, $f_2$, визначені за

$$f_1\left(S\left(w_1, w_2, w_2^{q+1}/2\right)\right) = S\left(1, w_2, w_2^{q+1}/2\right),\ f_2\left(S\left(w_1, w_2, w_2^{q+1}/2\right)\right) = S\left(1, 0, w_2\right).$$

У полі представлення $g_1 = S(g_{kn(1)_1}, g_{kn(1)_2}, g_{kn(1)_3})$ і $g_2 = S(g_{kn(2)_1}, g_{kn(2)_2}, g_{kn(2)_3})$ мають матричний вигляд. Наприклад, нехай $Q_1 = 379$. Тоді отримуємо наступну базову факторизацію для заданого типу $\left(r_{1(1)}, r_{2(1)}, r_{3(1)}\right) = \left(3^3, 3^2, 3\right)$ у формі $Q_1 = \left(Q_{1(1)}, Q_{2(1)}, Q_{3(1)}\right) = (1,5,1)$, де $Q_1 + Q_2 3^3 + Q_3 3^5 = 379$.

Обчислюємо

$$g_1(379) = g_{1(1)}(1)\, g_{2(1)}(5)\, g_{3(1)}(1) = S\left(\alpha^{14}, \alpha^{150}, \alpha^{232}\right) S\left(\alpha^{499}, \alpha^{561}, \alpha^{678}\right) S\left(\alpha^{608}, \alpha^{24}, \alpha^{632}\right) = S\left(\alpha^{393}, \alpha^{91}, \alpha^{0}\right).$$

Нехай $R_2 = 17$. Отримуємо $Q_2 = \left(Q_{1(2)}, Q_{2(2)}\right) = (8,1) = 17$ для заданого типу $\left(r_{1(2)}, r_{2(2)}\right) = \left(3^2, 3\right)$.

Обчислюємо

$$g_2(17) = g_{1(2)}(8)\, g_{2(2)}(1) = S\left(\alpha^{147}, \alpha^{149}, \alpha^{328}\right) S\left(\alpha^{36}, \alpha^{697}, \alpha^{24}\right) = S\left(\alpha^{183}, \alpha^{192}, \alpha^{433}\right).$$

Розглянемо покроковий алгоритм шифрування. У $x_2, x_3 \in F_{q^2}$ маємо повідомлення $x \in N(P_\infty)$, $x = S(x_1, x_2, x_3)$, $x_1 \in F_{q^2} \setminus \{0\}$ і відкритий ключ $[f_1, f_2, (w_l, g_l)]$, $l = \overline{1,2}$ для введення. Нехай $x = \left(\alpha^1, \alpha^2, \alpha^3\right) = S\left(\alpha^1, \alpha^2, \alpha^3\right)$. $Q = (Q_1, Q_2) = (379,17)$, $Q_1 \in \square_{\left|F_{q^2}\right|}$, $Q_2 \in \square_{|F_q|}$ обираються випадковим чином. Для наступного кроку обчислимо:

$$y_1 = w'(Q) \cdot x = w_1'(Q_1) \cdot w_2'(Q_2) \cdot x = S\left(\alpha^{145}, \alpha^{602}, \alpha^{329}\right),$$

$$y_2 = g'(Q) = g_1'(Q_1) \cdot g_2'(Q_2) = S\left(\alpha^{576}, \alpha^{370}, \alpha^{226}\right),$$

$$y_3 = f_1\left(w_1'(Q_1)\right) = S\left(\alpha^{0}, \alpha^{394}, \alpha^{383}\right),$$

$$y_4 = f_2\left(w_2'(Q_2)\right) = S\left(\alpha^{0}, 0, \alpha^{692}\right).$$

Отримуємо зашифрований текст $(y_1, y_2, y_3, y_4)$ повідомлення $x$.

Розглянемо покроковий алгоритм дешифрування. Маємо зашифрований текст $(y_1, y_2, y_3, y_4)$ і закритий ключ $\left[v_l, \left(\tau_{0(l)}, ..., \tau_{s(l)}\right)\right]$ як вхідні дані. Випадкові числа $Q = (Q_1, Q_2)$ будуть відновлені наступними кроками для розшифровки повідомлення $x$:

$$D^{(1)}(Q_1, Q_2) = \tau_{0(1)} y_2 \tau_{s(2)}^{-1} = \tau_{0(1)} S\left(\alpha^{576}, \alpha^{370}, \alpha^{226}\right) \tau_{s(2)}^{-1} = S\left(\alpha^{0}, \alpha^{273}, \alpha^{139}\right),$$

$$D^{*}(Q) = y_3^{-1} D^{(1)}(Q_1, Q_2) = S\left(\alpha^{0}, \alpha^{30}, \alpha^{149}\right) S\left(\alpha^{0}, \alpha^{273}, \alpha^{139}\right) = S\left(\alpha^{0}, \alpha^{32}, \alpha^{408}\right).$$

Отримуємо $v_1(Q_1) = \alpha^{32} = (202211)$.

Відновлення $Q_1$ зроблено раніше: $Q_1 = \left(Q_{1(1)}, Q_{2(1)}, Q_{3(1)}\right) = (1,5,1)$.

Компоненти масивів $w_1'(Q_1)$ і $w_1'(Q_1)$ будуть видалені із зашифрованого тексту $(y_1, y_2)$ для подальших обчислень: $y_2^{(1)} = \gamma_1'(Q_1)^{-1} y_2 = S\left(\alpha^{393}, \alpha^{91}, \alpha^{0}\right)^{-1} S\left(\alpha^{576}, \alpha^{370}, \alpha^{226}\right) = S\left(\alpha^{183}, \alpha^{192}, \alpha^{433}\right)$.

Повторюємо обчислення

$$D^{(2)}(Q_2) = \tau_{0(2)} y_2^{(1)} \tau_{s(2)}^{-1} = \tau_{0(2)} S\left(\alpha^{183}, \alpha^{192}, \alpha^{433}\right) \tau_{s(l/2)}^{-1} = S\left(\alpha^{0}, 0, \alpha^{589}\right),$$

$$D^{*}(Q) = D^{(2)}(Q_2) y_4^{-1} = S\left(\alpha^{0}, 0, \alpha^{589}\right) S\left(\alpha^{0}, 0, \alpha^{692}\right)^{-1} = S\left(\alpha^{0}, 0, \alpha^{2}\right).$$

Відновимо $Q_2$ за допомогою $v_2(Q_2) = \alpha^2 = (001000)$.

Виконуємо обернені обчислення $v_2(Q_2)^{-1}$. Ми знайшли групи бітів $v(Q)$ відповідно до типу $\left(r_{1(2)}, ..., r_{s(2)}\right) = \left(3^2, 3\right)$. Те саме обчислення, яке буде використано в прикладі для $v_1(Q_1)^{-1}$. Тоді отримаємо $Q_2 = \left(Q_{1(2)}, Q_{2(2)}\right) = (8,1) = 17$.

Отримуємо відкрите повідомлення:

$$x = w'(Q)^{-1} y_1 = \left[w_1'(Q_1) \cdot w_2'(Q_2)\right]^{-1} \cdot y_1 = \left[S\left(\alpha^{391}, \alpha^{39}, \alpha^{36}\right) S\left(\alpha^{481}, \alpha^{52}, \alpha^{637}\right)\right]^{-1} S\left(\alpha^{145}, \alpha^{602}, \alpha^{329}\right) = S\left(\alpha^{1}, \alpha^{2}, \alpha^{3}\right)$$

*Вихід*: повідомлення $x = \left(\alpha^1, \alpha^2, \alpha^3\right)$.

**Аналіз безпеки запропонованого методу**

Розглянемо і опишемо можливі атаки. По-перше, атака, відома як груба сила (BFA), може бути виконана над зашифрованим текстом. Вибравши $Q=(Q_1,Q_2)$, спробуємо розшифрувати текст $y_1=w'(Q)\cdot x=w_1'(Q_1)\cdot w_2'(Q_2)\cdot x$. У цьому випадку складність атаки дорівнює $q^3$.

По-друге, варіант BFA на $Q=(Q_1,Q_2)$, знов обираємо такий $Q=(Q_1,Q_2)$, щоб знайти $y_2=g'(Q)=g_1'(Q_1)\cdot g_2'(Q_2)$. У цьому випадку складність атаки також дорівнює $q^3$.

По-третє, якщо вибрати $Q_1$ відповідним значенню $w_{(1)_2}(Q_1)$ у векторі $y_3=f_1(w_1'(Q_1))=S(1,w_{(1)_2}(Q_1),*)$. У цьому випадку складність атаки дорівнює $q^2$. Крім того, можемо спробувати вибрати $Q_2$ з відповідним значенням $w_{(2)_2}(Q_2)$ у векторі $y_4$. У цьому випадку він менш складний і дорівнює $q$. Ми розглядаємо можливість використання матричного перетворення як можливого механізму захисту.

Далі можемо застосувати BFA до $(\tau_{0(l)},...,\tau_{s(l)})$ векторів. У цьому випадку складність атаки дорівнює $(q^2)^2$.

Крім того, існує атака на сам алгоритм. Параметри вилучення $w_{(1)_1}(Q_1)$, $w_{(2)_2}(Q_2)$ з $y_3$, $y_4$ не дозволяють обчислити $w_1'(Q_1)\cdot w_2'(Q_2)$ в $y_1=w_1'(Q_1)\cdot w_2'(Q_2)\cdot x$. Якщо ми просто спробуємо знайти параметри $Q_1,Q_2$, потрібні зусилля на рівні BFA зі складністю $q^2$. $q^2$. Оскільки $H(P_\infty)$ з $Herm|F_{q^2}$ визначається над полем $F_{q^2}$, яке є достатньо великим, ця атака просто неможлива.

**Висновки**

Для криптосистеми $H(P_\infty)$ з використанням $\beta$ на основі $Herm|F_{q^2}$ маємо наступні висновки. В цьому випадку LS $v=[V_1,...,V_s]=(v_{kn})=S(1,v_{kn(2)}.v_{kn(3)}.)$ є підгрупою $H(P_\infty)=\{S(\alpha,\beta,\gamma)|\alpha,\beta\in F_{q^2},\gamma^q+\gamma=\beta\}$, а RC $w=[W_1,...,W_s]=(w_{kn})=S(w_{kn(1)},w_{kn(2)},w_{kn(3)})$ – однакового типу з $v$. Фактично, розмір масивів $v$ і $w$ визначається типом $(r_1,...,r_s)_2$ і $(r_1,...,r_s)_3$ для $\beta,\gamma$ в $H(P_\infty)$ підгрупах. Таким чином, вони обидва повинні бути перетворені в елементи груп. Розв'язок задачі знайдено для випадку, коли поле має непарну характеристику. Ця вимога залишається також для розширених груп автоморфізмів. Гомоморфізм $H(P_\infty)$ групи $Herm|F_{q^2}$ має просте представлення поля непарної характеристики. Вектори, що використовують матриці LS і RC, тепер легко транскодуються. І це дає нам координати підгрупи $H(P_\infty)$. В свою чергу це дає перевагу розміру повідомлення для запропонованої конструкції криптосистеми MST3. В рамках аналізу безпеки розглянуто різноманітні атаки на компоненти схеми шифрування. Отримані результати дають можливість стверджувати, що реалізація атак має високу складність.

**Список літератури:**


1. Kotukh Y., Severinov E., Vlasov O., Tenytska A., Zarudna E. Some results of development of cryptographic transformations schemes using non-abelian groups // Радіотехніка. 2021. Вип. 204. С. 66–72.
2. Котух Є., Сєвєрінов О., Власов А. та ін. Методи побудови та властивості логарифмічних підписів // Радіотехніка. 2021. Вип. 205. С. 94–99. https://doi.org/10.30837/rt.2021.2.205.09
3. Kotukh Y., Khalimov G. Hard Problems for Non-abelian Group Cryptography, 2021 // Fifth International Scientific and Technical Conference "Computer and Information systems and technologies". https://doi.org/10.30837/csitic52021232176
4. Халімов Г., Котух Є., Сергійчук Ю., Марухненко О. Аналіз складності реалізацій криптосистеми на групі Сузукі // Радіотехніка. 2018. Вип. 193. С. 75–81.
5. Котух Є., Охріменко Т., Дяченко О., Ротаньова Н., Козіна Л., Зеленський Д. Криптоаналіз систем на основі проблеми слова з використанням логарифмічних підписів // Радіотехніка. 2021. Вип. 206. С. 106–114. https://doi.org/10.30837/rt.2021.3.206.09
6. Kotukh Y., Khalimov G. Towards practical cryptoanalysis of systems based on word problems and logarithmic

signatures // Proceedings of II International Conference Information security: problems and prospects, 25 Nov 2022, Baku, Azerbaijan, pp. 55–58.

7. Magliveras S. New approaches to designing public key cryptosystems using one-way functions and trap-doors in finite groups / S. Magliveras, D. Stinson, T. van Trung // Journal of Cryptology. 2002. Vol. 15. P. 285–297.

8. Lempken W. A public key cryptosystem based on non-abelian finite groups / W. Lempken, T. Van Trung, S.S. Magliveras, W. Wei // Journal of Cryptology. 2009. Vol. 22 (1). P. 62–74.

9. Khalimov G., Kotukh Y. et al. Towards advance encryption based on a Generalized Suzuki 2-groups // 2021 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME). Mauritius, 2021, pp. 1–6. doi: 10.1109/ICECCME52200.2021.9590932.

10.Khalimov G., Kotukh Y., Khalimova S. $MST_3$ Cryptosystem Based on a Generalized Suzuki 2-Groups [Electronic resource]. Access mode : http://ceur-ws.org/Vol-2711/paper1.pdf

11.Khalimov G., Kotukh Y., Didmanidze I., Sievierinov O., Khalimova S. and Vlasov A. Towards three-parameter group encryption scheme for MST3 cryptosystem improvement // 2021 Fifth World Conference on Smart Trends in Systems Security and Sustainability (WorldS4), London, United Kingdom, 2021, pp. 204–211. doi: 10.1109/WorldS451998.2021.9514009.

12.Khalimov G., Kotukh Y., Didmanidze I., Khalimova S. 2021. Encryption scheme based on small Ree groups // Proceedings of the 2021 7th International Conference on Computer Technology Appli-cations (ICCTA '21). ACM, New York, NY, USA, 33–37. https://doi.org/10.1145/3477911.3477917

13.Khalimov G., Kotukh Y., Shonia O., Didmanidze I., Sievierinov O., Khalimova S. Encryption Scheme Based on the Automorphism Group of the Suzuki Function Field // 2020 IEEE PIC S&T, Kharkiv, Ukraine, 2020, pp. 383–387. doi: 10.1109/PICST51311.2020.9468089.

14.Khalimov G., Kotukh Y., Khalimova S. Encryption scheme based on the extension of automorphism group of the Hermitian function field // Book of Abstract 20th Central European Conference on Cryptology. 2020. P. 30–32.

15.Khalimov G., Kotukh Y. et al. (2022). Encryption Scheme Based on the Generalized Suzuki 2-groups and Homomorphic Encryption // Chang SY., Bathen L., Di Troia F., Austin T.H., Nelson A.J. (eds). Silicon Valley Cybersecurity Conference. SVCC 2021. Communications in Computer and Information Science, vol 1536. Springer, Cham. https://doi.org/10.1007/978-3-030-96057-5_5

16.Khalimov G., Sievierinov O., Khalimova S., Kotukh Y., Chang S.-Y. and Balytskyi Y. Encryption Based on the Group of the Hermitian Function Field and Homomorphic Encryption // 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T). Kharkiv, Ukraine, 2021, pp. 465–469. doi: 10.1109/PICST54195.2021.9772219.

17.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 and T Proceedings, 2019, pp. 865–868.

18.Khalimov G., Kotukh Y. and Khalimova S. Encryption scheme based on the automorphism group of the Ree function field // 2020 7th International Conference on Internet of Things: Systems, Management and Security (IOTSMS). Paris, France, 2020, pp. 1–8. doi: 10.1109/IOTSMS52051.2020.9340192.

19.Khalimov G., Kotukh Y., Khalimova S. Improved encryption scheme based on the automorphism group of the Ree function field field // 2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), IEEE Xplore. 2021.

*Надійшла до редколегії 27.05.2023*

*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

**Коробчинський Максим Володимирович** – д-р техн. наук, професор, начальник 2-ї кафедри 2-го навчального факультету Воєнної академії імені Євгенія Березняка Міністерства оборони України; м. Київ, Україна; e-mail: mars_kor@ukr.net; ORCID: https://orcsd.org/0000-0001-8049-4730

# PHYSICS OF DEVICES, ELEMENTS AND SYSTEMS
# ФІЗИКА ПРИЛАДІВ, ЕЛЕМЕНТІВ І СИСТЕМ

**UDC 621.793:678.073** **DOI:10.30837/rt.2023.2.213.06**

*V. BORSHCHOV, O. LISTRATENKO, M. PROTSENKO, I. TYMCHUK, O. KRAVCHENKO, O. SUDDIA, M. SLIPCHENKO*

## NANOPOLYMER OPTICALLY TRANSPARENT STRUCTURES, SYSTEMS AND DEVICES

### Introduction

Analysis of trends in the development of promising materials and technologies shows that the main efforts of researchers are currently focused on creating objects with dimensions comparable to the range length of electron nanostructures. Nanomaterials, the raw materials for the creation of which are individual atoms, molecules, molecular systems, nanoparticles no larger than 100 nm in size, have fundamentally new, often unique properties that differ from the properties of macroobjects due to a sharp increase in the reactivity of nanoparticles due to their high specific surface area. On the nanometer scale there are qualitatively new effects, properties and processes determined by quantum mechanics, dimensional quantization in small structures and other phenomena and factors. At the same time, the electronic structure is responsible for such material properties as optical absorption, electronic conductivity, chemical reactivity, and mechanical characteristics. Therefore, nanostructures reveal significantly different properties than material in volume, which can be used for practical purposes. In this regard, nanotechnology opens up new perspectives for electronics, optics, chemical industry, energy, medicine, biotechnology and many other areas of science and technology.

One of the priority research areas actively developing in recent years is the creation of transparent polymer compositions containing nanoscale fillers, which open up new prospects for optical and optoelectronic instrumentation [1].

High-tech and relatively cheap polymer optics is a means to solve technical problems associated with reducing the complexity of assembly, improving the design and reliability of various optical devices.

At the same time, new polymeric materials have confirmed their promise not only for conventional optics, but also for the purposes of laser optics and technology, where polymer lenses, deflecting plates, prisms are used, and organic glasses activated by generating organic dyes have been developed as new solid-state active media.

Luminophor containing polymers and composites are very attractive as luminescent probes, optical media for luminescent solar concentrators, electroluminescent organic LEDs, important for creating modern electronic devices, and energy-saving light sources.

Current trend is to create photochrome and other so-called "smart" materials based on optically transparent polymers. Significant scale of the latest research is aimed at the synthesis and study of polymers with nonlinear optical properties [2].

Aim of carried out work is to perform a search and analysis of data obtained from results of theoretical and experimental studies, as well as from literary sources and patents in the field of optical and optoelectronic instrumentation. Generalization of the obtained data and recommendations for the creation of optically transparent nanocomposites. Results of the work can be useful for further improvement of nano-containing transparent polymer composites and design and technological solutions not only for optical devices, but also for products of scintillation technology, photovoltaics and many other applications.

### 1. Nanopolymer optically transparent composites

Polymer nanocomposites are polymeric materials that are filled with particles having at least one of the sizes in the nanometer range. The main differences between nanocomposites and macro- and microcomposites are in the huge specific surface area of the filler-matrix interface, in large

volume fraction of interfacial boundary, and in small average distances between the filler particles. When creating polymer nanocomposites, the main task of the polymer matrix is to ensure compatibility with nanoparticles and to ensure uniform distribution of nanoparticles. Therefore, following requirements are imposed on polymers for preparation of composites: good adhesion to surface of the filler, high strength, and a number of other properties that make it possible to carry out technological processes for preparation of polymer nanocomposites, required level of viscosity for impregnation or mixing with dispersed fillers, heat resistance under conditions of processing into products, etc. It should be noted that another important role of polymers is their stabilizing role. In composites, the filler-additives are of particular importance, since the electrical, magnetic, optical, and other properties of the material tend to depend substantially on the corresponding characteristics of the nanoparticles. Of great importance is the interaction between the filler and the polymer matrix at molecular level, which can lead to synergy of the beneficial properties of organic and inorganic components of the material.

To create them, polymers are filled with nanoparticles of noble metals or semiconductors 1–20 nm in size, in which the strong spatial localization of valence electrons leads to the appearance of properties that differ from those of both a solid state and isolated molecules. The most promising for obtaining quantum size effects are particles whose size does not exceed 10 nm [2, 3].

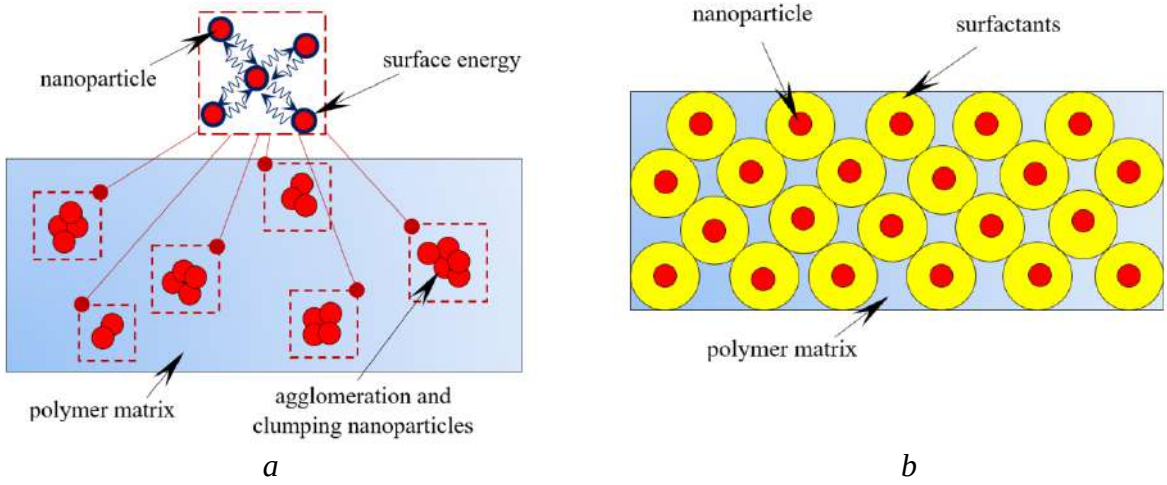


Fig. 1. Structural diagram of a polymer nanocomposite: *a* – surface of the nanoparticles is not treated with surfactants, *b* – surface of the nanoparticles is treated with surfactants

Due to the high surface energy and presence of functional groups capable of interaction on the surface, nanoparticles are prone to agglomeration and clumping (Fig. 1, *a*). Therefore, during conventional mixing with polymer melts, the sizes of a large proportion of particles are in the micron and submicron range. Treatment with surfactants capable of being adsorbed at interphase boundaries and preventing aggregation significantly increases degree of particle dispersion in the polymer matrix (Fig. 1, *b*). Thus, surfactants and blocking of functional groups on the particle surface make it possible to partially solve the problem of agglomeration. Nanocomposites containing high concentrations of a nanocrystalline component actually become hybrid materials with a comparable content of nanocrystals and a polymer matrix.

Under favorable conditions (homogeneous distribution of nanocrystals, absence of their coagulation, monodispersity), the nanomaterial is a homogeneous optical medium whose light scattering and rheological properties are similar to those of the polymer matrix even at high nanocrystal concentrations, and optical and physical properties are a superposition of the properties of both components. Small size of nanoparticles leads to fact that polymer nanocomposites can be considered as an optical medium, and for it, as for a homogeneous medium, optical parameters can be introduced – the refractive index and the absorption index. In this regard, nanostructuring is a new way to create optical media in which the resulting set of properties cannot be achieved by other means. High-

est concentration in an organic matrix can be obtained for inorganic nanocrystals coated with low-molecular shells that stabilize them. Common property of optical nanocomposites is that introduction of high concentrations of nanocrystals into the matrix leads to change in the properties and structure of the matrix. In this case, the greater the change, the higher the concentration of introduced nanocrystals. However, the magnitude with which this effect begins to manifest itself is different for different types of nanocomposites. This effect is observed regardless of method of synthesis and composition of the nanocomposite.

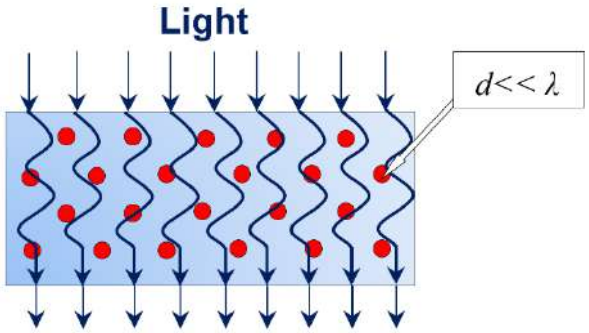


Fig. 2. Light scattering in an ordered system of nanoparticles in the bulk of a polymer material

Nanoparticles embedded in original polymers do not cause light scattering if they are uniformly distributed and their size is much smaller than the radiation wavelength (Fig. 2). Refractive index of the material with introduced nanoparticles is determined by following expression:

$$n = \frac{n_1 V_1 + n_2 V_2}{V_1 + V_2} \tag{1}$$

where $V_1$ and $V_2$ as well as $n_1$ and $n_2$ are volumes of source material and nanoparticles and refractive index of source material and nanoparticles respectively.

At high concentration of nanoparticles, the index of refraction of a nanocomposite with built-in nanoparticles can be much higher than that of the source material, which increases the light output of light-emitting semiconductor light-emitting diodes or light transmission for semiconductor light receivers and optical systems [3 – 5].

**2. Organosilicon composite for connecting optical elements**

Components of some units of optical systems (objectives, eyepieces, wrapping systems, achromatic wedges, complex prisms, mirror reflectors, light filters, polaroids, grids, etc.) are connected together into monoblocks. As a connecting substance, various organosilicon compounds are used, which can improve the manufacturability of structures and performance of optical systems. There are many connection methods such as gluing, sintering, optical contact, welding and soldering. In this case, connecting substance must meet following requirements: not change optical properties of the connected parts, provide sufficient mechanical, chemical, thermal and light strength of the connection.

Organosilicon lubricating compositions are used as an optical contact between light source and photodetector, which provide maximum light transmission in contact, are stable in temperature range of minus 70°C plus 200°C. They are non-toxic, chemically inert with respect to structural materials, have a low dependence of viscosity on temperature, and high adhesion to contact surfaces. However, known organosilicon compositions contain functional groups that lead to crosslinking of a polymer and formation of solid compounds.

To connect and seal optical elements using a plastic base and a thickener, a new composition was proposed in [6], which consists of a mixture of polydimethylsiloxane and polymethylphenylsiloxane liquids with a viscosity of 3000 to 40000 $mm^2/s$ at 20°C temperature and a silicon dioxide thickener. The composition has refractive index of 1.41 – 1.43 and penetration

value (density) of 160 – 280 units. Moreover, it operates in temperature range from minus 70°C to plus 300°C, with following composition (Table 1):

Table 1

Mixture of the optical composition

| | |
|---|---|
| Base (mixture of polydimethylsiloxane and polymethylphenylsiloxane liquid), wt. % | 90 – 96 |
| Thickener – silicon dioxide ($SiO_2$), wt. % | 10 – 4 |

The base of the silicon organic composition is mixture of polymethylsiloxane liquid (PMS), general formula: $(CH_3)_3SiO[(CH_3)_2SiO]_n\ Si(CH_3)_3$, with viscosity between 1000 and 50,000 $mm^2$/sec and a polymethylphenylsiloxane liquid (PFMS), general formula: $(CH_3)_3\ SiO\ [(CH_3)_2SiO]_k\ [CH_3(C_6H_5)SiO]_m\ Si(CH_3)_3$, where *k/m =10/1*, with viscosity from 10,000 to 20,000 $mm^2$/s in ratio PMS-60 – 40%, PFMS – 40 – 60%.

Manufacturing process of the organosilicon composition is as follows: in container equipped with heater, mixing device and thermometer, loaded with 180-270 g PMS fluid with viscosity of 1000-20000 $mm^2$ / s and 270 – 180 g PFMS fluid with viscosity of 10000 – 20000 $mm^2$ / s, the contents of the container stirred and obtained 450 g mixture with viscosity 3000 – 20000 $mm^2$ / s, which is basis of the composition, then added 50 – 20 g of silicon dioxide powder, the mass is heated to temperature of 40-60°C and stirred for 3 – 4 hours. After that the resulting mass is cooled to room temperature, unloaded and analyzed in terms of quality indicators:

1) Appearance – colorless transparent ointment plastic mass.

2) Penetration at 20°C – 160 – 280 units.

3) Refractive index ($n_d^{20}$) at 20°C – 1.41 – 1.43.

4) Frost resistance (pour point), °C – minus 70.

5) Thermal stability, % weight loss at 300°C for 2 hours – 1.0.

The organosilicon composition is non-toxic, chemically inert with respect to structural materials, has low dependence of viscosity on temperature, and high adhesion to contact surfaces. High viscosity of the base composition (3000 – 40000 $mm^2$/s) and small change in its value with temperature ensures normal operation of optical devices, smooth running and clear fixation of moving parts in winter and summer.

### 3. Plastic scintillator with nanostructured phosphors

Plastic scintillators (PS) are solid solutions of activating additives in polymer bases. History of their development begins in 1950, when the first scintillation composition based on polystyrene with pterphenyl was obtained. Creation of PS has become a new direction in development of scintillation method due to their unique properties. These include the following properties:

- high speed (0.5 – 3 ns);
- high transparency to its own radiation;
- manufacturability, ease of production and processing (possibility of obtaining PS of almost unlimited size and given shape);
- resistance to moisture, atmospheric and mechanical influences;
- relatively high radiation resistance;
- sufficient stability of scintillation characteristics in wide temperature range;
- relative cheapness;
- high fire safety and non-toxicity.

To date, polystyrene and vinyl toluene are widely used as the polymer base of PS. The main scintillation characteristics of the plastic scintillator based on vinyl aromatic polymer:

- light output ~ 8500 photon / MeV;
- main emission band – 420 nm;

- scintillation duration – 0.9 ns rise and 2 – 3 ns fall of the scintillation pulse.

Modern development of physical experiment requires creation of new advanced devices based on scintillators with improved time characteristics and light output values. But, at the same time, they must be cheap enough to be able to create a large-scale production of detector devices for experiments in high energy physics. Thus, there is need to improve the properties of PS, to create faster and more efficient plastic scintillators compared to already existing traditional PS [7 – 9].

PS proposed in [10] can be used in nuclear physics, high-energy physics, radiation chemistry, nuclear industry, radiation medicine, X-ray and gamma-ray astronomy. In diagnostics of fusion, in determining the lifetime of positrons and in a number of other tasks, in which are widely used fast-acting plastic scintillators with short luminescence time.

Technical solution considered in this work belongs to field of creating materials for scintillation technology, namely to plastic scintillators with nanostructured luminophores.

Since 60s of 20th century, not single fundamental technical solution has been proposed that would significantly increase light output of PS. The light output of three-component PS (polymer base, primary phosphor, secondary phosphor) primarily depends on the efficiency of transfer of electronic excitation energy from polymer matrix to the primary and, further, to the secondary phosphor. Due to low concentration of the secondary phosphor, energy transfer to it occurs due to photon mechanism, which leads to increase in duration of scintillation and decrease in the light output of the scintillator. Low concentration of the secondary phosphor in PS allows the self-absorption to be reduced, so that higher light output can be obtained. Attempt to increase efficiency of energy transfer by increasing concentration of the secondary phosphor leads to an increase in self-absorption and, consequently, to decrease in the light output of PS, therefore, this technical solution is used only in case of thin-film (0.001 – 0.01 cm) PS, which have very narrow scope.

Task of technical solution proposed in [10] is to obtain a new PS with a fundamentally new distribution of primary and secondary phosphors in the polymer matrix, due to which efficiency of nonradiative energy transfer from the primary to the secondary phosphor is close to 100%.

Technical result that can be obtained by implementing this solution:

1) the light output of the new PS relative to anthracene is up to 100 – 110%;

2) light attenuation coefficient at wavelength corresponding to maximum in fluorescence spectrum of the secondary phosphor 0.0015 – 0.0025 $cm^{-1}$.

3) duration of scintillation 1 – 3 ns.

This problem is solved by creating a new PS consisting of a polymeric base, which contains primary and secondary phosphors connected by silicon atoms in nanoscale branched macromolecules. Total number of primary and secondary phosphor links in a macromolecule is from 3 to 45. Ratio of number of primary phosphor links to number of secondary phosphor links:

$$2 \le \frac{N_{L1}}{N_{L2}} \le 14 \qquad (2)$$

where $N_{L1}$ is number of primary phosphor links in the macromolecule and $N_{L2}$ is number of secondary phosphor links in the macromolecule. Distance between the centers of any two adjacent links is no more than 1,2 nm.

As a polymer base, any polymer from group of vinyl aromatic polymers can be used. In this case, the primary phosphor is selected from the group of compounds in which the maximum of the long-wavelength absorption spectrum band is in range from 270 to 350 nm. Quantum yield of fluorescence is not less than 5 %. The secondary phosphor is selected from the group of compounds in which the maximum of long-wavelength band of absorption spectrum is in range from 330 to 400 nm. Quantum yield of fluorescence is not less than 30 %. An increase in the light output of the scintillator and reduction in duration of scintillation is achieved due to fact that in a nanosized branched macromolecule with claimed parameters, efficiency of nonradiative transfer of electronic excitation energy from units of the primary to the units of the secondary phosphor can reach 100 %.

In a conventional three-component scintillator (with uniform distribution of primary and secondary phosphor molecules in volume of the polymer matrix) efficiency of irradiation-free energy transfer does not exceed 0.1 %. In a conventional scintillator, there is a radiative transfer of electronic excitation energy from the primary to the secondary phosphor, efficiency of which cannot be greater than the quantum yield of the primary phosphor. For the main primary and secondary phosphors used in creation of PS, the efficiency of radiative transfer does not exceed 50 – 60%, while the light yield of PS relative to the light yield of anthracene is 60 – 65%. Consequently, increasing efficiency of irradiative energy transfer to 100 % will increase the luminous yield of PS up to 100 – 110 % relative to anthracene.

Decrease in light attenuation coefficient at wavelength corresponding to maximum in the PS fluorescence spectrum (increase in transparency) is achieved by choosing maximal ratio between the units of the primary and secondary phosphors:

$$k = \frac{N_{L1}}{N_{L2}} \tag{3}$$

Choice of maximal ratio is due to need to minimize absorption of the secondary phosphor at a wavelength corresponding to maximum of its fluorescence. Increase in the ratio leads to an increase in transparency and, at the same time, to decrease in efficiency of nonradiative energy transfer as a result of an increase in distance between units of the primary and secondary phosphors. To avoid this, the phosphors are distributed in

$$n_{L1} = \frac{N_{L1}}{k} \tag{4}$$

the macromolecule in such way that the distance between the centers of each unit of one secondary phosphor and group consisting of units of the primary phosphor is minimal, as shown in Fig. 3.

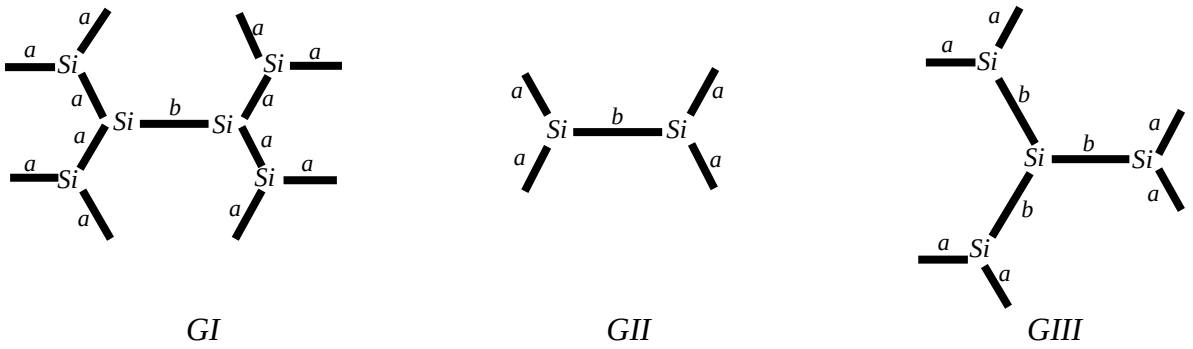


Fig. 3. Schemes of structure of branched nanoscale macromolecules

On Fig. 3 schematically shows structure of branched nanosized macromolecules with different ratios of number of units of the primary and secondary phosphors:

$$GI: \frac{N_{L1}}{N_{L2}} = \frac{12}{1}\ , \tag{5}$$

$$GII: \frac{N_{L1}}{N_{L2}} = \frac{4}{1}\ , \tag{6}$$

$$GIII: \frac{N_{L1}}{N_{L2}} = \frac{6}{3}. \tag{7}$$

Index (a) marks the primary phosphor links, and index (b) marks the secondary phosphor links. Nanostructured filler – nanosized branched macromolecules consisting of links corresponding to

primary and secondary phosphors are produced using one of the reactions of organometallic synthesis (Suzuki, Kumada, Stille, Ullmann), as well as the interaction of chlorine- or alkoxysilanes with lithium- or magnesiumorganic derivatives.

Scintillator blank is obtained by mixing the nanostructured filler with polymer selected as a base in twin-screw mixer with return channel (at 180°C temperature and screw rotation frequency of 600 rpm). Further, pressing (at temperature of 180°C) get samples of PS with diameter of 25 mm, height of 10 mm. Surface of the samples is carefully polished.

Measurement of light output of PS carried out on calibrated amplitude spectrometer. Duration of scintillation is measured with oscilloscope with bandwidth of 1000 MHz. Value of light attenuation coefficient at wavelength corresponding to maximum intrinsic fluorescence is determined using a spectrophotometer.

**4. New nanopolymer materials and nanoparticle dispersion methods**

Nanoparticles such as quantum dots (QDs) are of high interest for use in transformative devices. They can, for example, serve as an non-organic luminophore in transformation of blue light into other colors with narrow bandwidth and adjustable frequency of radiation using QDs, in order to be able to obtain high quality white color.

However, introduction of nanoparticles in many types of polymers leads to clumping nanoparticles. Therefore, relevant technical task is to create an alternative system of nanoparticle – polymer, especially a polymer system with quantum dots, in which causes of aggregation of nanoparticles would be eliminated, and polymer matrices had high values of glass transition temperature Tg to 150 – 200 ° C, for example, photochemically stable silicon-containing polymers.

Silicon-containing polymers can have much higher thermal stability and acceptable light transmission ratio than other organic polymers. However, QDs with conventional surface protective molecules are not dispersed in silicones and show aggregation resulting in reduced light transmission.

Thus, there is a problem of mixing nanoparticles into silicon-containing polymers. Phase separation between nanoparticles and polymers causes QDs agglomeration and drastically reduces quantum yield and light transmission ratio through nanoparticle/polymer mixtures.

In [11], technical solution was proposed that makes it possible to obtain well-dispersed QDs layers in silicones using protective molecules that can themselves attach to the surface of QDs. Group of protective molecules compatible with silicones has been developed. These protective molecules can easily coat the QDs and ensure the formation of uniform QDs/silicone polymer composites. These protective molecules are made up of two parts; one part connects to outer unprotected atoms on crystal surface of the QDs, and other part is compatible with silicone matrix. By surface modification, the nanoparticles can be easily mixed with the silicone matrix. New matrices can form very thin transparent films. The films have high thermal stability and can be used as new light-converting phosphors. With choice of matching silicone polymers and surface protective molecules for nanoparticles, it becomes possible to homogeneously mix most conventional nanoparticles in any given silicone matrix. The formed thin films of the nanoparticle/silicone matrix have high light transmission coefficient and are not inferior in stability compared to nanoparticles in purely inorganic matrices.

This kind of nanopolymer produced by this method can be used either alone or in a polymer product, and it seems possible to provide luminescence with high quantum yield and stability. In addition, the polymer can be stable with respect to effects of temperature and photochemistry. In this method, nanoparticles can be dispersed uniformly in the polymer, and agglomeration processes can be eliminated.

Such luminescent materials can also be used successfully in various devices. The present technical solution can be applied to devices including light sources and light converters designed to convert part of radiation of light source into light of converter, which is a solid polymer obtained according to the proposed technical solution.

Luminescent nanoparticles can be, for example, include compounds of semiconductor nanoparticles of groups II – VI selected from group consisting of CdS, CdSe, CdTe, ZnS, ZnSe, ZnTe, HgS, HgSe, HgTe, CdSeS, CdSeTe, CdSTe, ZnSeS, ZnSeTe, ZnSTe, HgSeS, HgSeTe, HgSTe, CdZnS, CdZnSe, CdZnTe, CdHgS, CdHgSe, CdHgTe, HgZnS, HgZnSe, HgZnTe, CdZnSeS, CdZnSeTe, CdZnSTe, CdHgSeS, CdHgSeTe, CdHgSTe, HgZnSeS, HgZnSeTe and HgZnSTe.

In another variant of applications of luminescent nanoparticles can be, for example, compounds of semiconductor nanoparticles of III-V groups, selected from group consisting of GaN, GaP, GaAs, A1N, A1P, AlAs, InN, InP, InAs, GaNP, GaNAs, GaPAs, A1NP, AlNAs, AlPAs, InNP, InNAs, InPAs, GaAlNP, GaAlNAs, GaAlPAs, GaInNP, GaInNAs, GaInPAs, InAlNP, InAlNAs and InAlPAs.

Thus, the silicone nanocomposite to the proposed technical solution is able to transmit light radiation with high efficiency with wavelength selected from the range of 420-750 nm at temperatures up to 100°C – 200°C.

## Conclusions

Analysis of some currently existing polymer and nanopolymer optical systems and their applications showed that complexity of structures and micro-dimensions of such optical systems for their wide application requires new easy-to-use and inexpensive optical materials. New types of polymer materials are replacing the traditional optical material (glass). In addition to fact that they make it possible to obtain structures of micro and nanosizes, there is already real opportunity to select their physical and optical properties – index of refraction, optical uniformity, light transmission, light scattering, stiffness and other ones, depending on specific task. Nanostructured optical polymer materials are increasingly being used to further improve and enhance efficiency of not only optical devices, but also products of scintillation technology, lighting engineering, photovoltaic, as well as applications in other fields of science and technology.

In this regard, the research aimed at finding new approaches to creation of nanocomposites on the basis of wide range of polymers and nanoparticles becomes relevant.

**References:**

1 Smirnov V.I. Physical foundations of nanotechnology and nanomaterials: a training manual. Ulyanovsk: UlSTU, 2017. 240 p.

2 Serova V.N. Optical and other materials based on transparent polymers. Serova: monograph. Feder. Agency for Education, Kazan. Gos. Technol. Un-t. Kazan : KSTU, 2010. 540 p.

3 Burunkova, Yu.E., Denisyuk, I.Yu., Sheklanova EB, Fokina, M.I. Optical polymer nanocomposites. St. Petersburg : ITMO University, 2017. 80 p.

4 Burunkova. Yu. E., Semina S.A., Kaporsky L.N., Levichev V.V. Nanomodified optical acrylate composites // Optich. J. 2008. V. 75, No. 10. p. 54–58.

5 Vilchinskaya S.S., Lisitsyn V.M. Optical materials and technologies: a training manual. Tomsk : Publishing House of Tomsk Polytechnic University, 2011. 107 p.

6 Patent RF № 2505569 Organosilicon composition. Patent publication: January 27, 2014.

7. Aspects of scintillation technology (edited by A.V. Gektin). Kharkov : ISMA, 2017. P. 264.

8. B.V. Grinev, N.R. Gurdjian, O.V. Zelenskaya, V.R. Lyubinsky, L.I. Mitsay, N.I. Molchanova, V.A. Tarasov. Detectors based on plastic scintillators for portal monitors – evaluation of sensitivity uncertainty // Ukrainian Metrological Journal. 2018. № 2. P. 46–54.

9. Zhmurin P.N., Eliseev D.A., Lebedev V.N., Pereymak V.N., Svidlo O.V., Velmozhnaya E.S. Fast plastic scintillator with the high light yield // Functional Materials. 2016. Vol. 23, №3. P. 408–413.

10. Patent RF № 2380726 Plastic scintillator with nanostructured luminophores. Patent Publication: 27.01.2010.

11. Patent RF № 2627378 New materials and methods for dispersing nanoparticles. Patent Publication: 08.16.2017.

*Received 07.06.2023*

*Information about the authors:*

**Borshchov Vyacheslav** – Professor, Doctor of Technical Sciences, LLC «Research and Production Enterprise «LTU», First Deputy Director – Chief Designer; Ukraine; e-mail: viatcheslav.borshchov@cern.ch; ORCID: https://orcid.org/0000-0002-5579-8932

**Listratenko Oleksandr –** Dr., Ph.D, LLC «Research and Production Enterprise «LTU», Leading Scientist; Ukraine; e-mail: sasha.listratenko.12@gmail.com; ORCID: https://orcid.org/0000-0001-7643-5295

**Protsenko Maksym –** Dr., Ph.D, LLC «Research and Production Enterprise «LTU», Head of the Department – Deputy Chief Designer; Ukraine; e-mail: max.protsenko.1978@gmail.com; ORCID: https://orcid.org/0000-0001-9313-1701

**Tymchuk Ihor –** Dr., Ph.D, LLC «Research and Production Enterprise «LTU», Chief Technologist; Ukraine; e-mail: ihortymchuk78@gmail.com; ORCID: https://orcid.org/0000-0002-6436-7253

**Kravchenko Oleksandr** – LLC «Research and Production Enterprise «LTU», Deputy Head of Department; Ukraine; e-mail: kravcenkoaleksandr671@gmail.com; ORCID: https://orcid.org/0000-0002-7145-4304

**Suddia Oleksandr –** LLC «Research and Production Enterprise «LTU», Scientist; Ukraine; e-mail: 4el1195@gmail.com; ORCID: https://orcid.org/0000-0002-2403-979X

**Slipchenko Mykola –** Professor, Doctor of Physical and Mathematical Sciences; Institute for Scintillation Materials National Academy of Sciences of Ukraine; Leading Scientist; Ukraine; e-mail: naukovets.big@gmail.com; ORCID: https://orcid.org/0000-0002-4242-4800

**УДК 004.056.5** **DOI:10.30837/rt.2023.2.213.07**

*І.О. МИЛЮТЧЕНКО, канд. техн. наук, П.О. КУЛЬКО*

# ЕЛЕКТРОННІ ІНФОРМАЦІЙНІ РЕСУРСИ: ВИЗНАЧЕННЯ ТА КЛАСИФІКАЦІЯ

Нині у науковому та суспільному просторі поряд із загальним поняттям «ресурси» важливим є поняття «інформаційні ресурси» (ІР). На підставі аналізу та узагальнення нормативних документів, стандартів, словників і довідників, праць науковців, ІР можна визначити, зокрема, як систематизовану сукупність документів, зафіксованих на паперових чи інших носіях, в інформаційних системах [1].

Стратегія воєнної безпеки України [2] передбачає серед іншого «адаптивне до змін безпекового середовища та збалансоване з можливостями держави використання людського капіталу, інформаційних, матеріальних, фінансових ресурсів України, їх підсилення ресурсами держав-партнерів».

Адаптивне та збалансоване використання, вибір методів та засобів захисту залежать від виду та призначення ІР. Стрімкий розвиток інформаційних технологій зумовив важливе значення електронних інформаційних ресурсів (ЕІР). Значення ЕІР, зокрема віддаленого доступу, збільшується в особливих умовах (пандемії, воєнного стану). Тому актуальною є проблема визначення поняття «електронний інформаційний ресурс» та ознак класифікації ЕІР.

Поняття ЕІР визначено як у правовому просторі України, зокрема у законі України «Про Національну програму інформатизації» [3], так й у працях науковців (П. Марченко, В. Копанєва, З. Савченко, Т. Ковтанюк, М. Женченко та ін.).

Інформаційні технології надають більше можливостей для фіксації інформації, її подальшого опрацювання, змінювання та розповсюдження. Разом із цим, зі зміною носіїв інформації сутність інформаційного об’єкту, головною складовою якого є інформація, не змінюється. Отже, цілком зрозуміло, що визначення ЕІР як «систематизованих відомостей і даних, створених, оброблених та збережених в електронній формі за допомогою технічних засобів та/або програмних продуктів» [3] базується на загальному визначенні ІР.

У нормативних документах України та роботах науковців використовуються різні формулювання поняття «електронні інформаційні ресурси» (табл. 1).

Таблиця 1

| Формулювання визначення ЕІР | Джерело |
|---|---|
| ЕІР – систематизовані відомості і дані, створені, оброблені та збережені в електронній формі за допомогою технічних засобів та/або програмних продуктів. | [3] |
| ЕІР – інформація, апаратні, програмні та інші засоби, що можуть бути надані користувачеві, наприклад, файл-сервером або базою даних. На файл-сервері вся сукупність документів подана файлами, які зберігаються в пам’яті комп’ютера з певним кодовим позначенням. Змістом файлу може бути зміст документа або інша інформація, що стосується документа. В базах даних сукупність документів подана одним або кількома спеціально організованими файлами. | [4] |
| ЕІР – інформаційні ресурси, що розміщені в електронних базах або банках даних, у комп’ютерних системах, системах автоматизованої обробки і передачі даних. При їх одержанні чи передачі за допомогою мережі Інтернет їх називають веб-ресурсами. | |
| ЕІР – вміщує такі аспекти поняття, як цифрова форма фіксації інформації, комп’ютерні засоби та програмне забезпечення для відтворення та керування, електронне середовище для розповсюдження (комп’ютерні мережі та засоби телекомунікаційного зв’язку). | [5] |
| ЕІР – інформаційні ресурси, якими управляє комп'ютер, у тому числі ті, що потребують використання периферійного пристрою, підключеного до комп'ютера. | [6] |
| ЕІР – інформаційний ресурс, який зберігається в електронному чи комп’ютеризованому форматі та може бути досягнутий, знайдений та перетворений засобами електронної мережі або іншої електронної технології обробки даних. | [7] |

Хоча формулювання терміну ЕІР залежать від сфери діяльності (інформаційна безпека, бібліотекознавство, архівознавство тощо) і відрізняються степенем докладності, але загалом мають певну подібність.

У табл. 2 наведено визначення певних видів ЕІР, зокрема національних ЕІР [9], державних ЕІР [9 - 12], науково-освітніх ЕІР [7], освітніх ЕІР [13]. Окремо досліджують поняття бібліотечних інформаційних ресурсів, які розглядаються як компоненти колекції бібліотек [17], подібного погляду дотримуються також закордонні дослідники [8, 16].

Таблиця 2

| Визначення деяких видів ЕІР | Джерело |
|---|---|
| Національні ЕІР – інформаційні ресурси незалежно від їх змісту, форми, часу та місця створення, форми власності, які існують та використовуються в електронному вигляді та призначені для задоволення потреб громадянина, суспільства, держави. Національні електронні ресурси включають державні, комунальні та приватні ресурси. | [9] |
| Державні ЕІР – відображена та задокументована в електронному вигляді інформація, необхідність захисту якої визначено законодавством. | [10] |
| Державні ЕІР – державні інформаційні ресурси незалежно від їх змісту, форми, часу і місця створення, які існують та використовуються в електронному вигляді та призначені для задоволення потреб громадян, суспільства, держави. Державні електронні інформаційних ресурсів є складовою Національного реєстру електронних інформаційних ресурсів. | [9] |
| Державні ЕІР – систематизовані відомості і дані, створені, оброблені та збережені в електронній формі за допомогою технічних та/або програмних засобів державних органів. | [11] |
| Державні ЕІР – систематизована, закріплена на матеріальних носіях і/або відображена в електронному вигляді інформація, право на володіння, використання або розпорядження якою належить державі або яка обробляється фізичними чи юридичними особами відповідно до наданих їм повноважень суб'єктами владних повноважень, призначена для задоволення потреб громадянина, суспільства, держави. | [12] |
| Науково-освітні ЕІР – електронні ресурси, які наповнюють науково-освітній інформаційний простір з метою цільового їх використання. | [7] |
| Освітні ЕІР – засоби навчання на цифрових носіях будь-якого типу або розміщені в інформаційно-телекомунікаційних системах, які відтворюються за допомогою електронних технічних засобів і застосовуються в освітньому процесі. | [13] |
| Бібліотечні ЕІР – опубліковані та неопубліковані первинні й вторинні документи на електронних носіях (книги, серіальні видання, дисертації тощо), фактографічні, повнотекстові й бібліографічні бази даних. | [17] |

ЕІР поділяють на категорії, кількість та зміст яких визначаються ознаками, зокрема функціональною (сфера використання), типом носія та контенту, технологією розповсюдження, статусом ЕІР тощо, причому деякі ознаки є спільними для ЕІР та ІР [1]. У табл. 3 наведені ознаки класифікації ЕІР, поділ ЕІР на категорії згідно з ознаками та зміст цих категорій (для деяких категорій зміст не пояснюється, оскільки є очевидним) відповідно до результатів дослідження ЕІР із різних джерел.

З порівняння ознак та категорій ЕІР (табл. 3) видно, що певні ознаки з різними формулюваннями подібні за змістом (зокрема ознаки 1 і 3), окрім того, деякі категорії повторюються у різних ознаках (зокрема ознаки 8 і 9), або відповідають певному виду діяльності (зокрема ознака 10 – економічній сфері).

В результаті порівняння означення та класифікації ЕІР виникає питання, чи входять технічні засоби та програмні продукти (так звані «е-ресурси») безпосередньо до складу ЕІР? Виходячи з головного визначення [3] – ні, «е-ресурси» – лише засіб обробки та перетворення, але за певними категоріями класифікації, зокрема за типом контенту, формою існування – так. Автори згодні з першим варіантом, але залишають у класифікації згадані категорії для повноти огляду.

Визначення та класифікацію ЕІР, складену в результаті аналізу та порівняння ознак класифікації, а також спільних ознак ЕІР та ІР [1] наведено на рис. 1.

Таблиця 3

| Номер ознаки | Ознака та джерело | Категорія | Зміст категорії |
|---|---|---|---|
| 1 | Вид інформації, призначеної для сприйняття [6] | електронні дані | інформація у вигляді чисел, літер, символів, зображень, включаючи графічну інформацію, відеоінформацію тощо або їхні комбінації |
| | | електронні програми | набори операторів чи підпрограм, які забезпечують виконання певних завдань, включаючи опрацювання даних |
| | | комбінація електронних даних і програм в одному ресурсі | мультимедіа, відеоігри |
| 2 | Ступень структурування [7] | безперервний текст | від безперервного тексту, який не має розподілу на абзаци, параграфи тощо, до формального представлення інформаційних даних у базах даних |
| | | формальне представлення інформації у базах даних | |
| 3 | Тип ресурсу (контенту) [7] | електронні дані | числові дані, символьні дані, зображення, звукові дані |
| | | електронні програми | системні, прикладні, сервісні (програмне забезпечення) |
| | | комбіновані | інтерактивні мультимедійні онлайнові служби |
| 4 | Тип носіїв і режим доступу [7] | локального доступу | інформаційні дані зафіксовані на окремому фізичному носієві, інформація з якого зчитується завдяки комп'ютерному пристрою |
| | | ресурси віддаленого доступу | інформаційні дані, які подаються в інформаційних мережах, зокрема, ресурси на Інтернет-серверах |
| 5 | Технологія розповсюдження [7] | локальні електронні видання, мережні, комбінованого розповсюдження | |
| 6 | Характер взаємодії з користувачем [7] | детерміновані, недетерміновані (інтерактивні) | |
| 7 | Форма існування [3, 14, 15] | база даних | систематизована сукупність даних, що відображає стан об’єктів та їх взаємозв’язків у визначеній предметній сфері [3]; бази даних, що містять задокументовану інформацію, є EIP або документів, або реквізитів документів. Залежно від цього бази даних є або сукупністю документів або документами [14] |
| | | вебсайт | сукупність програмних засобів, розміщених за унікальною адресою в обчислювальній мережі, у тому числі в мережі Інтернет, разом з інформаційними ресурсами, що перебувають у розпорядженні певних суб’єктів і забезпечують доступ юридичних та фізичних осіб до цих інформаційних ресурсів та інших інформаційних послуг через обчислювальну мережу [15] |
| 8 | Специфіка [7] | цільове призначення, періодичність, структура, правовий статус, наявність друкованого еквіваленту | |
| 9 | Статус [7, 18-20] | оригінал | самостійний ресурс, який не має аналогу |
| | | електронний аналог видання | в основному відтворює оригінал, зберігаючи розташування тексту на сторінці, ілюстрації, посилання, примітки |
| | | електронна версія | аналог, який має рівний з оригіналом правовий статус і який створюється одночасно із ним (на окремому носії) у відповідному форматі з метою надання його користувачам у мережному доступі або на окремому носії |
| | | електронні відтворення | візуально відповідають оригіналу (копії друкованих документів, зображення тривимірних об’єктів тощо) |
| | | електронний документ | документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов’язкові реквізити документа [18] |
| | | електронне видання | електронний документ, який пройшов редакційно-видавниче опрацювання, має вихідні відомості та призначений для розповсюджування в незмінному вигляді [19] |
| 10 | Суб’єкт укладання [4] | органи державної влади, організації ринку, що саморегулюються, суб’єкти господарювання, науково-дослідні установи, інше | |

Особливістю навчального контенту дисциплін спеціальності «Кібербезпека та захист інформації» є значний обсяг нормативно-правової текстової інформації (нормативні документи, стандарти, регламенти тощо), для засвоєння якої необхідні узагальнення, рубрикація та візуалізація тексту. Така методика відображена на рис. 1, який показує означення та класифікацію ЕІР. Подібну методику доцільно використовувати у навчально-методичній літературі.


Рис. 1. Визначення та класифікація ЕІР

**Висновки**

На основі огляду нормативних та наукових джерел показано важливість електронних інформаційних ресурсів, що зумовлено впливом інформаційних технологій. Зазначено певну узгодженість науковців щодо поняття ЕІР та його зв'язку із загальним визначенням інформаційних ресурсів. Розглянуто види та класифікацію електронних інформаційних ресурсів.

Аналіз поняття та класифікації EIP може бути корисним для забезпечення освітнього процесу за спеціальністю «Кібербезпека та захист інформації».

**Список літератури:**


1. Інформаційні ресурси: аналіз категорії та класифікація / І.О. Милютченко, Б.В. Онопко // Радіотехніка. 2018. Вип. 192. С. 157–161.

2. Стратегія воєнної безпеки України: Затверджено Указом Президента України № 121/2021 від 25.02.2021. URL: http://zakon.rada.gov.ua/laws/show/121/2021#Text (дата звернення 25.03.2023).

3. Про Національну програму інформатизації: Закон України №2807-IX від 01.02.2022. Режим доступу: http://zakon.rada.gov.ua/laws/show/2807-20#Text (дата звернення 25.03.2023).

4. Кравців Х. В. Організаційні основи формування електронних інформаційних ресурсів : Рукопис. Дипломна робота на здобуття ОКР "магістр" за спеціальністю 8.02010501 "Документознавство та інформаційна діяльність" / Тернопільський національний економічний університет. Тернопіль, 2017. URL: http://dspace.wunu.edu.ua/.pdf (дата звернення 25.03.2023).

5. Копанєва В.О. Бібліотека як центр збереження інформаційних ресурсів Інтернету. К. : Наук.-видав. центр Національна бібліотека України ім. В.І. Вернадського, 2009. 200 с. URL: http://www.irbis-nbuv.gov.ua (дата звернення 22.03.2023).

6. Женченко М. Бібліографічний опис електронних ресурсів: загальні вимоги // Вісник Книжкової палати. 2011. № 4. С.1–4.

7. Савченко З. В. Формування і використання інформаційних електронних науково-освітніх ресурсів // Інформаційні технології і засоби навчання. 2010. №4 (18). URL: http://www.ime.edu-ua.net/em18/content/10szvres.htm (дата звернення 24.03.2023).

8. Angadi Manjunath. "Use Pattern of Electronic Information Resources and Services in Libraries of Universities with Potential for Excellenct UPE in South India a Study", Karnatak University, 2018, URI http://hdl.handle.net/10603/225419.

9. Юдін О.К. Методологія захисту державних інформаційних ресурсів. Порівняльний аналіз основних термінів та визначень / О.К. Юдін, С.С. Бучик // Захист інформації. 2015. Т.17. №3. С. 218–224.

10. Положення про Реєстр інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління. Затверджено Постановою КМУ від 3 серпня 2005 р. № 688 (у редакції від 07.09.2022 р. № 991). URL: http://zakon3.rada.gov.ua/laws/show/688-2005-п#Text (дата звернення 25.03.2023).

11. Положення про систему електронної взаємодії державних електронних інформаційних ресурсів «Трембіта». Затверджено Постановою КМУ від 8 вересня 2016 р. № 606 (в редакції від 17.01.2023 р. № 38). URL: http://zakon3.rada.gov.ua/laws/show/606-2005-п#Text (дата звернення 25.03.2023).

12. Марущак А.І., Петров С.Г. Зміст поняття «державні електронні інформаційні ресурси» // Інформація і право. 2018. №4 (27). С.15–21.

13. Положення про Електронні освітні ресурси. Затверджено Наказом МОНУ від 01 жовтня 2012 року № 1060 (у редакції наказу від 29 травня 2019 року № 749). URL: http://zakon.rada.gov.ua/laws/show/z1695-12#Text (дата звернення 20.03.2023).

14. Віднесення електронних інформаційних ресурсів до Національного архівного фонду. Аналітичний огляд / Держ. архівна служба України ; Укр. наук.-досл. ін-т архів. справи та документознавства ; уклад.: Т.М. Ковтанюк, Н. М. Христова. К., 2012. 33 с. URL: http://undiasd.archives.gov.ua/doc/ao-eir-naf.pdf.

15. Про електронні довірчі послуги: Закон України №2155-VIII від 5 жовтня 2017 р. (в редакції 01.01.2023). URL: http://zakon.rada.gov.ua/laws/show/2155-19#Text (дата звернення 26.03.2023).

16. Dr. Parveen Kumari. Procurement, Management and Use of E-resource in Current Library Trends Common Issuses // International Journal of Digital Library Services, vol.5, issue 2, pp.150–159, April–June 2015, ISSN:2250-1142 (Online), ISSN:2249-302X (Print).

17. Рубан А. Формування та використання інформаційних ресурсів у бібліотеках України: огляд видань 2010–2014 років // Вісник Книжкової палати. 2016. № 1. С.26–33.

18. Про електронні документи та електронний документообіг: Закон України № 851-IV від 22.05.2003. Редакція від 01.08.2022. URL: https://zakon.rada.gov.ua/go/851-15 (дата звернення 20.03.2023).

19. Інформація та документація. Видання електронні. Основні види та вихідні відомості: ДСТУ 7157:2010. – [Чинний від 2010–07–01]. К. : Держспоживстандарт України, 2010. 20 с.

20. Діловодство та архівна справа. Терміни та визначення понять : ДСТУ 2732:2004. [Чинний від 2004–05–28]. К. : Держспоживстандарт України, 2010. 36 с.


*Надійшла до редколегії 05.04.2023*


*Відомості про авторів:*

**Милютченко Іван Олександрович –** Харківський національний університет радіоелектроніки, канд. техн. наук, професор кафедри радіоінженерії та систем технічного захисту інформації; Україна; e-mail: ivan.myliutchenko@nure.ua, ORCID: https://orcid.org/0000-0001-7559-8850

**Кулько Петро Олександрович –** Харківський національний університет радіоелектроніки, студент гр. СТЗІАм-22-1; Україна; e-mail: petro.kulko@nure.ua

**УДК 621.396.677.494** **DOI:10.30837/rt.2023.2.213.08**

*А.І. КОВАЛЕНКО, канд. техн. наук, С.В. ТІТОВ, канд. техн. наук,*
*О.В. ТІТОВА, канд. техн. наук, О.С. ЧОРНА, канд. техн. наук*

# ОЦІНКА ВИМОГ ДО ПАРАМЕТРІВ СИГНАЛІВ ПРИ V-ПОДІБНОМУ РОЗПОДІЛІ ЧАСТОТ У МАТЕМАТИЧНІЙ МОДЕЛІ ПЛОСКОЇ ФАЗОВАНОЇ АНТЕННОЇ РЕШІТКИ

## Вступ

Розвиток ефективних радіотехнічних систем різного призначення, таких як засоби локації ближньої дії, спеціальні системи зв'язку між об'єктами в заданих локальних ділянках простору, системи передавання енергії НВЧ-променем і формування в локальній ділянці простору високої щільності електромагнітної енергії, стає можливим завдяки використанню фокусування електромагнітного випромінювання. Фазовані антенні решітки (ФАР) надають найбільші можливості та гнучкість керування параметрами сфокусованого електромагнітного випромінювання (ЕМВ).

Різноманітні методи керування фокусуванням ЕМВ класифікуються та аналізуються в роботах [1 – 6]. У результаті дослідження, проведеного в [5, 6], було показано, що найефективнішими методами фокусування ЕМВ є методи, що ґрунтуються на взаємоузгодженому просторово-фазово-частотному (ПФЧ) і просторово-фазово-частотно-часовому управлінні. Для локалізації ЕМВ в заданому кутовому напрямку без сканування рекомендується використовувати методи фокусування, що ґрунтуються на ПФЧ-керуванні з використанням багатоступеневого V-подібного закону розподілу частот за апертурою ФАР.

Однак флуктуації параметрів сигналів і антен, спричинені різними випадковими факторами, обмежують потенційні можливості та можуть призвести до суттєвих змін сфокусованих просторово-часових імпульсів, а також до зниження їхньої пікової потужності. Тому представляє інтерес вивчення та обґрунтування вимог до параметрів випромінюваних сигналів при використанні різних методів фокусування ЕМВ [14, 15].

Мета статті – проведення статистичного дослідження, яке дозволить оцінити вплив різних випадкових і детермінованих змін електричних і конструктивних параметрів антен, а також систем управління випромінюваними сигналами під час використання багатоступеневого V-подібного розподілу частот за апертурою ФАР на рівень пікової потужності, тривалість і період повторення сфокусованих імпульсів. Основна увага приділяється вивченню впливу цих факторів на рівень пікової потужності, тривалість і період повторення сфокусованих імпульсів.

## Основні припущення

У статті [6] зазначено, що для формування послідовності сфокусованих просторово-часових імпульсів (ПЧІ) необхідно задати закон розподілу амплітуд, початкових фаз і частот випромінюваних сигналів по апертурі ФАР. Важливо забезпечити умови синфазного складання полів від усіх випромінювальних елементів в обраній точці фокусування. Параметри закону керування, заснованого на просторово-фазово-частотному (ПФЧ) підході, мають бути стабільними протягом часу, що дорівнює усередненій тривалості імпульсів на виході випромінювачів під час формування окремого ПЧІ, або протягом тривалості послідовності ПЧІ.

Вплив різних типів помилок під час виготовлення традиційних антен та елементів антенно-фідерного тракту на характеристики поля випромінювання було розглянуто в попередніх роботах [1, 8, 9, 12]. У даній статті особлива увага приділяється особливостям точності розташування фазових центрів випромінювачів і вимогам до дискретності й точності встановлення початкових фаз і несучих частот за апертурою плоских ФАР, специфічних для ПФЧ фокусування на основі V-подібних розподілів частот.

Параметри законів ПФЧ керування фокусуванням ЕМВ, як вид закону розподілу помилок, дисперсії та радіуси кореляції помилок, є вихідними величинами під час дослідження статистики поля випромінювання. Однак через велику кількість елементів у передавальних каналах і різних джерел нестабільностей, визначення точного закону розподілу помилок у кожному каналі ФАР досить складне. Тому для спрощення аналізу припускають, що помилки встановлення параметрів сигналів у каналах ФАР є некорельованими і рівноймовірними. За відсутності інформації про закон розподілу застосовується припущення про рівну ймовірність. Виявляється, що в найгіршому випадку помилка, викликана відхиленням дійсного закону від передбачуваного закону рівної ймовірності, не перевищує ±20 % сумарної похибки, якщо похибка, яку розглядають, є домінуючою [10, 11]. Це пояснюється тим, що закон рівної ймовірності знаходиться між модальними й антимодальними законами розподілу.

У статті розглядається вплив зазначених нестабільностей на рівень пікової потужності, тривалість і період повторення сфокусованих імпульсів. Проводиться оцінка максимальних значень помилок параметрів законів керування, за яких зазначені характеристики сфокусованих ПЧІ змінюються не більше ніж на 10 %.

**Вимоги до точності розташування фазових центрів випромінювачів**

Аналіз виразів для розрахунку щільності потоку потужності, створюваної плоскою ФАР у заданій точці простору [5 – 7], показує, що якість фокусування ПЧІ залежить від ступеня забезпечення заданих координат фазових центрів джерел випромінювання. При створенні конкретних зразків радіотехнічних систем із ФАР можливі помилки в забезпеченні обраних координат, і закони зміни миттєвих фаз не відповідатимуть вимозі когерентного складання сигналів випромінювачів у заданій точці простору. Тому процес формування послідовності сфокусованих ПЧІ може бути порушений. Для обґрунтування вимог до точності розташування фазових центрів випромінювачів у плоских ФАР проведемо математичне моделювання поля випромінювання під час використання багатоступеневих V-подібних законів розподілу частот за наявності зазначених помилок.

Вплив помилок у розташуванні фазових центрів окремих джерел випромінювання за рівноймовірного закону їхнього розподілу на математичне очікування нормованої щільності потоку потужності плоскої ФАР можна оцінити за виразом

$$\left\langle S_{\text{н}}(x,y,z,t)\right\rangle = \left\langle \frac{1}{S_{\max}} \left| \sum_{m=-\frac{N_x-1}{2}}^{\frac{N_x-1}{2}} \sum_{n=-\frac{N_y-1}{2}}^{\frac{N_y-1}{2}} \sqrt{\frac{P_{mn}\,G_{mn}}{4\pi z^2}} \exp\left\{ -j\left[ 2\pi f_{0mn}\left( t - \frac{R^{\Delta}_{\text{mn}}}{c} \right) + \varphi_{0mn} \right] \right\} \right|^2 \right\rangle; \quad (1)$$

де $S_{\max}$ – максимальне значення щільності потоку потужності плоскої ФАР. Відстань до точки спостереження від кожного випромінювального елемента з урахуванням помилок розташування фазових центрів дорівнює

$$R^{\Delta}_{mn} = \sqrt{(x - x^{\Delta}_{mn})^2 + (y - y^{\Delta}_{mn})^2 + (z - z^{\Delta}_{mn})^2}\ ; \quad (2)$$

де $x^{\Delta}_{mn} = x_{mn} + \frac{\Delta\rho}{\sqrt{2}}\Psi_1$, $y^{\Delta}_{mn} = y_{mn} + \frac{\Delta\rho}{\sqrt{2}}\Psi_2$, $z^{\Delta}_{mn} = \Delta h \Psi_3$ – значення координат фазових центрів джерел випромінювання плоскої ФАР з урахуванням помилок; $\Delta\rho$ і $\Delta h$ – максимальні значення помилок розташування фазових центрів джерел випромінювання; $\Psi_1, \Psi_2, \Psi_3$ – рівномірно розподілені в інтервалі [-1,1] випадкові числа.

Закон розподілу початкових фаз для здійснення когерентного складання полів в обраній точці фокусування матиме вигляд [6, 7]

$$\varphi_{0n} = -2\pi f_{0n}\left( \frac{z_F}{c} - \frac{R_{Fn}}{c} \right); \quad (3)$$

де $R_{Fn}=\sqrt{(x_F-x_n)^2+(y_F-y_n)^2+(z_F-z_n)^2}$ – відстань між точкою фокусування з координатами $P_F(x_F,y_F,z_F)$ і центром *n*-го джерела випромінювання з координатами $(x_n,y_n,z_n)$.

Закон розподілу частот по апертурі ФАР має вигляд [7]

$$f_{0mn}=\begin{cases} f_0+\gamma\left[\dfrac{|m|}{\gamma}\right]\Delta F_x, & \text{если } \gamma\left[\dfrac{|m|}{\gamma}\right]\Delta F_x \ge \gamma\left[\dfrac{|n|}{\gamma}\right]\Delta F_y, \\ f_0+\gamma\left[\dfrac{|m|}{\gamma}\right]\Delta F_y, & \text{если } \gamma\left[\dfrac{|m|}{\gamma}\right]\Delta F_x < \gamma\left[\dfrac{|n|}{\gamma}\right]\Delta F_y; \end{cases} \tag{4}$$

$$m\in\left[-\frac{N_x-1}{2};\dots 0;\dots\frac{N_x-1}{2}\right];\quad n\in\left[-\frac{N_y-1}{2};\dots 0;\dots\frac{N_y-1}{2}\right];$$

де γ – коефіцієнт зменшення щільності; $\left[\dfrac{|m|}{\gamma}\right]$ – оператор округлення результату до найближчого більшого цілого числа. Коефіцієнт зменшення щільності $\gamma=\dfrac{\Delta F_{\max}}{\Delta F_i Q}=\dfrac{N_i-1}{2Q}$ показує, у скільки разів збільшується крок частоти між сусідніми щаблями закону частотного розподілу (або визначає кількість випромінювальних елементів з однаковими несучими частотами в одному щаблі частотного розподілу).

Оцінки проведемо для випадку: розміри ФАР $L_x=L_y=L=1{,}3$ м; $\lambda=0{,}02$ м $(L/\lambda=65)$; $N_X=N_Y=65$ $(N=N_XN_Y=4225)$ і $P_{mn}=6$ Вт $(P_{изл.}=P_{mn}N=25$ кВт); амплітудний розподіл рівномірний A(x,y)=1; дискретність частоти між сусідніми випромінювачами $\Delta F_x=\Delta F_y=20$ *МГц* та, відповідно, максимальний рознос несучих частот за апертурою ФАР $\Delta F_{x\max}=\Delta F_{y\max}=640$ *МГц*. Це дає змогу формувати послідовність ПЧІ тривалістю $\tau_{пчі}=1{,}7$ нс із періодом повторення $T_{ПЧІ}=50$ нс.

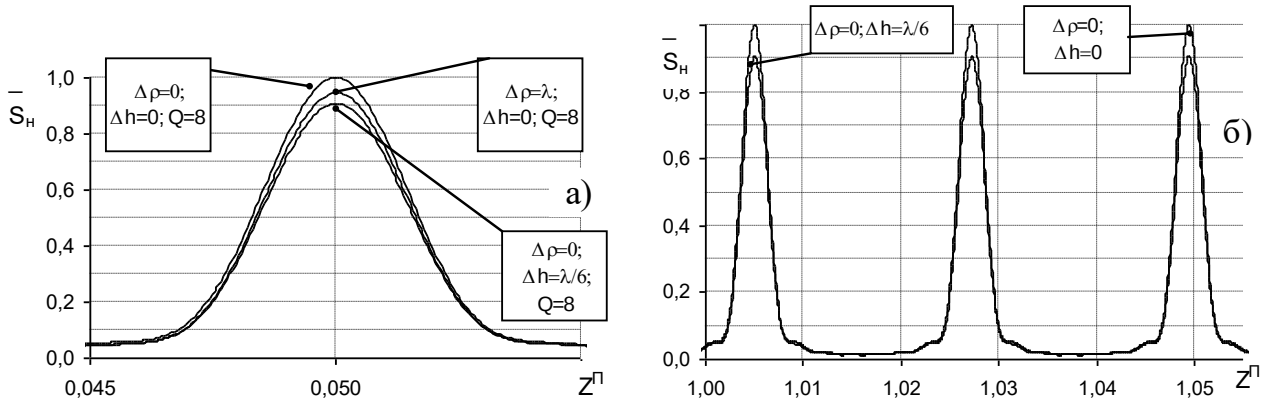


Рис. 1. Вплив помилок $\Delta\rho$ і $\Delta h$ на розподіл щільності потоку потужності ФАР за дальністю при $\gamma$=4 (Q=8): *а*) $z_F=0{,}05z_d$; *б*) $z_F=z_d$

На рис. 1 наведено залежності $\bar{S}_н=\langle S(x,y,z,t)/S_{\max}\rangle$ в напрямку нормалі до розкриву плоскої ФАР без урахування помилок розташування випромінювачів ($\Delta\rho=0$; $\Delta h=0$), а також з урахуванням максимальних значень помилок у площині X0Y, що дорівнює $\Delta\rho=\lambda$, та за віссю 0Z, що дорівнює $\Delta h=\lambda/6$, у разі використання багатоступеневого V-подібного закону розподілу частот по апертурі (див. вир. (4)) з параметром γ=4 (Q=8) для двох точок фокусування $z_F=0{,}05z_d$ і $z_F=z_d$ ($z^n=0{,}05$ і $z^n=1{,}0$) відповідно.

Як видно з рис. 1, вплив помилок розташування випромінювачів у площині X0Y на рівень щільності потоку потужності ЕМВ позначається тільки в першій половині зони Френеля. При цьому зменшення значення $S_H$ не перевищує 5 % на дальності $z_F = 0{,}05 z_d$ при $\Delta\rho = \lambda$. Зі збільшенням дальності до точки фокусування $z_F \geq 0{,}5 z_d$ вплив помилок розташування випромінювачів у площині X0Y стає несуттєвим. Вплив помилок розташування фазових центрів випромінювачів по осі 0Z не залежить від дальності до точки фокусування. Область допустимих значень $\Delta h$, у якій зменшення значення $S_H$ не перевищує 10 %, визначається з умови

$$\Delta h \leq \lambda/6 \ . \tag{5}$$

Проведене математичне моделювання показує, що помилки розташування фазових центрів окремих джерел випромінювання плоскої ФАР, що дорівнюють $\Delta\rho = \lambda$ і $\Delta h = \lambda/6$, практично не впливають на тривалість і період повторення ПЧІ.

**Вимоги до дискретності та точності встановлення початкових фаз і несучих частот за апертурою плоских ФАР**

Аналіз запропонованих методів формування послідовностей коротких ПЧІ під час використання багатоступеневих V-подібних законів розподілу опорних частот за апертурою плоских ФАР проводили без урахування можливих помилок установлення початкових фаз і опорних частот у передавальних каналах. Однак під час практичного здійснення синфазного складання полів від великої кількості джерел випромінювання завдяки випадковим неконтрольованим змінам параметрів закону ПФЧ керування випромінюваними сигналами можливе істотне погіршення характеристик ФАР.

Під час проведення розрахунків математичного очікування нормованого значення щільності потоку потужності плоскої ФАР з урахуванням помилок установлення опорних частот і початкових фаз випромінюваних сигналів приймали вихідні дані, наведені вище. Розрахунок здійснювався на основі виразу (1) з урахуванням випадкових помилок у встановленні заданої дискретності початкових фаз виду

$$\varphi_{0mn}^{\Delta} = -2\pi f_{0mn}\left(\frac{z_F}{c} - \frac{R_{Fmn}}{c}\right) + \Delta\varphi\Psi_1; \tag{6}$$

де $\Delta\varphi$ – максимальне значення помилки встановлення початкової фази в кожному випромінювальному елементі ФАР; $\Psi_1$ – випадкова величина, рівномірно розподілена в межах інтервалу [-1,1].

При цьому багатоступінчастий V-подібний закон розподілу несучих частот (див. (4)) з урахуванням помилок матиме вигляд

$$f_{0mn}^{\Delta} = \begin{cases} f_0 + \gamma\left[\frac{|m|}{\gamma}\right]\Delta F_x + \Delta f\Psi_2, & \text{если } \gamma\left[\frac{|m|}{\gamma}\right]\Delta F_x \geq \gamma\left[\frac{|n|}{\gamma}\right]\Delta F_y, \\ f_0 + \gamma\left[\frac{|n|}{\gamma}\right]\Delta F_y + \Delta f\Psi_2, & \text{если } \gamma\left[\frac{|m|}{\gamma}\right]\Delta F_x < \gamma\left[\frac{|n|}{\gamma}\right]\Delta F_y; \end{cases}$$

де $\Delta f$ – максимальне значення помилки встановлення несучої частоти в кожному випромінювальному елементі ФАР; $\Psi_2$ – випадкова величина, рівномірно розподілена в межах інтервалу [-1,1].

Розглянемо вплив помилок в установці заданих дискретностей несучої частоти і початкової фази в кожному випромінювальному елементі на характеристики випромінювання плоскої ФАР. На рис. 2 наведено значення математичного очікування нормованої щільності потоку потужності випромінювання плоскої ФАР $\overline{S}_н = \langle S(x,y,z,t)/S_{\max} \rangle$ у напрямі нормалі

до розкриву без урахування помилок установлення опорних частот і початкових фаз (Δφ = 0; Δf = 0; Q = 32), з урахуванням максимального значення помилки установлення початкових фаз Δφ=π/2 та з урахуванням максимального значення помилки установлення опорних частот Δf=$\Delta F_x/8=\Delta F_y/8$ у разі використання багатоступеневого V-подібного закону розподілу частот за апертурою (див. (4)) для точки фокусування $z_F = z_d$ .

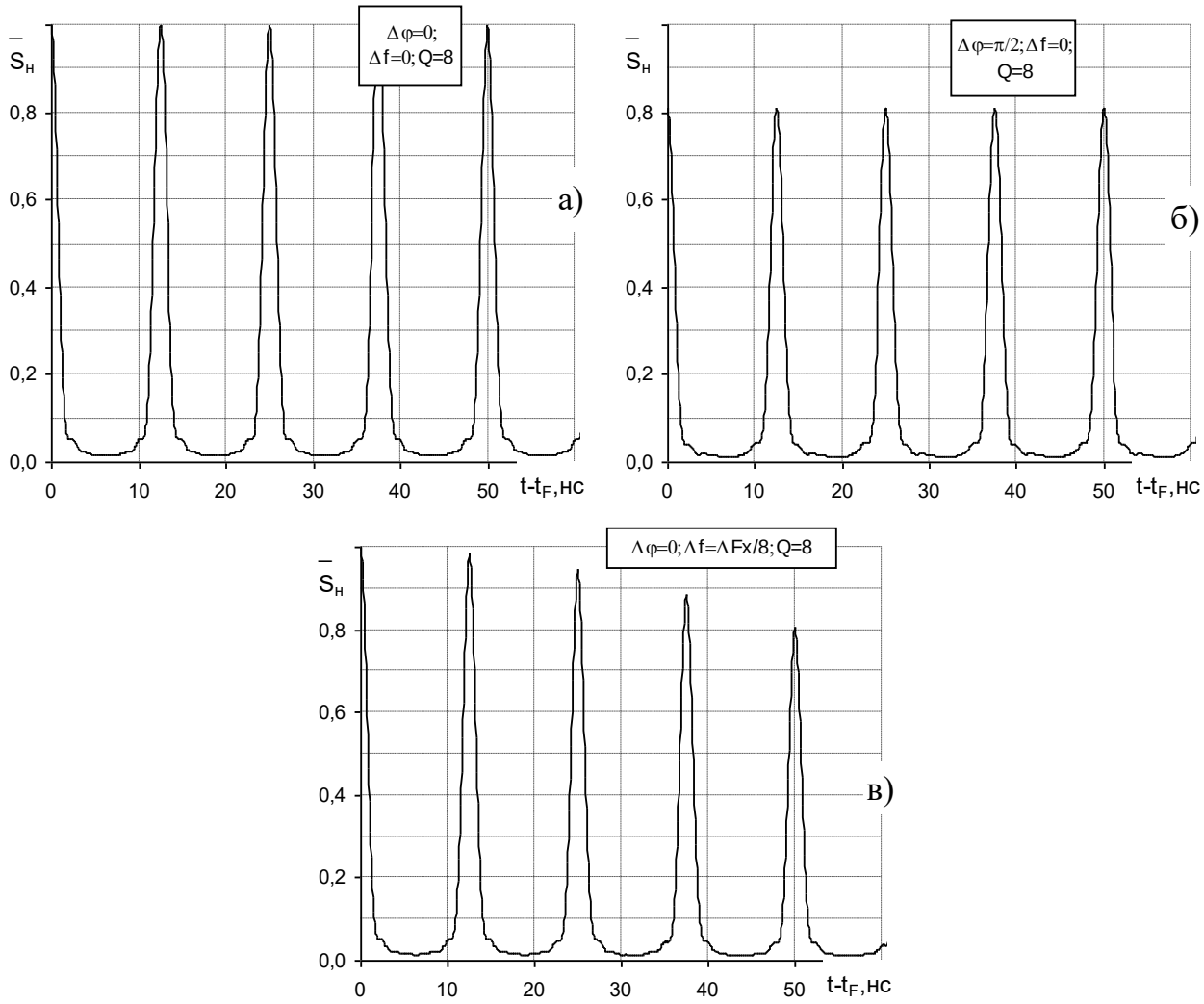


Рис. 2. Залежності математичного очікування нормованої щільності потоку потужності ФАР від помилок Δφ і Δf: *а*) за Δφ=0, Δf=0; *б*) за Δφ=p/2, Δf=0; *в*) за Δφ=0, Δf=ΔFx/8

Як видно з рис. 2, вплив помилок у встановленні заданої дискретності початкових фаз на характеристики сформованої послідовності ПЧІ не залежить від часу випромінювання. Вплив помилок у встановленні заданої дискретності несучих частот залежить від часу випромінювання, оскільки фазові помилки

$$\Delta\varphi_{0mn} = 2\pi f_{0mn}^{\Delta}\left(t - t_F\right),$$

зумовлені неточністю встановлення несучих частот випромінюваних сигналів, наростають із часом. На рис. 3 наведено залежності математичного очікування нормованого значення щільності потоку потужності випромінювання плоскої ФАР $\bar{S}_н$ від часу спостереження з урахуванням максимального значення помилки встановлення опорних частот Δf=2,0 МГц у разі використання багатоступеневого V-подібного закону розподілу частот за апертурою (див. (4)) з максимальними розносами несучих частот $\Delta F_{\max}$ , рівними 160 , 320 МГц.

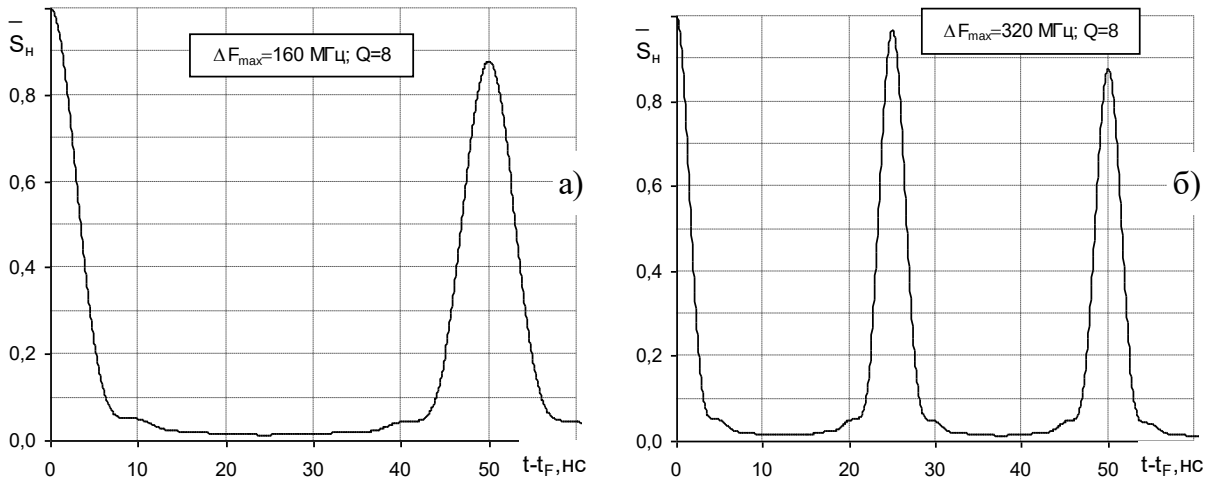


Рис. 3. Залежності математичного очікування нормованої щільності потоку потужності ФАР від часу випромінювання за Δf=2,0 МГц: *а* – ΔFmax=160 МГц; *б* – ΔFmax=320 МГц

Аналіз рис. 3 показує, що вплив помилок установлення несучих частот не залежить від обраного значення максимального розносу несучих частот за апертурою та визначається значенням помилки установлення несучої частоти у випромінювальних елементах Δf (або абсолютною нестабільністю частоти).

На рис. 4 наведено залежність математичного очікування нормованого значення щільності потоку потужності випромінювання плоскої ФАР від значень абсолютної нестабільності частоти Δf і різних значень тривалості пачки ПЧІ. Як видно з рис. 4, при врахуванні впливу помилок встановлення несучої частоти у випромінювальних елементах необхідно враховувати тривалість сформованої пачки ПЧІ. Як відомо [12, 13], в наявних передавальних пристроях сантиметрового діапазону хвиль значення довготривалої (за кілька годин і до доби) відносної нестабільності частоти забезпечується на рівні $10^{-5}...10^{-6}$, а короткочасної (за час до одиниць хвилин) – може досягати значень $10^{-10}...10^{-12}$ [13]. З урахуванням цього тривалість пачки ПЧІ, за якої густина потоку потужності знижується не більше ніж на 10 % через помилки встановлення несучої частоти у випромінювальних елементах ФАР, можна вибирати з умови $\Delta f T \le 0{,}1$, де $T = nT_{пчі}$ тривалість пачки періодичної послідовності $n$ сформованих ПЧІ.

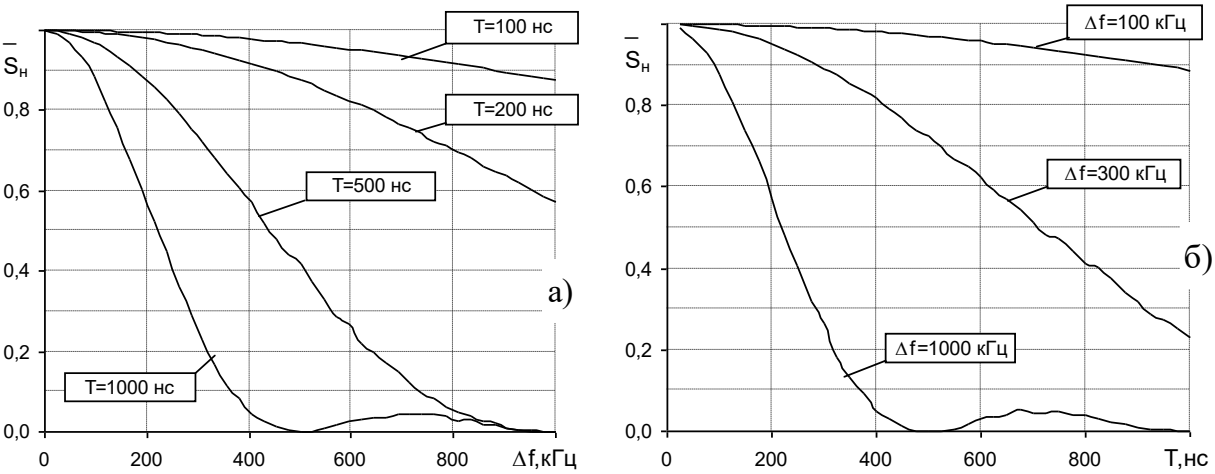


Рис. 4. Залежність математичного очікування нормованої щільності потоку потужності випромінювання плоскої ФАР: *а* – від тривалості пачки ПЧІ; *б* – від Δf

На рис. 5 наведено залежність $\bar{S}_н$ у напрямку нормалі до розкриву ФАР від максимальних значень помилок встановлення початкових фаз для точки фокусування $z_F = z_d$. Як

видно з рис. 5, область допустимих значень максимальних помилок установлення початкових фаз $\Delta\varphi$ за апертурою плоскої ФАР, у якій зменшення значення $\overline{S}_н$ не перевищує 10 %, визначається з умови

$$\Delta\varphi \le \pi/3. \qquad (7)$$

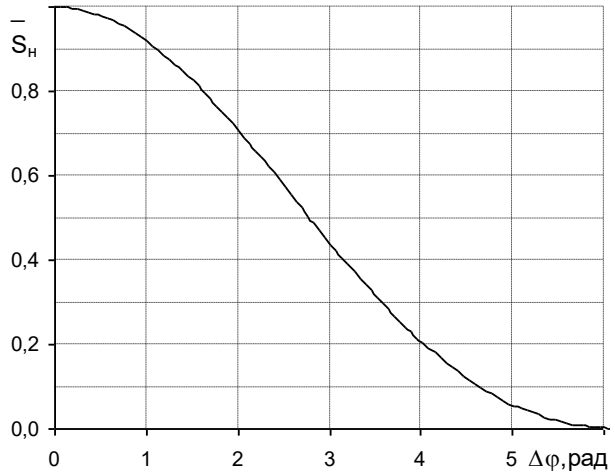


Рис. 5. Залежність математичного очікування нормованої щільності потоку потужності випромінювання ФАР від помилок $\Delta\varphi$ за умови $z_F=z_d$

Проведене математичне моделювання показує, що дискретність і випадкові помилки встановлення початкових фаз сигналів у передавальних каналах плоскої ФАР, що дорівнюють $\Delta\varphi = \pi/3$, практично не впливають на тривалість і період повторення послідовності ПЧІ.

**Висновки**

1. Розглянуті помилки розташування випромінювачів за апертурою ФАР у площині X0Y впливають на рівень щільності потоку потужності ЕМВ. Найсуттєвіше це позначається в першій половині зони Френеля. Зі збільшенням дальності до точки фокусування $z_F \ge 0{,}5z_d$ вплив цих помилок стає менш істотним. Вплив помилок розташування фазових центрів випромінювачів по осі 0Z не залежить від дальності до точки фокусування. Область допустимих значень $\Delta\rho$ і $\Delta h$, в якій зменшення значення $S_H$ не перевищує 10 %, визначається з таких умов: $\Delta\rho \le \lambda$ і $\Delta h \le \lambda/6$.

2. Вплив помилок установки початкових фаз на характеристики сформованої послідовності ПЧІ не залежить від часу випромінювання. Область допустимих значень максимальних помилок встановлення початкових фаз $\Delta\varphi$ за апертурою плоскої ФАР, у якій зменшення значення $S_H$ не перевищує 10 %, визначається з умови $\Delta\varphi \le \pi/3$. Дискретність і випадкові помилки встановлення початкових фаз окремих джерел випромінювання плоскої ФАР, що дорівнюють $\Delta\varphi = \pi/3$, практично не впливають на тривалість і період повторення послідовності ПЧІ.

3. Вплив помилок установлення несучих частот залежить від тривалості випромінювання, оскільки фазові помилки, зумовлені неточністю установлення несучих частот випромінюваних радіоімпульсів, наростають із часом. Аналіз помилок установлення несучих частот у каналах плоскої ФАР показав, що їхній вплив не залежить від обраного значення максимального розносу несучих частот за апертурою та визначається значенням помилки установлення несучої частоти у випромінювальних елементах (або абсолютною нестабільністю частоти). Тривалість пачки ПЧІ, за якої щільність потоку потужності знижується не більше ніж на 10 % через помилки встановлення несучих частот у випромінювальних елементах ФАР, обирається з умови $\Delta fT \le 0{,}1$, де $T = nT_{пчі}$ – тривалість пачки періодичної послідовності $n$ сформованих ПЧІ.

**Список літератури:**

1. Сазонов Д.М. Антенны и устройства СВЧ. Москва : Высш. шк., 1988. 432 с.
2. Зиолковски Р.В. Новые импульсы направленной электромагнитной энергии // SPIE. Microwave and Particle Beam Sources and Propagation. 1988. Vol. 873.
3. Фельсен Л.В., Хейшан Е. Методы фокусировки луча от распределенных апертур // SPIE. Microwave and Particle Beam Sources and Propagation. 1988. Vol.873.
4. Содин Л.Г. Характеристики импульсного излучения антенн (электромагнитного снаряда) // Радиотехника и электроника. 1992. Т.37, № 5. С. 849–857.
5. Гомозов В.И., Гомозов А.В. Новый метод фокусировки электромагнитных излучений // Антенны. 2001. Вып. 3(49). С. 54-60.
6. Гомозов В.И., Гомозов А.В. Титов С.В. Пространственно-фазово-частотная фокусировка сигналов в плоских ФАР при V-образной дискретизации частот // Радиотехника. 2001. Вып. 122. С. 201–207.
7. Гомозов В.И., Гомозов А.В., Титов С.В. Метод формирования последовательностей сфокусированных пространственно-временных импульсов при использовании многоступенчатого V-образного распределения частот по апертуре плоских ФАР // Радиотехника. 2002. Вып. 130. С. 33–38.
8. Сканирующие антенные системы СВЧ. Т.I ; пер. с англ. под ред. Г.Т.Маркова и А.Ф. Чаплина. Москва : Сов. радио, 1966. 536 с.
9. Шифрин Я.С. Вопросы статистической теории антенн. Москва : Сов. радио, 1970. 384 с.
10. Маляревский Н.М. Погрешность измерения вероятностей // Известия вузов. 1962. № 2. С. 73–76.
11. Рабинович Б.Е. Методика суммирования частных погрешностей в области радиотехнических измерений // Вопросы радиоэлектроники. Сер. VI. Радиоизмерительная техника // Науч.-техн. сб. 1961. Вып. 4. С. 3–20.
12. Kovalenko A., Titov S., Titova E., Cherna O. Estimation of requirements to signal parameters at V-shaped frequency distribution in mathematical model of multi-position transmitter system // Radiotekhnika. 2022. No209. P. 178–184. DOI: 10.30837/rt.2022.2.209.17
13. Уманский В.С. Усилительный тракт импульсных передающих устройств СВЧ. Москва : Сов. радио, 1973. 256 с.
14. Гомозов А.В., Гомозов В.И., Ермаков Г.В., Титов С.В. Фокусировка электромагнитного излучения и ее применение в радиоэлектронных средствах СВЧ ; под ред. В.И. Гомозова. Харьков : КП «Городская типография», 2011. 330 с.
15. Математическое и информационное обеспечение многоступенчатого V-образного управления частотой пространственно-распределенной передающей системы / С. В. Титов, Е. В. Титова // Системи обробки інформації. Харьков : ХУПС. 2016. Вип. 2(139). С. 63–67.

*Надійшла до редколегії 15.05.2023*

*Відомості про авторів:*

**Коваленко Андрій Іванович** – канд. техн. наук, старший науковий співробітник, Харківський національний університет радіоелектроніки, доцент кафедри системотехніки, Україна; e-mail: andrey.kovalenko@nure.ua; ORCID: https://orcid.org/0000-0003-2882-5082

**Тітов Сергій Володимирович** – канд. техн. наук, доцент, Харківський національний університет радіоелектроніки, доцент кафедри системотехніки, Україна; e-mail: serhii.titov@nure.ua; ORCID: https://orcid.org/0000-0003-0910-4415

**Тітова Олена Вітольдіївна** – канд. техн. наук, доцент, Харківський національний університет радіоелектроніки, доцент кафедри інформатики, Україна; e-mail: olena.titova@nure.ua; ORCID: https://orcid.org/0000-0001-8894-2040

**Чорна Ольга Сергіївна** – канд. техн. наук, Харківський національний університет радіоелектроніки, старший викладач кафедри системотехніки, Україна; e-mail: olha.chorna@nure.ua; ORCID: https://orcid.org/0000-0001-6745-8137

**УДК 621.396.96** **DOI:10.30837/rt.2023.2.213.09**

*І.В. СВИД, канд. техн. наук*

# ПОРІВНЯЛЬНИЙ АНАЛІЗ ЯКОСТІ ВИЯВЛЕННЯ ПОВІТРЯНИХ ОБ'ЄКТІВ ВТОРИННИМИ РАДІОЛОКАЦІЙНИМИ СИСТЕМАМИ

## Вступ

Суттєву роль в інформаційному забезпеченні системи контролю повітряного простору та управління повітряного руху відіграють вторинні радіолокаційні системи спостереження повітряного простору, до яких відносять вторинні радіолокатори [1 – 5] та запитальні системи ідентифікації за ознакою «свій-чужий» [6 – 9]. Слід зазначити, що у існуючих мережах радіолокаційних систем спостереження супровід повітряних об'єктів (ПО), як правило, здійснюється за інформацією первинних радіолокаційних систем спостереження [10 – 14], а вторинні радіолокаційні системи спостереження використовуються у якості джерел додаткової радіолокаційної інформації [15 – 17]. Але перехід на автоматичне залежне спостереження [18 – 22, 10] передбачає обов'язкову наявність лише вторинних радіолокаційних систем спостереження повітряного простору. У зв'язку з цим, актуальними є питання оцінки якості виявлення повітряних об’єктів вторинними радіолокаційними системами, специфіка побудови та функціонування яких суттєво відрізняються від первинних радіолокаційних систем спостереження повітряного простору. Специфіка вторинних радіолокаційних систем спостереження повітряного простору обумовлена [23 – 42]:

- реалізацією літакового відповідача (ЛВ) вторинних радіолокаційних систем за принципом відкритої одноканальної системи масового обслуговування з відмовами [23 – 25];
- одноканальним принципом обслуговування сигналів запиту [26 – 28];
- використанням специфічних сигналів (інтервально-часових та позиційних кодів) у якості сигналів запиту та відповіді [29 – 32];
- несинхронним принципом побудови мережі вторинних радіолокаційних систем спостереження повітряного простору [33 – 36].

Ці особливості реалізації вторинних радіолокаційних систем спостереження та наявність значної інтенсивності навмисних та ненавмисних (внутрісистемних) завад [10] значної інтенсивності зумовили суттєве зменшення коефіцієнта готовності літакових відповідачів $P_0$ вторинних радіолокаційних систем [37, 38, 42]. При цьому слід зазначити, що коефіцієнт готовності літакових відповідачів є відносною пропускною здатністю літакового відповідача [23] інформаційних систем, що розглядаються. Ці обставини необхідно враховувати при реалізації пристроїв виявлення ПО за сигналами вторинних радіолокаційних систем спостереження повітряного простору.

Слід зазначити, що побудова існуючих вторинних радіолокаційних систем спостереження за принципом несинхронної мережі, де використовується обслуговування першого вірно прийнятого сигналу запиту та відкритої одноканальної системи масового обслуговування з відмовами [24], негативно впливає як на якість обробки радіолокаційної інформації, так і на процес виявлення повітряних об’єктів зазначеними інформаційними системами. Тобто така побудова зазначених радіолокаційних систем відкриває широкі можливості як до несанкціонованого використання відповідачів інформаційних систем, що розглядаються, для отриманні координатної та польотної інформації, так і для повної паралізації літакових відповідачів шляхом постановки корельованих завад необхідної інтенсивності. Тому робота літакового відповідача в полі дії багатьох вторинних радіолокаційних систем спостереження, що створюють внутрісистемні завади значної інтенсивності, призводить до того, що коефіцієнт гото-

вності відповідача (КГ) $P_0$ завжди менше одиниці. При цьому слід зазначити, що коефіцієнт готовності літакового відповідача є функцією інтенсивності потоку сигналів запиту, утвореного потоком сигналів запиту від радіолокаційних систем спостереження, потоком навмисних корельованих завад, а також потоком сигналів запиту, що утворився з потоку навмисних та ненавмисних некорельованих завад.

Метою роботи є порівняльний аналіз оптимальної та квазіоптимальної структур виявлення повітряних об'єктів вторинними радіолокаційними системами.

**Порівняльний аналіз якості виявлення повітряних об'єктів вторинними радіолокаційними системами спостереження повітряного простору**

Виявлення ПО вторинними радіолокаційними системами здійснюється на підставі виявлення пачок прийнятих сигналів відповіді. Наявність кінцевого значення КГ ЛВ та присутність значної інтенсивності внутрісистемних та навмисних завад приводить до збільшення імовірності подавлення окремих імпульсів сигналів відповіді (СВ), що приводить до значного ускладнення алгоритмів виявлення ПО вторинними радіолокаційними системи. Тому особливу актуальність має завдання оптимізації виявлювача ПО, у зв'язку з наявністю значних потоків, як внутрісистемних, так і навмисних завад, що є характерним для інформаційних систем, що розглядаються [25 – 27].

Розглянемо задачу статистичного синтезу оптимального виявлювача ПО за пачкою сигналів відповіді з урахуванням коефіцієнта готовності ЛВ та імовірності подавлення окремих імпульсів сигналів відповіді при дії внутрісистемних та навмисних корельованих та некорельованих завад в каналі відповіді.

Будемо розглядати спільний вплив навмисних та внутрісистемних завад у каналі запиту, що включає: випромінювання СВ з імовірністю $(1-P_0)$, внутрісистемних завад у каналі відповіді, які приводять до подавлення окремих СВ з імовірністю $P_p$, та флуктуаційних шумів з рівномірною характеристикою в смузі пропускання приймача системи вторинної радіолокації у каналі відповіді.

Позначимо вибірку бінарно-квантованих радіолокаційних спостережень повітряного простору, отриманих за $k$-м сигналом запиту вторинної радіолокаційної системи усередині деякого кільця дальності, через $Y_k = (y_{1k},...,y_{nk})$, де $y_{ik}$ приймають значення нуль або одиниця, $i = 1,2,...,n$; $k = 1,2,...,N$; $n$ – значність коду СВ; $N$ – загальне число СВ в пачці сигналів, що приймаються.

Якщо маємо гіпотезу $H_1$ про присутність у радіолокаційних спостереженнях сигналів із шумом, то в кожному сигналі запиту з імовірністю $(1-P_0)P_p$ радіолокаційні спостереження створені тільки шумом і з імовірністю $P_0(1-P_p)$ – сумою сигналу та шуму. Функцію правдоподібності (ФП) гіпотези наявності сигналу $H_1$ для пачки сигналів, які приймаються $\vec{Y} = \|Y_1, Y_2,..., Y_N\|$, у випадку, що розглядається, можливо записати у наступному виді:

$$L(\vec{Y} \mid H_1; P_0; P_p) = \prod_{k=1}^{N} \left\{ P_0(1-P_p) \prod_{i=1}^{n} P_{11}^{y_{ik}}(k)(1-P_{11}(k))^{1-y_{ik}} + (1-P_0)P_p \prod_{i=1}^{n} P_{01}^{y_{ik}}(1-P_{01})^{1-y_{ik}} \right\}, \quad (1)$$

де $P_{11}(k) = \int_{z_o}^{\infty} x \exp[-(x^2 + q_k^2)/2] I_0(q_k x) dx$, $q_k = qg(k)$; $q$ – відношення сигнал/завада за центром діаграми спрямованості антени вторинної радіолокаційної системи; $z_0$ – поріг виявлення сигналів, $I_0(x)$ – функція Бесселя, $g(k)$ – діаграма спрямованості антени системи вторинних радіолокаційних систем спостереження повітряного простору.

При цьому можна зазначити, що функція правдоподібності (ФП) гіпотези $H_0$, яка свідчить про відсутність сигнальної пачки СВ в радіолокаційних спостереженнях, дорівнює ФП гіпотези $H_1$ при $P_0 = 0$, тобто справедливе наступне співвідношення:

$$L\left(\vec{Y} \mid H_0\right) = L\left(\vec{Y} \mid H_1; 0\right). \quad (2)$$

Виходячи з викладеного вирішальне правило оптимального виявлення пачки СВ складається в порівнянні відношення правдоподібності прийнятої реалізації $l = \ln\left[L(\vec{Y} \mid H_1; P_o; P_p) / L(\vec{Y} \mid H_0)\right]$ з порогом виявлення $l_0$.

При цьому слід зазначити, що для наведених виразів ФП (1) чи (2) оптимальне вирішальне правило виявлення ПО буде приймати вигляд

$$l = \sum_{k=1}^{N} \eta(k, s_k) \geq l_0, \quad (3)$$

де $\eta$ – функція, яка визначає величинам $s_k$ вагу $\eta(k, s_k)$, яку можна розрахувати за виразом

$$\eta(k, s_k) = \ln\left\{ P_o(1-P_p)\left[\frac{P_{11}(k)}{P_{01}}\right]^{s_k}\left[\frac{1-P_{11}(k)}{1-P_{01}}\right]^{n-s_k} + (1-P_o)P_p \right\}, \quad (4)$$

де через $s_k$ позначене число виявлених імпульсів в $k$-му сигналі відповіді:

$$s_k = \sum_{i=1}^{n} y_{ik}, \quad 0 \leq s_k \leq n.$$

Відповідно до виразів (3) та (4), які вирішують правило виявлення повітряного об'єкта та містять у собі наступні операції: визначення кількості імпульсів, виявлених в $k$-му СВ, а також вибір заздалегідь розрахованої величини $\eta(k, s_k)$, яка залежить від положення даного сигналу запиту в пачці, отриманого в цьому запиті значення $s_k$, значення КГ $P_0$ та імовірності подавлення сигналів $P_p$.

Аналізуючи викладене, можна заключити, що оптимальне вирішальне правило виявлення пачки СВ вторинних радіолокаційних систем повинно враховувати значність коду сигналів $n$, коефіцієнт готовності літакового відповідача $P_0$ та імовірність подавлення СВ $P_p$. При цьому слід зазначити, що коли покласти $P_0 = 1$, $P_p = 0$ и $n = 1$, тоді співвідношення (3) та (4) є алгоритмом вагового виявлення пачки бінарно-квантованих сигналів для первинної радіолокаційної системи. В іншому окремому випадку, коли $P_0 = 1$ та $P_p = 0$, правило виявлення збігається з відомим правилом виявлення пачки сигналів при квантуванні огинаючої сигналу, що приймається, на $n+1$ рівень.

Отримані вирази дозволяють побудувати схему оптимального виявлювача $N$ бінарно-квантованих $n$-імпульсних сигналів відповіді радіолокаційної системи, що розглядається. Ускладнення отриманого алгоритму виявлення в порівнянні з відомим алгоритмом для первинних радіолокаційних систем полягає в тому, що необхідно використовувати лічильник для підрахунку імпульсів СВ та зберігання в запам'ятовувальному пристрої матриці вагових коефіцієнтів, які дозволяють врахувати КГ літакового відповідача та імовірність подавлення окремих імпульсів СВ.

Отримаємо розрахункові вирази для оцінки характеристик виявлення ПО розглянутого виявлювача. Зазначимо, що у КВ вторинних радіолокаційних систем відношення сигнал/завада досить велике. Це дозволяє приймати прямокутну апроксимацію діаграм спрямованості антени системи вторинних радіолокаторів.

При такій постановці питання для прямокутної огинаючої пачки СВ відношення сигнал/шум $q_k = q$ при $k = 1, \ldots, N$ відповідно, а величина $P_{11}$ не залежить від номера СВ в приймаємій пачці, а залежить лише від кількості виявлених у цьому сигналі відповіді імпульсів $s_k$.

Позначимо через $r_s$ число СВ пачки усередині фіксованого кільця дальності, в кожному з яких виявлено $s$ імпульсів, де $s = 0,1,\ldots,n$. Зазначимо, що з визначення $r_s$ слідує, що $r_0 + r_1 + \ldots + r_n = N$.

Поєднуючи в сумі (3) доданки з однаковими значеннями $s_k$ та з огляду на те, що кількість таких складових дорівнює $r_s$, отримуємо наступний вид правила виявлення пачки СВ вторинних радіолокаційних систем спостереження повітряного простору:

$$l = \sum_{s=0}^{n} r_s \eta(s) \geq l_0, \tag{5}$$

де $\eta(s)$ визначається за виразом (4), в котрому як $P_{11}$, так і $P_{01}$ не залежать від $k$.

Зазначимо, що з виразу (2) слідує, що імовірність хибної тривоги $F$ для системи вторинних радіолокаційних систем збігається з імовірністю правильного виявлення, якщо КГ ЛВ дорівнює нулю. Для цього випадку отримаємо вираз тільки для ймовірності правильного виявлення. Тоді випадкові величини $r_0, r_1, .., r_n$, як правило, підпорядковуються поліноміальному розподілу, що дозволяє записати вираз для імовірності правильного виявлення:

$$D = \sum_{\substack{r_0+\ldots+r_n=N \\ r_s>0}} \frac{N!}{r_0! r_1! \ldots r_n!} \prod_{s=0}^{n} \left\{ P_0 (1-P_p) C_n^s P_{11}^s (1-P_{11})^{n-s} + (1-P_0) P_p C_n^s P_{01}^s (1-P_{01})^{n-s} \right\}^{r_s}. \tag{6}$$

Підсумовування у зазначеному виразі (6) має проводитись за всіма наведеними числами $N$ у вигляді суми $n$ невід'ємних складових $r_0, r_1, .., r_n$, для яких виконується умова виявлення (5). Як слідує з наведеного виразу, імовірність правильного виявлення пачки СВ суттєво залежить від КГ літакового відповідача та імовірності подавлення окремих імпульсів СВ.

Для СВ з значністю інтервально-часового коду $n = 2$ умова виявлення (5) приймає наступний вид:

$$r_1 + \omega r_2 \geq c. \tag{7}$$

Відповідно до умови (7) виявлення пачки двохімпульсних СВ вторинними радіолокаційними системами зводиться до порівняння з порогом суми числа $r_1$ СВ з одним виявленим імпульсом і взятого з вагою $w$ числа кодів відповіді із двома виявленими імпульсами $r_2$. При цьому слід зазначити, що величина ваги показує, наскільки при виявленні ПО сигнали відповіді із двома виявленими імпульсами цінніше, ніж СВ з одним виявленим імпульсом. У випадку, якщо завада у каналі відповіді відсутня, тобто $P_p = 0$, величина ваги дорівнює двом і умова (7) зводиться до порівняння з порогом сумарного числа імпульсів у пачці СВ.

Якщо позначити через $A_i$ імовірність виявлення $i$ імпульсів у відповідному СВ ($i = 1,2$), то можна записати такі вирази:

$$A_0 = P_0 P_{10}^2 + (1-P_0) P_{00}^2, \; A_2 = P_0 P_{11}^2 + (1-P_0) P_{01}^2, \; A_1 = 2P_0 P_{11} P_{10} + 2(1-P_0) P_{01} P_{00}.$$

Тоді вираз для імовірності правильного виявлення повітряного об'єкта вторинними радіолокаційними системами приймає вид

$$D = \sum_{\substack{0 \leq r_i \leq N \\ r_0+r_1+r_2=N}} \frac{N!}{r_0! r_1! r_2!} A_0^{r_0} A_1^{r_1} A_2^{r_2}.$$

Підсумовування в даному виразі також робиться за всіма представленнями числа $N$ у вигляді суми $n$ невід'ємних складових $r_0, r_1, .., r_n$, для яких виконується умова виявлення.

При цьому слід зазначити, що так як $r_0 = N - r_1 - r_2$, то множник, що містить факторіали, є добутком біноміальних коефіцієнтів:

$$\frac{N!}{r_0!r_1!r_2!}=\frac{N!(N-r_2)!}{r_2!(N-r_2)!r_1!(N-r_2-r_1)!}=C_N^{r_2}C_{N-r_2}^{r_1}.$$

Перетворюючи умови підсумовування величин, отримаємо

$$D=\sum_{r_2=0}^{N}\sum_{r_1=\max\{0,c-wr_2\}}^{N-r_2}C_N^{r_2}C_{N-r_2}^{r_1}A_0^{N-r_1-r_2}A_1^{r_1}A_2^{r_2}=\sum_{r_2=0}^{N}C_N^{r_2}A_2^{r_2}\sum_{r_1=\max\{0,c-wr_2\}}^{N-r_2}C_{N-r_2}^{r_1}A_0^{N-r_1-r_2}A_1^{r_1}, \quad (8)$$

що і є оптимальним алгоритмом виявлення ПО вторинними радіолокаційними системами спостереження повітряного простору.

Зазначимо, що обробка СВ у вторинних радіолокаційних системах в сучасному використанні включає декодування СВ за цілочисловою логікою обробки $n/n$. Це обставина виключає з процесу виявлення ту частину імпульсів СВ, які залишилися після подавлення окремих імпульсів СВ у каналі відповіді. Імовірність проходження корисних та хибних сигналів через дешифратор для такої обробки сигналів можливо визначити виходячи з наступних виразів:

$$D_{11}=P_{11}^n;\ F_{01}=P_{01}^n,$$

тому що сигнали на виході дешифратора $x_k$ при надходженні на його вхід $Y_k$ є результатом логічного множення.

ФП гіпотези $H_1$ для пачки декодованих сигналів, що приймаються, можливо записати у вигляді співвідношення

$$L(\vec{X}\mid H_1;P_0;P_p)=\prod_{k=1}^{N}\left\{P_0(1-P_p)\prod_{i=1}^{n}D_{11}^{x_{ik}}(1-D_{11})^{1-x_{ik}}+(1-P_0)P_p\prod_{i=1}^{n}F_{01}^{x_{ik}}(1-F_{01})^{1-x_{ik}}\right\}.$$

У зазначеному випадку оптимальне вирішальне правило виявлення пачки, яка попередньо минула дешифратор СВ, зводиться до цифрового накопичення та порівняння з порогом числа декодованих СВ. Значення порога виявлення в цьому випадку також залежить від КГ ЛВ та імовірності подавлення СВ.

Імовірність правильного виявлення пачки СВ після декодування можна визначити з виразу

$$D=\sum_{j=c_1}^{N}C_N^j\left[P_0(1-P_p)D_{11}+(1-P_0)P_pF_{01}\right]^j\left[P_0(1-P_p)(1-D_{11})+(1-P_0)P_p(1-F_{01})\right]^{N-j}, \quad (9)$$

де $c_1$ – поріг прийняття рішення.

Таким чином, оптимізація виявлення пачки декодованих СВ зводиться до вибору порогів виявлення як і для синтезованого виявлювача, тобто з урахуванням КГ ЛВ та імовірності подавлення імпульсів СВ.

Проведемо порівняльну оцінку якості виявлення ПО за пачкою СВ синтезованого (оптимального) (8) та квазіоптимального (9) виявлювачів повітряних об'єктів для СВ с $n=2$. Імовірність правильного виявлення при постійному значенні імовірності хибної тривоги на виході виявлювача ПО, розраховану за виразом (8) з постійними параметрами $P$ та $w$, наведено на рис. 1. Розрахунки виконано при $C/N=0{,}3$; $N=27$; $q=2$ і для різних значень $P=P_0(1-P_p)$. Як слідує з рис. 1, при $P=1$ найкращі результати отримуємо для $w=2$, а зі зменшенням значення $P$ величина оптимальної ваги збільшується. Так, при $P=0{,}6$ оптимальна вага складає $w=2{,}4$ , а при $P=0{,}4$ найкращі результати отримуються для $w=3$.

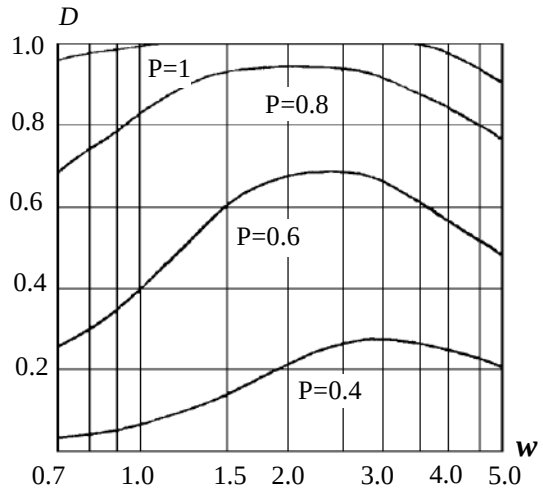


Рис. 1. Залежність $D = f(w, P)$

Для кожного значення співвідношення сигнал/завада, КГ ЛВ та імовірності подавлення СВ, як для синтезованого, так і для реалізованого у вторинних радіолокаційних системах алгоритмів виявлення ПО за пачкою СВ існують оптимальні значення як порогів, так і ваг, що забезпечують максимум $D$ при постійній імовірності хибної тривоги $F$.

Для реалізованого у вторинних радіолокаційних системах квазіоптимального виявлювача, що порівнює з порогом $c_1$ (9), загальне число дешифрованих СВ, також існує оптимальне значення порога, яке залежить від відношення сигнал/завада і величини $P$. Зі збільшенням співвідношення сигнал/завада і зниженням $P$ оптимальне значення порога збільшується при підтримці постійної величини імовірності хибної тривоги вибором відповідного порога виявлення.

У порівнянні із синтезованим виявлювачем повітряних об'єктів, що порівнює з порогом число декодованих СВ, програє в пороговому сигналі 1–1,5 дБ, за умови вибору для кожного з виявлювачів оптимальних для них значень порогових рівнів і ваг.

Програш у граничному сигналі при виборі постійного порога виявлення $c_1$ пачки дешифрованих СВ замість оптимального змінного $c_1$, який максимізує імовірність виявлення $D$ при постійної $F$, також суттєво залежить від величини $P$ (рис. 2).

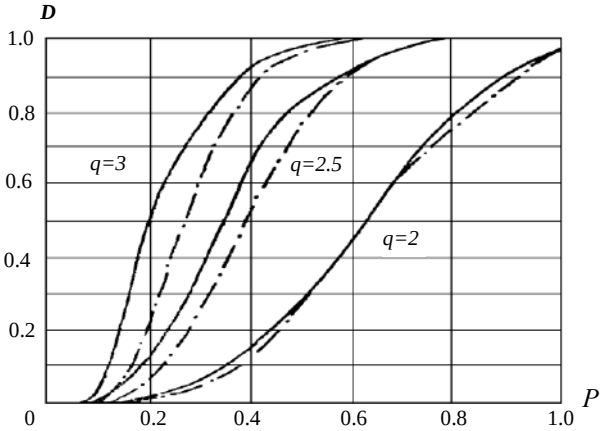


Рис. 2. Залежність $D = f(q, P)$

Для виявлення пачки СВ після декодування при $P < 1$ та досить великому співвідношенні сигнал/завада оптимальне значення порога виявлення наближається до одиниці (рис. 2). При

цьому варто відмітити, що величина $q$, при якій виконується ця умова, залежить від довжини пачки СВ, КГ ЛВ і ймовірності подавлення СВ.

Зазначимо, що вторинні радіолокаційні системи реалізуються на принципі несинхронної мережі, що дозволяє захистити запитувачі від несинхронних завад. Ця обставина та результати, які наведено на рис. 3, дозволяють зробити висновок, що поріг виявлення ПО для вторинних радіолокаційних систем при впливі як внутрісистемних, так і навмисних завад у КЗ та КВ варто вибирати незначним.

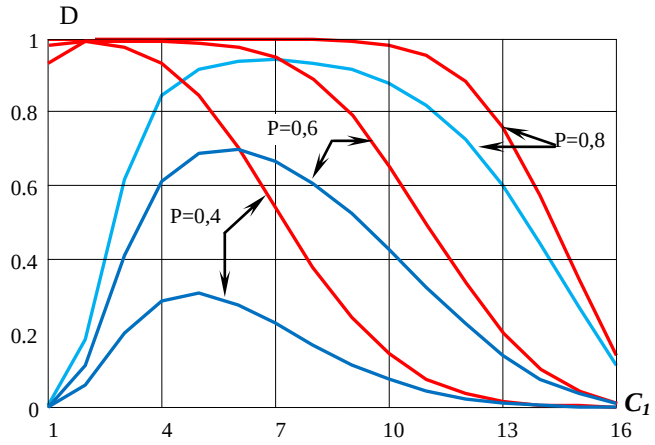


Рис. 3. Імовірність виявлення як функція порогу виявлення

Аналіз характеристик виявлення показує, що оптимальні пороги виявлення ПО за пачкою СВ суттєво залежать від КГ ЛВ та імовірності подавлення окремих імпульсів СВ у КВ. Застосування ж декодування СВ та наступного накопичення при виборі оптимального порога суттєво знижує характеристики виявлення в порівнянні з оптимальною обробкою пачки СВ (рис. 3). Так, при порозі виявлення, що дорівнює 7 та величині $P = 0{,}8$, імовірність виявлення ПО для оптимального алгоритму складає 1, а для квазіоптимального – 0,95. При $P = 0{,}6$ імовірності відповідно дорівнюють 0,95 та 0,7, а при $P = 0{,}4$ – відповідно 0,55 та 0,23.

Розглянемо область великих значень співвідношень сигнал/завада, при яких флуктуаційними завадами у КВ можна знехтувати. У цьому випадку характеристики виявлення визначаються довжиною відповідної пачки прийнятих сигналів, КГ ЛВ та імовірністю подавлення окремих імпульсів СВ у КВ.

Імовірності правильного виявлення пачок СВ для оптимального та квазіоптимального алгоритмів, при постійних значеннях $N$ та $P$, сходяться до границі

$$D = \sum_{i=c}^{N} C_N^i P^i (1-P)^{N-i}, \qquad (10)$$

величина якої залежить від цифрового порога виявлення $c$.

При заданих значеннях $D, N$ та $c$ вираз (10) являє собою рівняння відносно $P$. Корінь цього рівняння є граничним значенням КГ та імовірності подавлення імпульсів СВ $P$, що має наступні властивості:

- якщо $P$ більше за порогове значення, то для КВ вторинних радіолокаційних систем існує таке значення співвідношення сигнал/завада, що при заданому $P$ забезпечує задане значення імовірності правильного виявлення ПО;

- якщо $P < P^*(D, N, c)$, то незалежно від значення співвідношення сигнал/завада у каналі відповіді низький КГ ЛВ та висока ймовірність подавлення імпульсів СВ не дозволяють ймовірності $D$ досягти заданої величини при фіксованих $N$ та $c$. На відміну від співвідношення сигнал/завада збільшення довжини пачки сигналів, що приймаються, завжди дозволяє досягти заданої величини ймовірності $D$ незалежно від значення $P$.

На рис. 4 наведено залежності порогового значення $P$ від довжини пачки $N$ сигналів, що приймаються, для різних значень імовірності виявлення $D$. Суцільна крива відповідає порогу, що дорівнює одиниці, штрихова крива – порогу, що дорівнює двом. Як видно з рис. 4, імовірність правильного виявлення, що дорівнює 0,95 при $N=12$ та виборі порога, рекомендованого для первинної радіолокаційної системи, досягається при $P=0{,}4$, у той час як при виборі порога, що дорівнює двом, ця ймовірність досягається при $P=0{,}22$. Це вказує на те, що вибір порога для виявлення сигналів вторинними радіолокаційними системами суттєво відрізняється від оптимального порога виявлення для первинних радіолокаційних систем.

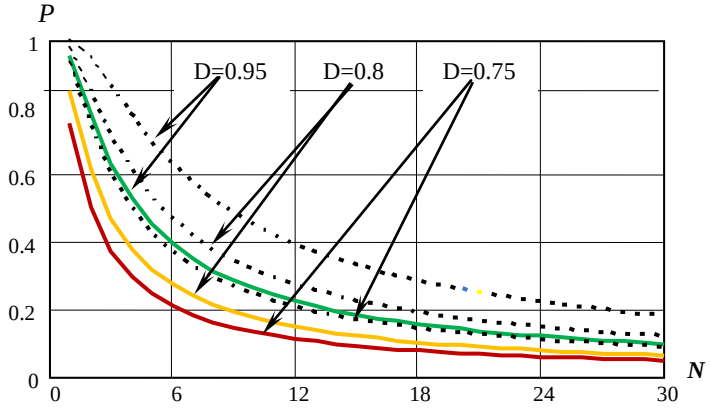


Рис. 4. Залежність $P=f(D,N)$

Таким чином, підвищення імовірнісних характеристик системи вторинних радіолокаційних систем при роботі ЛВ у полі значних потоків навмисних та внутрісистемних завад забезпечується вибором порогів виявлення залежно від значень КГ відповідача та імовірності подавлення окремих імпульсів СВ. З іншого боку, застосування оптимальних для даних умов роботи відповідача порогів виявлення на системах вторинних радіолокаційних систем дозволяє знизити вимоги до пропускної здатності ЛВ при значній інтенсивності потоків внутрісистемних та навмисних корельованих завад.

**Висновки**

Аналіз характеристик виявлення повітряних об’єктів системами вторинних радіолокаційних систем показує що:

1. Оптимальні пороги виявлення повітряних об’єктів в системах вторинної радіолокації суттєво залежать від коефіцієнта готовності літакового відповідача та імовірності подавлення окремих імпульсів сигналів відповіді в каналі відповіді.

2. Використання декодування сигналів відповіді та подальшого накопичення при виборі оптимального порога значно знижує показники якості виявлення в порівнянні з оптимальною обробкою пачки сигналів відповіді.

3. Цифровий поріг виявлення повітряних об’єктів системою вторинної радіолокації значною мірою залежить від імовірності подавлення сигналів в каналі запиту та каналі відповіді.

**Список літератури:**

1. M. Leonardi and D.D. Fausto. Secondary Surveillance Radar Transponders classification by RF fingerprinting // 2018 19th International Radar Symposium (IRS), 2018, pp. 1–10. doi: 10.23919/IRS.2018.8448244.

2. M. Skolnik. Improvements for air-surveillance radar // Proceedings of the 1999 IEEE Radar Conference. Radar into the Next Millennium (Cat. No.99CH36249), 1999, pp. 18–21. doi: 10.1109/NRC.1999.767195.

3. I. Obod, I. Svyd, O. Maltsev and S. Starokozhev. The Effect of Masking Interference on the Quality of Request Signal Detection in Aircraft Responders of the Identification Friend or Foe Systems // 2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T), 2020, pp. 721–726. doi: 10.1109/PICST51311.2020.9467955.

4. F. L. Neindre, G. Ferre, D. Dallet, F. Letellier and K. Pitois. A Successive Interference Cancellation-based Receiver for Secondary Surveillance Radar // IEEE Transactions on Aerospace and Electronic Systems, 2022. doi: 10.1109/TAES.2022.3193649.

5. M. Barbary, A. S. Hafez and T. Crew. An Industrial Design and Implementation Approach of Secondary Surveillance Radar System // 2021 International Telecommunications Conference (ITC-Egypt), 2021, pp. 1–9. doi: 10.1109/ITC-Egypt52936.2021.9513961.

6. О.П. Черних, І.І. Обод, І.В.Свид. Інформаційне забезпечення на основі мереж спостереження повітряного простору // Eastern-European Journal of Enterprise Technologies, 2/9(50) 2011. Харків, 2011. С. 23–25. doi: 10.15587/1729-4061.2011.1850.

7. I. Svyd et al. Fusion of Airspace Surveillance Systems Data // 2019 3rd International Conference on Advanced Information and Communications Technologies (AICT), 2019. doi :10.1109/aiact.2019.8847916

8. I. Svyd, I. Obod, O. Maltsev, V. Andrusevich, B. Bakumenko and O. Vorgul. Optimal Measurement of Signal Data Parameters of Requesting Radar Systems // 2021 IEEE 3rd Ukraine Conference on Electrical and Computer Engineering (UKRCON), 2021, pp. 138–141. doi: 10.1109/UKRCON53503.2021.9575235.

9. I. Svyd, I. Obod, O. Maltsev and A. Hlushchenko. Secondary Surveillance Radar Response Channel Information Security Improvement Method // 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), 2020, pp. 341–345. doi: 10.1109/DESSERT50317.2020.9125018.

10. Свид І. В. Обробка радіолокаційної інформації систем спостереження повітряного простору : монографія. / І. В. Свид. Дніпро : ЛІРА ЛТД, 2022. 224 с.

11. Y. Jiang, Z. Yang, C. Bo, and D. Zhang. Continuous IFF response signal recognition technology based on capsule network // Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, 2021, pp. 455–468. doi: 10.1007/978-3-030-90196-7_39.

12. I. Svyd, I. Obod and O. Maltsev. Interference Immunity Assessment Identification Friend or Foe Systems // Ageyev D., Radivilova T., Kryvinska N. (eds) Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies, vol 69. Springer, Cham, pp. 287–306, 2021. doi: 10.1007/978-3-030-71892-3_12.

13. T. M. Schuck, B. Shoemaker and J. Willey. Identification friend-or-foe (IFF) sensor uncertainties, ambiguities, deception and their application to the multi-source fusion process // Proceedings of the IEEE 2000 National Aerospace and Electronics Conference. NAECON 2000. Engineering Tomorrow (Cat. No.00CH37093), 2000, pp. 85–94. doi: 10.1109/NAECON.2000.894896.

14. Толюпа С.В., Дружинін В.А., Гордієвський О.Т. Розпізнавання групових об'єктів у багатопозиційних системах оперативного супроводження // Сучасний захист інформації. 2012. No 1. С. 66–70.

15. Обод І.І., Стрельницький О.О. Інформаційна безпека інформаційної мережі систем спостереження повітряного простору // Системи обробки інформації. 2015. № 9(134). С. 96–98.

16. V. Semenets et al. Quality Assessment of Measuring the Coordinates of Airborne Objects with a Secondary Surveillance Radar // Ageyev D., Radivilova T., Kryvinska N. (eds) Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies. 2021. Vol 69. Springer, Cham, pp. 105–125. doi: 10.1007/978-3-030-71892-3_5.

17. I. Ivashko, O. Krasnov and A. Yarovoy. Performance analysis of multisite radar systems // 2013 European Microwave Conference, 2013, pp. 1771–1774. doi: 10.23919/EuMC.2013.6687021.

18. Обод І.І., Стрельницький О.О. Захист інформації в мережі систем спостереження повітряного простору // Системи обробки інформації. 2016. № 2(139). С. 47–49.

19. J. Xu, X.-Z. Dai, X.-G. Xia, L.-B. Wang, J. Yu and Y.-N. Peng. Optimizations of Multisite Radar System with MIMO Radars for Target Detection // IEEE Transactions on Aerospace and Electronic Systems, vol. 47, no. 4, pp. 2329–2343, OCTOBER 2011. doi: 10.1109/TAES.2011.6034636.

20. I. Svyd, I. Obod, O. Maltsev, O. Vorgul, V. Chumak and B. Bakumenko. Estimation of the Spatial Coordinates of Air Objects in Synchronous Radar Networks for Airspace Observation // 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T), 2021, pp. 425–428. doi: 10.1109/PICST54195.2021.9772227.

21. Обод И.И., Булай А.Н., Луценко Ю.А. Оценка точности определения местоположения воздушных объектов в синхронных информационных сетях радиолокации // Системи обробки інформації. 2006. № 9(58). С. 69–75.

22. Обод И.И., Булай А.Н., Луценко Ю.А. Оценка точности определения местоположения воздушных объектов в синхронных информационных сетях // Системи обробки інформації. 2006. № 9(58). С. 69–71.

23. H. You, X. Jianjuan, G. Xin. Radar Data Processing with Applications // Publishing House of Electronics Industry. 2016. doi: 10.1002/9781118956878.

24. Chen Su, Chuanyun Zou, Liangyu Jiao, Qianglin Zhang. A MIMO Radar Signal Processing Algorithm for Identifying Chipless RFID // Tags. Sensors (Basel). 2021 Dec 12;21(24):8314. doi: 10.3390/s21248314

25. Обод І.І., Стрельницький О.О., Андрусевич В.А. Методи підвищення якості інформаційного забезпечення системами спостереження повітряного простору // Системи обробки інформації. 2014. № 4(120). С. 53–55.

26. Обод І.І., Шевцова В.В. Порівняльний аналіз запитальних систем передачі інформації системи контролю повітряного простору // Зб. наук. пр. Харк. нац. ун-ту Повітряних Сил. 2013. № 1(34). С. 123–125.

27. І. Обод, І. Свид, О. Мальцев. Обробка даних радіолокаційних систем спостереження повітряного простору : навч. посібник. Харків : Друкарня Мадрид, 2021. 255 с.
28. J. Li, P. Stoica. MIMO Radar Signal Processing. Wiley-IEEE Press, 2008. 448 p.
29. S. M. Wu, G. A. Ybarra and W. E. Alexander. A complex optimal signal-processing algorithm for frequency-stepped CW data // IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing, vol. 45, no. 6, pp. 754–757, June 1998. doi: 10.1109/82.686697.
30. Толюпа С.В., Дружинін В. А., Наконечний В.С., Цьопа Н.В., Батрак Є.О. Методи та алгоритми обробки радіолокаційної інформації у багатопозиційних системах зі змінною просторовою конфігурацією. К.: Логос, 2014, 230 с.
31. Обод И.И. Обнаружение воздушных целей системой вторичной радиолокации // Радіоелектронні і комп'ютерні системи. 2005. № 3. С.25–28.
32. G. Lee, S. Lee, K. Kim and N. Kwak. Probabilistic Track Initiation Algorithm Using Radar Velocity Information in Heavy Clutter Environments // 2018 15th European Radar Conference (EuRAD), 2018, pp. 277–280. doi: 10.23919/EuRAD.2018.8546666.
33. Conte, E., Daddio, E., Farina, A., and Longo, M. Multistatic radar detection – Synthesis and comparison of optimum and suboptimum receivers // IEE Proceedings F: Communications Radar and Signal Processing, vol. 130, no. 6, pp. 484–494, 1983.
34. I. Prokopenko, V. Vovk and K. Prokopenko. Fast resource management algorithm for multi-position radar systems // 2015 16th International Radar Symposium (IRS), 2015, pp. 1045–1051. doi: 10.1109/IRS.2015.7226339.
35. V. Andrusevich and I. Obod. Assessment of the Quality of Information Support by Air Radar Surveillance Systems // Advanced Information Systems, vol. 5, no. 2, pp. 78–82, 2021. doi: 10.20998/2522-9052.2021.2.10.
36. I. Prokopenko, V. Vovk, S. Stavitsky and V. Medvedev. Optimization of use of resource in multi-position radar systems // 2014 IEEE Microwaves, Radar and Remote Sensing Symposium (MRRS), 2014, pp. 92–97. doi: 10.1109/MRRS.2014.6956673.
37. I. Obod et al. Optimization of Data Processing Structure for Multi-Position Radar Surveillance Systems // 2021 IEEE 3rd Ukraine Conference on Electrical and Computer Engineering (UKRCON), 2021, pp. 133–137. doi: 10.1109/UKRCON53503.2021.9575286.
38. I. Svyd, I. Obod, O. Maltsev, O. Vorgul, I. Vorgul and I. Shevtsov. Method for Increasing the Interference Immunity of the Channel for Measuring of the Short-Range Navigation Radio System // 2022 IEEE 16th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), Lviv-Slavske, Ukraine, 2022, pp. 802–807. doi: 10.1109/TCSET55632.2022.9767069.
39. I. Shevtsov et al. A Method for Increasing the Capacity of Radio Systems of Short-Range Navigation // 2022 IEEE 2nd Ukrainian Microwave Week (UkrMW), Ukraine, 2022, pp. 629–633. doi: 10.1109/UkrMW58013.2022.10037138.
40. S. Starokozhev et al. Frequency Efficiency Evaluation of Query Airspace Surveillance Systems // 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T), Kharkiv, Ukraine, 2021, pp. 501–505. doi: 10.1109/PICST54195.2021.9772190.
41. S. Starokozhev et al. Optimization of the Probability of Transmission of Flight Data in the Response Channel of Secondary Radar Systems // 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T), Kharkiv, Ukraine, 2021, pp. 511–515. doi: 10.1109/PICST54195.2021.9772199.
42. V. Semenets et al. Method of increasing the relative throughput of requesting radar systems // Przegląd Elektrotechniczny, vol. 1, no. 11, 2022, pp. 99–103. doi: 10.15199/48.2022.11.17.

*Надійшла до редколегії 21.05.2023*

*Відомості про автора:*
**Свид Ірина Вікторівна** – кандидат технічних наук, доцент, Харківський національний університет радіоелектроніки, завідувач кафедри мікропроцесорних технологій і систем; Харків, Україна; email: iryna.svyd@nure.ua; ORCID: http://orcid.org/0000-0002-4635-6542

# ABSTRACTS РЕФЕРАТИ

## SYSTEMS AND METHODS OF INFORMATION PROTECTION
## СИСТЕМИ І МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ

UDC 004.056.5

**Hash-based cryptography, its security and feasibility in modern cryptosystems** / *Ya.A. Derevianko, Ye.G. Kachko, I.D. Gorbenko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2023. №213. P. 7–17.

Hash-based signatures are one of the most promising classes of cryptographic schemes considered quantum resistant ones. The strength of cryptographic hash functions is one of the most important aspects of ensuring the security of hash-based schemes.

Since classical hash-based signatures require tracking the number of signatures used, they were considered to be stateful for a long time. The SPHINCS scheme overcome this limitation, subsequently refined to SPHINCS+.

The paper provides an assessment of the security of ES based on hash functions relative to side channel attacks. It also gives an analysis of recommendations for the use of one of the candidates of the NIST competition, based on hash cryptography - SPHINCS+, and conclusions about the feasibility of its use.

*Key words:* cryptographic schemes; hash function; SPHINCS scheme; NIST.

5 tabl. 3 fig. Ref: 14 items.

УДК 004.056.5

**Криптографія на основі гешу, її захищеність та доцільність застосування у сучасних криптосистемах /** *Я.А. Дерев'янко, О.Г. Качко, І.Д. Горбенко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2023. Вип. 213. С. 7–17.

ЕП на основі гешу є одним із найбільш перспективних класів криптографічних схем, які вважаються квантово стійкими. Стійкість криптографічних геш функцій є одним з найважливіших аспектів забезпечення захищеності схем на основі гешу.

Оскільки класичні ЕП на основі гешу вимагають відстеження кількості використаних підписів, довгий час вони вважалися такими, що мають стан. Це обмеження було подолано схемою SPHINCS, яку згодом було вдосконалено до SPHINCS+.

У роботі наводиться оцінка захищеності ЕП на геш функціях відносно атак бічними каналами. Також проводиться аналіз рекомендацій щодо використання одного з кандидатів конкурсу NIST, який базується на геш криптографії – SPHINCS+, і робляться висновки щодо доцільності його використання.

*Ключові слова:* криптографічні схеми; геш функції; схема SPHINCS; NIST.

Табл. 5. Іл. 3. Бібліогр.: 14 назв.

UDC 004.056.5

**Analysis of pseudorandom number generation processes in EP CRYSTALS-Dilithium** / *S.O. Kandiy* // Radiotekhnika: All-Ukr. Sci. Interdep. Mag. 2023. №213. P. 18–30.

The paper provides an analysis of pseudorandom number generation processes in the Crystals-Dilithium post-quantum electronic signature scheme, a finalist in the NIST PQC post-quantum cryptography competition. The main focus is on the pseudo-random number generator based on the AES block cipher in counter mode. A formal model was built for this pseudo-random number generator that meets the requirements of the latest version of the AIS 31 standard, containing requirements for secure pseudorandom number generators. A pseudo-random number generator based on the AES block cipher in counter mode is shown to satisfy the requirements of functional class DRG.3, provided that the initial value for the generator is obtained from a truly random number source (either a physically truly random or a non-physical truly random source) or another generator of pseudo-random numbers having a security class not lower than the DRG class.3. In addition, the use of shake128/256 for the generation of pseudorandom sequences in Crystals-Dilithium will be analyzed. Based on the results of the analysis, recommendations are given regarding the compilation parameters depending on the conditions of use. Namely, it is concluded that an AES-based generator is more vulnerable to side-channel attacks, from which it follows that it is not recommended to use the DILITHIUM_USE_AES flag unless there are additional guarantees to protect the machine from side-channel attacks. If the operating system's cryptographic API is trusted, it is recommended to use the DILITHIUM_RANDOMIZED_SIGNING compilation flag. In systems with low trust in the cryptographic API of the operating system, it is possible to use a variant with deterministic signature generation.

*Key words:* post-quantum cryptography; EP Crystals-Dilithium; DRNG, AES-CTR RNG, SHAKE-256, AIS 31.

1 tab. 5 fig. Ref: 13 items.

УДК 004.056.5

**Аналіз процесів генерації псевдовипадкових чисел в ЕП CRYSTALS-Dilithium /** *С.О. Кандій* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2023. Вип. 213. С. 18–30.

Наведено аналіз процесів генерації псевдовипадкових чисел в схемі постквантового електронного підпису Crystals-Dilithium, який є фіналістом конкурсу NIST PQC з постквантової криптографії. Основна увага зосереджена на генераторі псевдовипадкових чисел на основі блочного шифру AES в режимі лічильника. Для цього

генератора псевдовипадкових чисел побудована формальна модель, що відповідає вимогам останньої версії стандарту AIS 31, який містить вимоги до безпечних генераторів псевдовипадкових чисел. Показано, що генератор псевдовипадкових чисел на основі блочного шифру AES в режимі лічильника задовольняє вимогам функціонального класу DRG.3, за умови якщо початкове значення для генератора отримано з джерела дійсно випадкових чисел (як фізичного дійсно випадкового, так і нефізичного дійсно випадкового джерела) або іншого генератора псевдовипадкових чисел, що має клас безпеки не нижчий за клас DRG.3. Додатково будо проаналізовано використання shake128/256 для генерацій псевдовипадкових послідовностей у Crystals-Dilithium. За результатами аналізу були надані рекомендації щодо параметрів компіляції в залежності від умов використання. А саме, був зроблений висновок, що генератор на основі AES більш вразливий до атак по побічним каналам, звідки випливає, що не рекомендовано використовувати флаг DILITHIUM_USE_AES, якщо немає додаткових гарантій захисту машини від атак по побічним каналам. Якщо є довіра до криптографічного API операційної системи, то рекомендовано використовувати флаг компіляції DILITHIUM_RANDOMIZED_SIGNING. У системах з низькою довірою до криптографічного API операційної системи можливо використовувати варіант з детермінованим виробленням підпису.

*Ключові слова:* постквантова криптографія; ЕП Crystals-Dilithium; DRNG, AES-CTR RNG, SHAKE-256, AIS 31.

Табл. 1. Іл. 5. Бібліогр.: 13 назв.

UDC 004.056.5

**Deep learning-based models' application to generating a cryptographic key from a face image** / *A.A. Kuznetsov, D.O. Zakharov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2023. №213. P. 31–40.

Generating cryptographic keys, such as passwords or pin codes, involves utilizing specialized algorithms that rely on complex mathematical transformations. These keys necessitate secure storage measures and complex distribution and processing mechanisms, which often incur substantial costs. However, an alternative approach emerges, proposing the generation of cryptographic keys based on the user's biometric data. Since one can generate keys "on the fly," there is no longer a requirement for key storage or distribution. These generated keys, derived from biometric information, can be effectively employed for biometric authentication, offering numerous advantages. Additionally, this alternative approach unlocks new possibilities for constructing information infrastructure. By utilizing biometric keys, the initiation of cryptographic algorithms like encryption and digital signatures becomes more streamlined and less burdensome in storing and processing procedures. This paper explores biometric key generation technologies, focusing on applying deep learning models. In particular, we employ convolutional neural networks to extract significant biometric features from human face images as the foundation for subsequent key generation processes. A comprehensive analysis involves extensive experimentation with various deep-learning models. We achieve remarkable results by optimizing the algorithm's parameters, with the False Reject Rate (FRR) and False Acceptance Rate (FAR) approximately equal and less than 10%. With code-based cryptographic extractors' post-quantum level of security, we ensure the continued protection and integrity of sensitive information within the cryptographic framework.

*Key words:* deep learning models, machine learning; face recognition; cryptography; biometric authentication.

5 tabl. 5 fig. Ref: 34 items.

УДК 004.056.5

**Застосування моделей глибокого навчання для генерації криптографічного ключу із зображення обличчя** / *О.О. Кузнецов, Д.О. Захаров* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2023. Вип. 213. С. 31–40.

Генерація криптографічних ключів, таких як паролі чи пін-коди, передбачає використання спеціалізованих алгоритмів, які спираються на складні математичні перетворення. Ці ключі вимагають заходів для безпечного зберігання та складних механізмів розповсюдження та обробки, що часто потребують значних витрат. Однак з'являється альтернативний підхід, який пропонує генерацію криптографічних ключів на основі біометричних даних користувача. Оскільки ключі можна генерувати «на льоту», більше не потрібно зберігати або розповсюджувати ключі. Ці згенеровані ключі, отримані з біометричної інформації, можна ефективно використовувати для біометричної автентифікації, пропонуючи численні переваги. Крім того, цей альтернативний підхід відкриває нові можливості для побудови інформаційної інфраструктури. Завдяки використанню біометричних ключів ініціація криптографічних алгоритмів, таких як шифрування та цифрові підписи, стає більш оптимізованою та менш обтяжливою в процедурах зберігання та обробки. Ця стаття досліджує технології генерації біометричних ключів, зосереджуючись на застосуванні моделей глибокого навчання. Зокрема, ми використовуємо згорточні нейронні мережі для вилучення важливих біометричних характеристик із зображень людського обличчя як основи для подальших процесів генерації ключів. Комплексний аналіз передбачає широкі експерименти з різними моделями глибокого навчання. Ми досягаємо значних результатів, оптимізувавши параметри алгоритму, коли частка хибних відхилень (FRR) і частка хибних акцептів (FAR) приблизно однакові та менше 10 %. Завдяки постквантовому рівню безпеки криптографічних екстракторів на основі коду ми забезпечуємо постійний захист і цілісність конфіденційної інформації в криптографічній структурі.

*Ключові слова:* моделі глибокого навчання; машинне навчання; розпізнавання облич; криптографія; біометрична автентифікація.

Табл. 5. Іл. 5. Бібліогр.: 34 назв.

UDC 004.056.5

**CERT-UA assessment based on the CSIRT ENISA Maturity Model** / *O.I. Peliukh, M.V. Yesina, D.Yu. Holubnychyi* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2023. №213. P. 41–48.

Cybersecurity threats are steadily increasing in today's world, which is characterised by increased openness and integration into the global network. The proliferation of cyber incidents, including hacker attacks, confidential data leaks and information theft, is becoming an extremely pressing issue in this context. Accordingly, the eradication of these threats requires the development of effective methods of responding to cyber incidents. The central theme of this article is to consider the critical importance of assessing and improving the effectiveness of cyber incident response teams. The structure of such a team, including cybersecurity specialists, network engineers, analysts, etc., is aimed at identifying, analysing and overcoming threats in cyberspace. The key aspects of assessing such a team, like abilities, experience, communication skills and level of cooperation, are presented clearly through the prism of the updated ENISA CSIRT Maturity Model. The article uses the Computer Emergency Response Team in Ukraine (CERT-UA), a national team operating under the leadership of the State Service for Special Communications and Information Protection of Ukraine, to illustrate the methods of assessing a cyber incident response team. The assessment of the team, based on the ENISA CSIRT Maturity Model, points to key aspects that determine its effectiveness. The paper provides a clear view of the process of measuring cyber incident response teams through a systematic approach that identifies their strengths and weaknesses. The maturity analysis of the CERT-UA provides recommendations for further development of the team, which can be an important resource for academics, cybersecurity experts and government officials interested in improving the effectiveness of cyber threat response. It highlights the importance of assessing cyber incident response teams to ensure cybersecurity and information protection. Awareness of this issue contributes to continuous improvement and readiness to respond effectively to growing challenges in the modern digital environment.

*Key words:* CERT-UA; CSIRT; CSIRT ENISA maturity model; maturity assessment; incident response.

5 tabl. 1 fig. Ref: 7 items.

УДК 004.056.5

**Оцінка CERT-UA на основі Моделі зрілості CSIRT ENISA /** *О.І. Пелюх, М.В. Єсіна, Д.Ю. Голубничий* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2023. Вип. 213. С. 41–48.

У сучасному світі, який характеризується підвищеною відкритістю та інтеграцією в глобальну мережу, неухильно зростають загрози, пов'язані з кібербезпекою. Розповсюдження кіберінцидентів, що містять хакерські атаки, витоки конфіденційних даних та крадіжки інформації, стає надзвичайно актуальною проблемою в цьому контексті. Відповідно до цього викорінення цих загроз передбачає розробку ефективних методів реагування на кіберінциденти. Центральною темою статті є розгляд надзвичайної вагомості оцінки та підвищення рівня дієвості команд реагування на кіберінциденти. Структура такої команди, включаючи фахівців з кібербезпеки, мережевих інженерів, аналітиків тощо, спрямована на виявлення, аналіз та подолання загроз у кіберпросторі. Ключові аспекти оцінки такої команди, такі як здібності, досвід, комунікаційні навички та рівень співпраці, наочно представлені через призму оновленої Моделі зрілості CSIRT ENISA. Для ілюстрації методів оцінки команди реагування на кіберінциденти в статті використовується національна команда реагування на комп'ютерні надзвичайні події в Україні (CERT–UA), яка функціонує під керівництвом Державної служби спеціального зв'язку та захисту інформації України. Оцінка команди, здійснювана на основі Моделі зрілості CSIRT ENISA, вказує на ключові аспекти, що визначають її дієвість. Стаття надає чітке уявлення про процес оцінки команд реагування на кіберінциденти за допомогою систематичного підходу, що визначає їхні сильні та слабкі сторони. За допомогою дослідження зрілості CERT-UA наводяться рекомендації щодо подальшого розвитку команди, що може бути важливим ресурсом для вчених, експертів у сфері кібербезпеки та державних службовців, які мають інтерес до вдосконалення дієвості реагування на кіберзагрози. Підкреслюється значущість оцінки команд реагування на кіберінциденти з метою гарантування кібербезпеки та захисту інформації. Усвідомлення цієї проблематики сприяє постійному вдосконаленню та готовності ефективно реагувати на зростаючі виклики в сучасному цифровому середовищі.

*Ключові слова:* CERT-UA; CSIRT; модель зрілості CSIRT ENISA; оцінка зрілості; реагування на інциденти.

Табл. 5. Іл. 1. Бібліогр.: 7 назв.

UDC 621.391:519.2

**Construction of a three-parameter encryption scheme on Hermitian groups in the MST3 cryptosystem /** *Y. Kotukh, G. Khalimov, M. Korobchinsky* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2023. № 213. P. 49–55.

The article proposes a method for constructing a three-parameter encryption scheme based on Hermitian groups, which improves the security parameters of the existing MST3 cryptosystem. The challenge of improving existing approaches to building cryptosystems is driven by successes in building a quantum computer with sufficient computing power to render many public-key cryptosystems insecure. In particular, we are talking about those cryptosystems based on the complexity of factorization or the discrete logarithm problem, such as RSA, ECC, etc. There are several proposals that have become classic over the past almost 20 years for using non-commutative groups to build quantum-resistant cryptosystems The unsolvable word problem is an interesting area of research for cryptosystem construction. It was formulated by Wagner and Magyarik and lies in the plane of application of permutation groups. Logarithmic signatures (LS) were proposed by Magliveras. In this context, the logarithmic signature is a special type of factorization, it is

applied to finite groups. The latest version of this implementation is known as MST3 and is based on the Suzuki group.

In 2008, Magliveras demonstrated a transitive limit of LS for the MST3 cryptosystem. Svaba later proposed the eMST3 cryptosystem with improved security options. A secret homomorphic cover was added for this improvement. Then, in 2018, T. van Trung proposed an MST3 approach using strong aperiodic LS for abelian *p*-groups. Kong and colleagues conducted an extensive analysis of MST3 and noted that since there are no publications yet on the quantum vulnerability of the algorithm, it can be considered a candidate for the post-quantum era.

One valuable idea is to improve encryption efficiency by optimizing the computational overhead. This is done while reducing the large size of the key space. This approach can be applied to LS calculations outside the center of the group. And this was done over the final fields of the small dimensions using groups with high order.

*Key words:* MST3; cryptosystem; word problem; logarithmic signature; random cover; Hermitian function field.

Ref: 19 items..

УДК 621.391:519.2

**Побудова трьохпараметричної схеми шифрування на групах Ерміта в криптосистемі MST3** / *Є.В. Котух, Г.З. Халімов, М.В. Коробчинський* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2023. Вип. 213. С. 49–55.

Запропоновано метод побудови трьохпараметричної схеми шифрування на основі груп Ерміта, що покращує параметри безпеки існуючої криптосистеми MST3. Проблема вдосконалення існуючих підходів до побудови криптосистем зумовлена успіхами у створенні квантового комп'ютера з достатньою обчислювальною потужністю, щоб зробити багато криптосистем із відкритим ключем незахищеними. Зокрема, мова йде про криптосистеми, засновані на складності факторизації, або проблеми дискретного логарифмування, такі як RSA, ECC тощо. Існує кілька пропозицій, які стали класичними за останні майже 20 років, щодо використання некомутативних груп для створення квантово стійкої криптосистеми. Нерозв'язна проблема слова є цікавою сферою дослідження для побудови криптосистем. Вона була сформульована Вагнером і Магьяриком і лежить у площині застосування груп перестановок. Логарифмічні підписи були запропоновані Магліверасом. У цьому контексті логарифмічний підпис є особливим типом факторизації, вона застосовується до скінченних груп. Остання версія цієї реалізації відома як MST3 і базується на групі Сузукі.

У 2008 р. Magliveras продемонстрував транзитивний ліміт LS для криптосистеми MST3. Пізніше Сваба запропонував криптосистему eMST3 із покращеними параметрами захисту. Для цього вдосконалення було додано секретне гомоморфне покриття. Потім, у 2018 р., Т. ван Трунг запропонував підхід MST3 з використанням сильних аперіодичних логарифмічних підписів для абелевих *p*-груп. Конг і його колеги провели широкий аналіз MST3 і відзначили, що оскільки наразі немає публікацій про квантову вразливість алгоритму, його можна вважати кандидатом для використання в постквантову еру.

Однією з цінних ідей є підвищення ефективності шифрування шляхом оптимізації обчислювальних витрат. Це робиться при зменшенні великого розміру ключового простору. Цей підхід можна застосувати до розрахунків логарифмічних підписів поза центром групи. І це було зроблено над кінцевими полями малих розмірів з використанням груп з високим порядком.

*Ключові слова:* MST3; криптосистема; проблема слова; логарифмічна сигнатура; випадкове покриття; функціональне поле Ерміта.

Бібліогр.: 19 назв.

## PHYSICS OF DEVICES, ELEMENTS AND SYSTEMS
## ФІЗИКА ПРИЛАДІВ, ЕЛЕМЕНТІВ І СИСТЕМ

UDC 621.793:678.073

**Nanopolymer optically transparent structures, systems and devices** / *V.M. Borshchov, O.M. Listratenko, M.A. Protsenko, I.T. Tymchuk, O.V. Kravchenko, O.V. Syddia, M.I. Slipchenko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2023. №213. P. 56–64.

Search and analysis of results of theoretical and experimental studies on literature and patent sources in fields of optical and optical-electronic instrumentation are carried out. Current state and development trends of transparent polymer compositions containing nanoscale fillers, which open up new prospects for optical and optical-electronic instrumentation, are considered. Obtained data and recommendations on improvement and creation of new optically transparent nanocomposites are generalized, and can be used not only for connecting components of optical systems, but also for products in scintillation technology, lighting engineering, photovoltaics, and in many other fields of science and technology. Examples of some currently existing polymer and nanopolymer optical systems are considered, including an organosilicon composition for connecting optical elements, a plastic scintillator with nanostructured phosphors with improved time characteristics and light output values, an LED with multilayered scatterer with a variable index of refraction and an improved yield of radiation, optical compositions with a high refractive index on high transparency silicones for connection with optical elements in light-emitting devices or for lighting devices with a remote phosphor, as well as new materials and methods for dispersing nanoparticles. Given examples clearly show that complexity of the structures and micro dimensions of modern optical and optoelectronic products for their successful implementation and widespread adoption require new easy-to-use and not expensive optically transparent nanomaterials and technologies for their manufacture.

*Key words:* nanoparticles; nanomaterials; optically transparent polymer nanocomposites.
1 tab. 3 fig. Ref: 11 items.
УДК 621.793:678.073

**Нанополімерні оптично прозорі структури, системи та пристрої /** *В.М. Борщов, О.М. Лістратенко, М.А. Проценко, І.Т. Тимчук, О.В. Кравченко, О.В. Суддя, М.І. Сліпченко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2023. Вип. 213. С. 56–64.

Проведено пошук та аналіз результатів теоретичних і експериментальних досліджень за літературними і патентними джерелами в області оптичного і оптико-електронного приладобудування. Розглянуто сучасний стан і тенденції розвитку прозорих полімерних композицій, що містять нанорозмірні наповнювачі, які відкривають нові перспективи перед оптичним і оптико-електронним приладобудуванням. Узагальнено отримані дані та рекомендації щодо удосконалення та створення нових оптично прозорих нанокомпозитів, які можуть бути застосовані не тільки для з'єднання компонентів вузлів оптичних систем, але також і для виробів в сцинтиляційній техніці, світлотехніці, фотовольтаїці і в багатьох інших областях науки і техніки. Розглянуто приклади деяких існуючих полімерних і нанополімерних оптичних систем, в тому числі кремнійорганічних композицій для з'єднання оптичних елементів, пластмасового сцинтилятора з наноструктурованими люмінофорами з поліпшеними характеристиками швидкодії і значеннями світлового виходу, світлодіода з багатошаровим розсіювачем із змінним індексом заломлення і з поліпшеним виходом випромінювання, оптичних композицій з високим коефіцієнтом заломлення на силіконах високої прозорості для з'єднання з оптичними елементами в світловипромінюючих пристроях або для пристроїв освітлення з віддаленим люмінофором, а також нових матеріалів і способів диспергування наночастинок. Наведені приклади наочно показують, що складність структур і мікророзміри сучасних оптичних і оптико-електронних виробів для їх успішної реалізації та широкого впровадження вимагають нових простих у використанні і недорогих оптично прозорих наноматеріалів і технологій їх виготовлення.

*Ключові слова:* наночастинки; наноматеріали; оптично прозорі полімерні нанокомпозити.
Табл. 1. Іл. 3. Бібліогр.: 11 назв.

## INFORMATION METHODS OF RADIO ENGINEERING, SIGNAL PROCESSING
## ІНФОРМАЦІЙНІ МЕТОДИ РАДІОТЕХНІКИ, ОБРОБКА СИГНАЛІВ

UDC 004.056.5

**Electronic information resources: definition and classification** / *I.O. Myliutchenko, P.O. Kulko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2023. № 213. P. 65–69.

The article provides a review of normative documents and scientific works devoted to the concept of "electronic information resource" as an important type of information resources, caused by the influence of information technologies. The classification of electronic information resources is given, summarizing the most common features and categories and also taking into account the correspondence between the features of the classification of information resources and electronic information resources.

*Key words:* information security; electronic information resource; document; classification.
3 tab. 1 fig. Ref: 20 items.
УДК 004.056.5

**Електронні інформаційні ресурси: визначення та класифікація /** *І.О. Милютченко, П.О. Кулько* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2023. Вип. 213. С. 65–69.

Проведено огляд нормативних документів та наукових робіт, присвячених поняттю «електронний інформаційний ресурс» як важливого виду інформаційних ресурсів, зумовленого впливом інформаційних технологій. Наведено класифікацію електронних інформаційних ресурсів, яка узагальнює найбільш поширені ознаки та категорії, а також враховує відповідність ознак класифікації інформаційних ресурсів та електронних інформаційних ресурсів.

*Ключові слова:* інформаційна безпека; електронний інформаційний ресурс; документ; класифікація.
Табл. 3. Іл. 1. Бібліогр.: 20 назв.

UDC 621.396.677.494

**Estimation of requirements for signal parameters at V-shaped frequency distribution in the mathematical model of a planar phased array antenna** / *A.I. Kovalenko, S.V. Titov, E.V. Titova, O.S. Chorna* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2023. №213. P. 70–77.

A brief review provides methods of focusing electromagnetic radiation of a flat phased array antenna based on mutually consistent spatial-amplitude-phase-frequency control of the radiated signals and limitations of their potential capabilities arising from various random fluctuations of signal and antenna parameters. The performed statistical study revealed the influence of various random and deterministic changes in the electrical and structural parameters of antennas, control systems for radiated signals with a V-shaped frequency distribution over the aperture of a flat phased array on the peak power level, duration, and repetition period of focused pulses. The parameters of the law of spatial-amplitude-phase-frequency control should be stable for a time equal to the average pulse duration at the output of the

emitters when forming a single spatiotemporal pulse, and when forming a sequence of spatiotemporal pulses within duration of this packet of spatiotemporal pulses. The requirements for the accuracy and stability of parameters of the space-phase-frequency signal control law are considered. The analyses of influence of various deviations from the set values of the parameters of the law of spatial-phase-frequency control of emitted signals in the channels of a multi-position system of emitters in the formation of sequences of spatiotemporal pulses is analyzed. It is shown that the influence of errors in the location of the phase centers of the emitters in the direction of radiation does not depend on the distance to the focusing point, but is significant and requires special measures to reduce them. The influence of initial phase setting errors on the characteristics of the generated sequence of spatiotemporal pulses also does not depend on the radiation time. The range of permissible values of the maximum initial phase setting errors behind the aperture of a flat phased antenna array, in which the decrease in the power flux density value does not exceed 10%, should not exceed $\pi/3$. The discreteness and random errors in establishing the initial phases of individual radiation sources of a flat phased array equal to $\pi/3$ practically do not affect the duration and repetition period of the sequence of spatiotemporal pulses.

*Key words:* pulse; focusing; transmitter; antenna; model; system; power; frequency; deviation; accuracy.

5 fig. Ref: 15 items.

УДК 621.396.677.494

**Оцінка вимог до параметрів сигналів при V-подібному розподілі частот у математичній моделі плоскої фазованої антенної решітки** / *А.І. Коваленко, С.В. Тітов, О.В. Тітова, О.С. Чорна* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2023. Вип. 213. С. 70–77.

Проводиться короткий огляд методів фокусування електромагнітного випромінювання плоскої фазованої антенної решітки на основі взаємоузгодженого просторово-амплітудно-фазово-частотного управління випромінюваними сигналами та обмежень їх потенційних можливостей, що виникають через різні випадкові флуктуації параметрів сигналів і антен. Проводиться статистичне дослідження впливу різних випадкових та детермінованих змін електричних та конструктивних параметрів антен, систем управління випромінюваними сигналами при V-подібному розподілі частот по апертурі плоскої фазованої антенної решітки на рівень пікової потужності, тривалість та період повторення сфокусованих імпульсів. Параметри закону просторово-амплітудно-фазово-частотного управління повинні бути стабільні протягом часу, рівного усередненій тривалості імпульсів на виході випромінювачів при формуванні одиночного просторово-часового імпульсу, а при формуванні послідовності просторово-часових імпульсів – протягом тривалості цієї пачки просторово-часових імпульсів. Розглянуто вимоги до точності та стабільності параметрів закону просторово-фазово-частотного управління сигналами. Проведено аналіз впливу різноманітних відхилень від заданих значень параметрів закону просторово-фазово-частотного управління випромінюваними сигналами в каналах багатопозиційної системи випромінювачів при формуванні послідовностей просторово-часових імпульсів. Показано, що вплив помилок розташування фазових центрів випромінювачів у напрямку випромінювання не залежить від дальності до точки фокусування, але є суттєвим і потрібне вживання спеціальних заходів щодо їх зниження. Також вплив помилок установки початкових фаз на характеристики сформованої послідовності просторово-часових імпульсів не залежить від часу випромінювання. Область допустимих значень максимальних помилок встановлення початкових фаз за апертурою плоскої фазованої антенної решітки, у якій зменшення значення щільності потоку потужності не перевищує 10 % не повинна перевищувати $\pi/3$. Дискретність і випадкові помилки встановлення початкових фаз окремих джерел випромінювання плоскої фазованої антенної решітки, що дорівнюють $\pi/3$, практично не впливають на тривалість і період повторення послідовності просторово-часових імпульсів.

*Ключові слова:* імпульс; фокусування; випромінювач; антена; модель; система; потужність; частота; відхилення; точність.

Іл. 5. Бібліогр.: 15 назв.

## RADAR AND RADIONAVIGATION
## РАДІОЛОКАЦІЯ І РАДІОНАВІГАЦІЯ

UDC 621.396.96

**Comparative analysis of the quality of detection of air objects by secondary radar systems** / *I.V. Svyd* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2023. №213. P. 78–87.

The work is devoted to a comparative analysis of the quality of detection of air objects by secondary radar systems. The purpose of the work is a comparative analysis of the optimal and quasi-optimal structure for detecting air objects by secondary interrogation radar systems. A significant role in the information support of the airspace control and air traffic control system is played by secondary radar systems for airspace surveillance, which include secondary radars and identification problems on the basis of “friend or foe” identification. Note that in existing networks of radar surveillance systems, tracking of airborne objects is usually carried out using information from primary radar surveillance systems, and secondary radar surveillance systems are used as sources of additional radar information. In this regard, the problems of assessing the quality of detection of air objects by secondary radar systems, the specifics of the construction and operation of which differ significantly from the primary airspace surveillance radar systems, are relevant. Thus, increasing the probabilistic characteristics of the system of secondary radar systems when an aircraft transponder oper-

ates in the field of significant flows of intentional and intra-system interference is ensured by choosing detection thresholds depending on the values of the transponder readiness coefficient and the probability of suppression of individual response signal pulses. On the other hand, the use of detection thresholds on secondary radar systems that are optimal for the given operating conditions of the transponder makes it possible to reduce the requirements for the throughput of the aircraft transponder with a significant intensity of flows of intra-system and intentional correlated interference. Analysis of the characteristics of detection of air objects by secondary radar systems shows that: optimal thresholds for detecting air objects in secondary radar systems significantly depend on the readiness factor of the aircraft transponder and the probability of suppression of individual pulses of response signals in the response channel; the use of decoding response signals and subsequent accumulation when choosing the optimal threshold significantly reduces the detection quality indicators compared to optimal processing of a burst of response signals; the digital threshold for detecting air objects in a secondary radar system largely depends on the probability of signal suppression in the request channel and response channel.

*Key words:* radar system; airspace; surveillance system; analysis; quality; detection; secondary radar system; detection threshold; response signal; request signal.

4 fig. Ref: 42 items.

УДК 621.396.96

**Порівняльний аналіз якості виявлення повітряних об'єктів вторинними радіолокаційними системами /** *І.В. Свид* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2023. Вип. 213. С. 78–87.

Роботу присвячено порівняльному аналізу якості виявлення повітряних об'єктів вторинними радіолокаційними системами. Метою роботи є порівняльний аналіз оптимальної та квазіоптимальної структур виявлення повітряних об’єктів вторинними запитальними радіолокаційними системами. Суттєву роль в інформаційному забезпеченні системи контролю повітряного простору та управління повітряного руху відіграють вторинні радіолокаційні системи спостереження повітряного простору, до яких відносять вторинні радіолокатори та запитальні системи ідентифікації за ознакою «свій-чужий». Зазначимо, що у існуючих мережах радіолокаційних систем спостереження супровід повітряних об'єктів, як правило, здійснюється за інформацією первинних радіолокаційних систем спостереження, а вторинні радіолокаційні системи спостереження використовуються у якості джерел додаткової радіолокаційної інформації. У зв'язку з цим, актуальними є питання оцінки якості виявлення повітряних об’єктів вторинними радіолокаційними системами, специфіка побудови та функціонування яких суттєво відрізняються від первинних радіолокаційних систем спостереження повітряного простору. Таким чином, підвищення імовірнісних характеристик системи вторинних радіолокаційних систем при роботі літакового відповідача у полі значних потоків навмисних та внутрісистемних завад забезпечується вибором порогів виявлення залежно від значень коефіцієнта готовності відповідача та імовірності подавлення окремих імпульсів СВ. З іншого боку, застосування оптимальних для даних умов роботи відповідача, порогів виявлення на системах вторинних радіолокаційних систем дозволяє знизити вимоги до пропускної здатності літакового відповідача при значній інтенсивності потоків внутрісистемних та навмисних корельованих завад. Аналіз характеристик виявлення повітряних об’єктів системами вторинних радіолокаційних систем показує, що: оптимальні пороги виявлення повітряних об’єктів в системах вторинної радіолокації суттєво залежать від коефіцієнта готовності літакового відповідача та імовірності подавлення окремих імпульсів сигналів відповіді в каналі відповіді; використання декодування сигналів відповіді та подальшого накопичення при виборі оптимального порога значно знижує показники якості виявлення в порівнянні з оптимальною обробкою пачки сигналів відповіді; цифровий поріг виявлення повітряних об’єктів системою вторинної радіолокації значною мірою залежить від імовірності подавлення сигналів в каналі запиту та каналі відповіді.

*Ключові слова:* радіолокаційна система; повітряний простір; система спостереження; аналіз; якість; виявлення; вторинна радіолокаційна система; поріг виявлення; сигнал відповіді; сигнал запиту.

Іл. 4. Бібліогр.: 42 назв.

COLLECTION OF SCIENTIFIC PAPERS
**RADIOTEKHNIKA**
Issue 213
In English and Ukrainian

ЗБІРНИК НАУКОВИХ ПРАЦЬ
**РАДІОТЕХНІКА**
Випуск 213
Англійською та українською мовами

*Коректор Л.І. Сащенко*

Підп. до друку 30.06.2023. Формат 60x90/8. Папір офсет. Гарнітура Таймс. Друк. ризограф.
Ум. друк. арк**.** 10,9. Обл.-вид. арк. 8,0. Тираж 300 прим. Зам. № 547. Ціна договір.

Харківський національний університет радіоелектроніки (ХНУРЕ)
Просп. Науки, 14, Харків, 61166.

Оригінал-макет підготовлено і збірник надруковано у ПФ „Колегіум”, тел. (057) 703-53-74.
Свідоцтво про внесення суб’єкта видавничої діяльності до Державного реєстру видавців.
Сер. ДК №1722 від 23.03.2004.