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 6

Kharkiv
Kharkiv National
University of Radio Electronics
2024

UDC 621.3

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

Website: rt.nure.ua

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

The authors are responsible for the content of the article.

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 № 3 dated 20.03.2024.

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 6

Харків
Харківський національний
університет радіоелектроніки
2024

УДК 621.3

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

Сайт: rt.nure.ua

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

За зміст статті відповідальні автори.

Відповідальні за випуск: *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 № 3 від 20.03.2024.

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

CONTENT

SYSTEMS AND METHODS OF INFORMATION PROTECTION

RADIO ENGINEERING DEVICS

MEANS OF TELECOMMUNICATIONS

PHYSICS OF DEVICES, ELEMENTS AND SYSTEMS

RELATED PROBLEMS OF RADIO ENGINEERING

RADAR AND RADIO NAVIGATION

ЗМІСТ

СИСТЕМИ І МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ

РАДІОТЕХНІЧНІ ПРИСТРОЇ

ЗАСОБИ ТЕЛЕКОМУНІКАЦІЙ

ФІЗИКА ПРИЛАДІВ, ЕЛЕМЕНТІВ І СИСТЕМ

СУМІЖНІ ПРОБЛЕМИ РАДІОТЕХНІКИ

РАДІОЛОКАЦІЯ І РАДІОНАВІГАЦІЯ

SYSTEMS AND METHODS OF INFORMATION PROTECTION
СИСТЕМИ І МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ

УДК 004.056.5 **DOI:10.30837/rt.2024.1.216.01**

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

ДОСЛІДЖЕННЯ МЕТОДІВ ТА АЛГОРИТМІВ ДЛЯ ГЕНЕРАЦІЇ (ПСЕВДО)ВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ НАД ДОВІЛЬНИМ АЛФАВІТОМ

Вступ

Робота присвячена дослідженню алгоритмів для генерації (псевдо)випадкових послідовностей над довільним алфавітом, оцінці їх складності (часової та ємнісної). Це дослідження важливе в зв'язку з тим, що для сучасних постквантових алгоритмів застосовують саме такі послідовності для генерації ключів та випадкових компонентів електронного підпису та інкапсуляції ключів, наприклад [1 – 3].

1. Генерація двійкової послідовності

Для побудови генераторів, що виробляють випадкові чи псевдовипадкові послідовності над алфавітом потужності $q>1$, в роботі застосовують підхід, згідно з яким спочатку формуються двійкові випадкові чи псевдовипадкові послідовності, які задовольняють відомим статистичним характеристикам, з яких потім певним чином отримуються послідовності q-х символів.

Для генерації таких двійкових послідовностей можна застосовувати різні засоби, наприклад:

- спеціальні пристрої, наприклад серії «Гряда» [24], а також квантові генератори серії QRNG [25];
- кросплатформні засоби, основані на застосуванні команд процесора, наприклад команди *rdrand* для процесорів *Intel*, яка, в залежності від обраного режиму, генерує випадкову послідовність завдовжки 16, 32 або 64 біта;
- спеціальні функції операційних систем, наприклад для генерації випадкових даних в ОС WINDOWS, застосовують функцію криптопровайдера CryptGenRandom, в ОС LINUX – випадкові дані з заданою кількістю байтів зчитуються з пристрою /dev/random.

Для подальшої роботи були згенеровані двійкові послідовності завдовжки 13 мільйонів байтів кожним зі способів і виконано їх тестування за допомогою статистичних тестів NIST (NIST 800-22).

2. Генератори послідовностей з довільним алфавітом

2.1. Означення основних понять

Скінченним автоматом називають впорядкований набір $A=(X,S,Y,h,f)$, де X,S,Y – скінченні множини, $h: X\times S\to S$ та $f: X\times S\to Y$ – відображення. Множини X,Y та S називаються *вхідним алфавітом*, *вихідним алфавітом* та *множиною станів* (або *внутрішнім алфавітом*) автомата A. Відображення h та f називають відповідно *функцією переходів* та *функцією виходів* цього автомата. Автомат називається *автономним*, якщо функції h і f не залежать від першого аргументу. В цьому випадку множину X не згадують та вважають, що $h: S\to S$, $f: S\to Y$.

Згідно із загальновизнаним означенням, *генератором псевдовипадкових послідовностей* (*ПВП*) називають скінченний автономний автомат $A=(S,Y,h,f)$, де S та Y позначають відповідно внутрішній і вихідний алфавіти автомата A, $h: S\to S$ і $f: S\to Y$ є, відповідно,

функціями переходів і виходів цього автомата. Генератор ПВП функціонує в дискретні моменти часу або такти, виробляючи за довільним елементом $s_0 \in S$ (*початковим станом* автомата A) *внутрішню послідовність* $s_0, s_1, \ldots$, де $s_{i+1} = h(s_i)$ та *вихідну послідовність* (*гаму*) $\gamma_i = f(s_i)$, $i = 0, 1, \ldots$. Для будь-якого натурального L відображення $\Gamma_L : s_0 \mapsto \gamma_0, \gamma_1, \ldots, \gamma_{L-1}$, де $\gamma_i = f(h^i(s_0))$, $i \in \overline{0, L-1}$, $s_0 \in S$, називається *гамоутворювальним відображенням генератора* A*, обмеженим на довжині* L (див. [4]).

Генератор випадкових послідовностей визначається як дискретне джерело, що виробляє послідовність випадкових величин $\xi_1, \xi_2, \ldots$, які приймають значення у певній скінченній множині Y. Такий генератор задається набором усіх скіченновимірних розподілів ймовірностей цих випадкових величин, тобто розподілів вигляду $\{\mathbf{P}(\xi_{i_1} = a_1, \ldots, \xi_{i_k} = a_k) : a_1, \ldots, a_k \in Y\}$, де $1 \le i_1 < \ldots < i_k$, $k = 1, 2, \ldots$

Як відомо, основною вимогою до якісного генератора ПВП є псевдовипадковість. Нагадаємо формальне означення цього поняття [5 – 7].

Розглянемо таку гру між Дослідником та Криптоаналітиком.

1. Дослідник генерує випадковий рівноймовірний початковий стан $s_0 \in S$ генератора $A = (S, Y, h, f)$. Після цього він з ймовірністю $1/2$ вибирає або відрізок гами $\gamma = \gamma_0, \gamma_1, \ldots, \gamma_{L-1}$, вироблений генератором за початковим станом s_0, або випадкову рівноймовірну послідовність довжини L над алфавітом Y.

2. Дослідник передає Криптоаналітику послідовність $y = y_0, y_1, \ldots, y_{L-1}$, отриману в результаті вибору, зробленого на кроці 1.

3. Криптоаналітик, використовуючи будь-який статистичний критерій, розв'язує задачу перевірки гіпотези $H_0 : y = \gamma$; проти альтернативи $H_1 : y$ є суто випадковою послідовністю.

Нехай $T > 0$, $\varepsilon \in (0, 1/2)$. За означенням (див. [4]) генератор A називається (T, L, ε)-*псевдовипадковим*, якщо будь-який критерій для розрізнення зазначених вище гіпотез H_0 та H_1, що має середню ймовірність помилки не вище ε, використовує принаймні T (умовних) операцій (нагадаємо, що середня ймовірність помилки критерію визначається за формулою $1/2(\Pr(H_1 \mid H_0) + \Pr(H_0 \mid H_1))$, де $\Pr(H_1 \mid H_0)$ та $\Pr(H_0 \mid H_1)$ – ймовірності помилок першого та другого роду відповідно).

Іншими словами, генератор гами є (T, L, ε)-псевдовипадковим, якщо не існує способу відрізнити його вихідну послідовність довжини L, отриману при випадковому рівноймовірному початковому стані, від суто випадкової послідовності такої ж довжини над алфавітом Y з середньою ймовірністю помилки не вище ε, використовуючи менше ніж T операцій.

Аналогічно визначається поняття стійкового генератора випадкових послідовностей. Припустимо, що Криптоаналітик має доступ до оракула, який з імовірністю $1/2$ є визначеним генератором (гіпотеза H_0) та з такою ж ймовірністю є генератором випадкових рівноймовірних послідовностей над алфавітом Y (гіпотеза H_1). Тоді визначений генератор називається (T, L, ε)-*псевдовипадковим*, якщо будь-який критерій для розрізнення зазначених гіпотез, що має середню ймовірність помилки не вище ε, використовує принаймні T (умовних) операцій.

2.2. Допустимі перетворення двійкових послідовностей

Нехай Q – скінченна множина потужності $q > 1$, A – алгоритм, що переробляє деякі послідовності бітів в окремі символи над алфавітом Q. Назвемо такий алгоритм (та перетворення, яке він реалізує) *допустимим*, якщо випадкові рівноймовірні послідовності бітів перетворюються у випадкові рівноймовірні символи.

2.2.1. Алгоритм A_1 (Метод відбору[1]).

Нехай l – найменше натуральне число таке, що $q \le 2^l$, і алгоритм A_1 визначається наступним чином.

1. Згенерувати двійковий вектор довжини l.

2. Якщо ціле число, двійковим записом якого є згенерований вектор, менше за q, повернути це число як результат і завершити роботу. Інакше – повернутися до кроку 1.

Твердження 1. Алгоритм A_1 є допустимим.

Доведення. Нехай $x = x_1, x_2, \ldots$ – послідовність незалежних випадкових рівноймовірних двійкових векторів довжини l, $y = \mathrm{A}_1(x)$ – випадковий символ, що формується за нею з використанням алгоритму A_1. Для будь-якого $i \in \overline{0, q-1}$ позначимо U_i подію, яка полягає в тому, що $y = i$. Ця подія відбувається тоді й тільки тоді, коли існує невід'ємне ціле число k таке, що послідовність двійкових чисел, з якої отримується символ y, має вигляд $\tilde{x}_1, \ldots, \tilde{x}_k, y$, де $\tilde{x}_1, \ldots, \tilde{x}_k \ge q$. Отже,

$$\mathbf{P}\{U_i\} = 2^{-l} \sum_{k=0}^{\infty} (1 - 2^{-l} q)^k = 2^{-l} \frac{1}{1 - (1 - q2^{-l})} = q^{-1},$$

що й треба було довести.

Зауважимо, що середнє число бітів (випадкової рівноймовірної) вхідної послідовності, потрібних для отримання одного q-го символу за допомогою алгоритму A_1, дорівнює

$$lq2^{-l} \sum_{k=0}^{\infty} (k+1)(1 - 2^{-l} q)^k = 2^l lq^{-1} < 2l = 2\lceil \log q \rceil.$$

2.2.2. Алгоритм A_2. (Метод швидкої гральної кістки [8]).

Наступний алгоритм A_2 вдосконалює попередній та надає змогу зменшити кількість бітів, потрібних для формування одного q-го символу.

1. Покласти $v = 1$, $c = 0$.

2. Виконувати у циклі такі обчислення:

– згенерувати випадковий рівноймовірний біт b та покласти $v = 2v$; $c = 2c + b$;

– якщо $q \le c < v$, покласти $v = v - q$, $c = c - q$;

– якщо $c < q \le v$, повернути значення c як результат і завершити роботу.

Отже, наведений алгоритм знаходить за послідовністю незалежних випадкових рівноймовірних бітів q-й символ c, який формується в циклі при першому виконанні умови $c < q \le v$.

В [8] доведено таке твердження.

Твердження 2. Алгоритм A_2 є допустимим. При цьому для будь-якого $\alpha > 0$ середнє число бітів, потрібних для формування одного q-го символу за допомогою цього алгоритму, асимптотично дорівнює

$$\log q + \frac{1}{2} + \frac{1 - \gamma}{\ln 2} + F(\log q) + O(q^{-\alpha}),\ q \to \infty,$$

де $\gamma = 0{,}5772\ldots$ – константа Ойлера, F – певний періодичний тригонометричній поліном.

З практичного погляду становлять інтерес такі алгоритми, що не є допустимими, але перетворюють випадкові рівноймовірні послідовності бітів у символи, розподіл яких є близьким до рівномірного на множині Q.

Для будь-якого $\varepsilon \in (0, 1)$ назвемо алгоритм A *ε-допустимим*, якщо для випадкової рівноймовірної двійкової послідовності x символ $y = \mathrm{A}(x)$ задовольняє умову

[1] Застосовують в алгоритмах [1 – 3]

$$|\mathbf{P}(y=i)-q^{-1}|\le\varepsilon,\ i\in\overline{0,q-1}. \quad (1)$$

2.2.3. Алгоритм A_3. (Метод *Уокера* [9, с. 144]).

Розглянемо алгоритм A_3, що визначається наступним чином:

1. Згенерувати вектор $x\in\{0,1\}^l$.

2. Обчислити $y=\lfloor 2^{-l}q\hat{x}\rfloor$, де $\hat{x}$ – ціле число з двійковим записом x.

Твердження 3. Алгоритм A_3 є 2^{-l}-допустимим.

Доведення. Для кожного $i\in\overline{0,q-1}$ мають місце такі співвідношення:

$$\lfloor 2^{-l}q\hat{x}\rfloor=i\Leftrightarrow 2^l qi\le\hat{x}<2^l q(i+1)\Leftrightarrow\lceil 2^l qi\rceil\le\hat{x}<\lceil 2^l q(i+1)\rceil.$$

Отже, якщо $\hat{x}$ є випадковим числом з рівномірним розподілом на множині $\{0,1,...,q-1\}$, то

$$\mathbf{P}(y=i)=2^{-l}\left(\lceil 2^l q(i+1)\rceil-\lceil 2^l qi\rceil\right)=q^{-1}+2^{-l}\theta,$$

де $|\theta|<1$, що й треба було довести.

У зв'язку з твердженням 3 є важливим питання про вибір параметра l або, іншими словами, про те, наскільки малим повинно бути значення ε у формулі (1) для того, щоб вважати розподіл символу $y=\mathrm{A}_3(x)$ "практично рівномірним".

Природна відповідь на це питання полягає в тому, що розподіл ймовірностей на скінченній множині є "практично рівномірним", якщо його неможливо надійно відрізнити від суто рівномірного за допомогою оптимального (байєсівського) критерію, маючи вибірку з цього розподілу певного обмеженого обсягу.

Наступне твердження є наслідком теореми 3 в [10].

Твердження 4. Найменший обсяг вибірки, необхідний для розрізнення із середньою ймовірністю помилки $\delta\in(0,1/2)$ розподілу ймовірностей $P=(P(x):x\in Q)$ на скінченній множині Q потужності $q>1$ та рівномірного розподілу на цій множині, становить

$$t\ge\frac{2(1-h(\delta))\ln 2}{\Delta(P)},$$

де $h(\delta)=-\delta\ln\delta-(1-\delta)\ln(1-\delta)$, $\Delta(P)=q^{-1}\sum_{x\in Q}(qP(x)-1)^2$.

Наслідок. Найменший обсяг вибірки, необхідний для розрізнення 2^{-l}-допустимого та рівномірного розподілів ймовірностей на множині з q елементів, становить не менше ніж $\frac{2(1-h(\delta))\ln 2}{q^2 2^{-2l}}$, тобто є величиною порядку $2^{2l}q^{-2}$.

Зокрема, якщо довжина вихідної послідовності генератора, до якої має доступ криптоаналітик, не перевищує 2^{64} q-х символів, то метод Уокера можна використовувати на практиці при $l=32+\lceil\log q\rceil$.

3. Обґрунтування криптографічних властивостей генераторів над довільним алфавітом, що будуються за допомогою допустимих перетворень

Розглянемо генератор Γ_{A} (псевдо)випадкових послідовностей над алфавітом Q, який визначається за генератором двійкових послідовностей Γ та допустимим алгоритмом A таким чином: якщо $x=x_1,x_2,...$ – вихідна послідовність генератора Γ, то $y=\mathrm{A}(x)$ є вихідною послідовністю генератора Γ_{A} (тут и далі $\mathrm{A}(x)$ позначає послідовність, члени якої отри-

муються шляхом послідовного застосування алгоритму A до відповідних відрізків послідовності x, які не перетинаються).

Твердження 5. Якщо Γ є (T, L, ε)-псевдовипадковим генератором, то Γ_{A} є $(T-t, L', \varepsilon)$-псевдовипадковим, де L' – мінімальна довжина усіх скінченних послідовностей $y = \mathrm{A}(x)$, що отримуються з двійкових послідовностей x довжини L, t – максимальна часова складність обчислення таких послідовностей y за допомогою алгоритму A.

Доведення. Припустимо, що існує критерій D, якій відрізняє вихідну послідовність довжини L' генератора Γ_{A} із середньою ймовірністю помилки не вище ніж ε, використовуючи не більше ніж $T-t$ операцій. Побудуємо критерій $\tilde{D}$, який розв'язує аналогічну задачу для генератора Γ.

Нехай x – двійкова послідовність довжини L, що є або вихідною послідовністю генератора Γ (гіпотеза H_0) або суто випадковою (гіпотеза H_1). Тоді критерій $\tilde{D}$ полягає в обчисленні послідовності $y = \mathrm{A}(x)$ (довжини не менше за L') та застосуванні до неї критерію D. Якщо D приймає висновок про справжність гіпотези H_ν, то такий саме висновок приймає і критерій $\tilde{D}$, $\nu = 1, 2$. Зрозуміло, що $\tilde{D}$ виконує не більше ніж $(T-t)+t = T$ операцій.

Оцінимо середню ймовірність помилки цього критерію.

Нехай справджується гіпотеза H_0 і $\tilde{D}$ припускається помилки. Тоді припускається помилки критерій D, приймаючи послідовність $y = \mathrm{A}(x)$ за суто випадкову. Отже, $\Pr_{\tilde{D}}(H_1 \mid H_0) \le \Pr_D(H_1 \mid H_0)$, тобто ймовірність помилки першого роду критерію $\tilde{D}$ не перевищує ймовірність помилки першого роду критерію D.

Нехай зараз справджується гіпотеза H_1 і $\tilde{D}$ припускається помилки. Тоді послідовність x є суто випадковою, а критерій D оголошує не суто випадковою послідовність, яка обчислюється за x з використанням алгоритму A. Але тоді внаслідок допустимості алгоритму A критерій D припускається помилки. Отже, $\Pr_{\tilde{D}}(H_0 \mid H_1) \le \Pr_D(H_0 \mid H_1)$, тобто ймовірність помилки другого роду критерію $\tilde{D}$ не перевищує ймовірність помилки другого роду критерію D.

Таким чином, на підставі наведених міркувань середня ймовірність помилки критерію $\tilde{D}$ не перевищує ε, що однак суперечить припущенню про (T, L, ε)-псевдовипадковість генератора Γ.

Твердження доведено.

Отримане твердження свідчить про те, що генератор Γ_{A}, отриманий з вхідного генератора Γ за допомогою допустимого алгоритму A, є не гірше за Γ.

4. Експериментальне дослідження алгоритмів $\mathbf{A_1}$, $\mathbf{A_2}$, $\mathbf{A_3}$

Алгоритми відрізняються кількістю бітів (розміром двійкової послідовності), яка може бути постійною для заданого алфавіту або залежати від конкретних бітів послідовності.

Для забезпечення отримання рівноймовірних символів алгоритми можуть виключати застосовування деяких послідовностей, коректувати їх довжину

Реалізації алгоритмів передбачають отримання послідовності зі значеннями в інтервалі [0..q-1], де q – параметр алгоритму, визначає потужність алфавіту. Алгоритми легко перетворити в алгоритми генерації вектору з елементами в діапазоні $\left[-\frac{q}{2}..\frac{q}{2}\right]$, якщо від кожного елементу вектору відняти значення $\frac{q}{2}$, або навпаки, значення $\frac{q}{2}$ віднімати від елементу.

4.1. Алгоритм A_1. (*Метод відбору*)

Нехай l – найменше натуральне число таке, що $q \le 2^l$, і алгоритм A_1 визначається наступним чином. Довжина двійкової послідовності для генерації одного значення завжди дорівнює l, але, якщо ціле число, двійковим записом якого є ця послідовність, не менше ніж q, то послідовність не застосовується.

Алгоритм генерації заданої кількості чисел для довільного алфавіту:

Вхід

q – визначає потужність алфавіту, зазвичай, $q \neq 2^k$
n – кількість чисел, які треба сформувати
Вихід
R – вектор, який складається з n чисел, значення яких в діапазоні [0..q – 1].
1 Визначення значення $l = \lceil log_2 q \rceil$, $m = 2 * l$
2 Цикл для формування компонентів вектору
j := 0 Номер елементу вектору
parts := 0 Кількість порції завдовжки l в наявній бітовій послідовності
k:= 0 Номер поточної порції
while j < n do
if k = parts then Бітової послідовності не було або вона вичерпана
$bytes = \left\lceil \frac{m*(n-j)}{8l} \right\rceil * l$
b := create_b(bytes)
k:= 0 Номер поточної порції
$parts = \frac{bytes*8}{l}$ *Кількість порцій завдовжки l*
end if
*part:= subst(b, k*l, l)* *Виділення наступної порції*
value:= number (part) *Формування значення для part*
if value < q then *Значення підходить?*
R[j]:=value;
j:=j + 1
end if
k:=k + 1
end while

Для оптимізації алгоритму в разі, коли значення l фіксоване, крок 1 алгоритму можна не виконувати, а задати значення l як константу.

Для зменшення розміру необхідної бітової послідовності можна враховувати імовірність «не відхилення» значення, тоді m обчислюється за формулою: $m = \left\lceil \frac{2^l}{q} \right\rceil$. Експериментальні результати (див. п. 4.4), отримані з урахуванням цього кроку.

Для оптимізації кроку виділення бітів послідовності замість виділення окремих бітів виділяється уся порція, в якості розміру порції вибирають число, кратне розміру байту або напівбайту, а потім зайві біти, які відповідають старшим розрядам числа, якщо вони є, встановлюють в 0. Такий прийом застосовують в алгоритмах 1, 3.

4.2. Алгоритм A_2. (*Метод швидкої грального кістки)*

Згідно цьому методу для числа обирається змінна кількість бітів від $\lceil log_2 q \rceil$. Середня кількість бітів дорівнює приблизно $\lceil log_2 q \rceil + 1$.

Вхід

q – визначає потужність алфавіту, зазвичай, $q \neq 2^k$
n – кількість чисел, які треба сформувати
Вихід
R – вектор, який складається з n чисел, значення яких в діапазоні [0..q – 1].
1 Визначення значення $l = \lceil log_2 q \rceil$, $m = l + 1$
2 Поточна кількість сформованих бітів len_bit = 0
3 Поточна номер біту k = 0
4 Цикл для формування компонентів вектору
j := 0 Номер елементу вектору

```
while j < n do
        v = 1, c = 0;                   Ініціалізація змінних
        Цикл генерації поточного елементу вектору
        R[j] = q;
        while (R[j] >=q)
                Генерація послідовності, якщо вона не була сформована або вичерпана
                        if   len_bit = k then
                                 len_bit = (m * (n – j) + 7) / 8 * 8;  Бітів
                                len_byte = len_bit / 8;                          Байтів
                                b := create_b(bytes)
                                k:= 0     Номер поточного біту послідовності
                        end if
                        v = 2 * v;
                        c = 2 * c + GET_BIT(b, k);
                        ++k;
                        if v >= q then
                                if c < q then        Знайшли значення
                                        R[j] = c;
                                else
                                        v -= q;
                                        c -= q;
                                end if
                        end if
                end while
                j:=j + 1
        end while
        part:= subst(b, k*l, l)      Виділення наступної порції
        value:= number (part)     Формування значення для part
        if value < q then             Значення підходить?
                R[j]:=value;
                j:=j + 1
        end if
        k:=k + 1
end while
```

4.3. Алгоритм A_3. (*Метод Уокера*)

Цей метод передбачає застосування бітової послідовності фіксованої довжини l, для відповідного числа обчислюється значення компоненту вектору за формулою

$$R\,[i] = \frac{q*Number\,(b)}{2^l}, \qquad (2)$$

де b – бітова послідовність завдовжки l бітів , а $Number\,(b)$ – відповідне ціле число.

Значення l обирається за формулою $l = \lceil log_2 q \rceil + 16$.

Вхід

q – визначає потужність алфавіту, зазвичай, $q \neq 2^k$

n – кількість чисел, які треба сформувати

Вихід

R – вектор, який складається з n чисел, значення яких в діапазоні [0..q – 1].

1 Визначення значення $l = \lceil log_2 q \rceil + 16$

2 Генерація бітової послідовності b завдовжки l * n

$$bytes = \left\lceil \frac{n * l}{8} \right\rceil$$

```
        b := create_b(bytes)
```

3 Цикл для формування компонентів вектору

```
j := 0                          Номер елементу вектору
k:= 0                           Номер поточної порції
while j < n do
        part:= subst(b, k*l, l)          Виділення наступної порції
        value:= number (part)     Формування значення для part
```

$R\,[i] = \frac{q*value}{2^l}$

```
        j:=j + 1
end while
```

4.4. Часові та просторові характеристики алгоритмів

Експериментальне дослідження виконувалося для q = 3329 [1] та q = 8380417 [2, 3], які застосовуються для генерації відкритих параметрів та для q = 5, 9 [2, 3] для генерації особистих ключів. Для кожного значення q для трьох алгоритмів формувалося n = 100000 чисел. Отримані числові послідовності тестувалися відповідно до статистичних алгоритмів. Усі тести пройдено.

Вимірювався час генерації послідовності (часові характеристики) та кількість потрібних байтів двійкової послідовності. Для збільшення точності виміру залежності часу від алгоритму для усіх алгоритмів двійкова послідовність генерувалася завчасно і час її генерації не враховувався.

Для першого та третього алгоритму розглянуто два варіанти.

1. Виділення окремих бітів ланцюжка;

2. Виділення цілого ланцюжка

Далі розглянуто окремо результати для генерації відкритих даних, для яких суттєвим є не тільки час генерації, але і обсяг потрібних даних, а потім для генерації приватних даних, для яких найбільш суттєвим є незалежність часу генерації

4.4.1. Результати для генерації відкритих даних.

Результати виміру для варіанту 1 представлені в табл. 1, а для варіанту 2 – в табл. 2. В табл. 2 наведено також результати для Алгоритму A_2 для полегшення порівняння.

Таблиця 1

Генерація відкритих даних: Варіант 1

Алгоритм	Bytes	Tacts	bytes	Tacts
	q = 3329		q = 8380417	
Алгоритм A_1	187500	22829550	300012	36210220
Алгоритм A_2	162500	4894893	300000	6340177
Алгоритм A_3 (l = 16)	350000	42039398	300000	57110407

Таблиця 2

Генерація відкритих даних: Варіант 2

Алгоритм	Bytes	Tacts	Bytes	Tacts
	q = 3329		q = 8380417	
Алгоритм A_1	187500	586519	495742	139929
Алгоритм A_2	162500	4894893	300000	6340177
Алгоритм A_3 (l = 16)	350000	124457	400000	104412

Для кожного значення q в таблиці перша колонка задає кількість байтів в двійковій послідовності, а колонка 2 – кількість тактів для генерування цієї послідовності та перетворення її в відповідну послідовність з заданим алгоритмом.

Для варіанту 1, в якому перетворення виконується побітно, і за часом, і за довжиною послідовності, кращім є Алгоритм A_2.

Для варіанту 2, в якому виділення виконується порціями, а також розмір порції може збільшуватись для більш ефективного виділення, для алгоритмів 1 та 3 отримали суттєве покращення не менше ніж в 39 разів. Для обох значень q = 3329 та q = 8380417 найбільш ефективним є алгоритм 3. Алгоритм A_3 є найкращим і з боку константного часу, тому що не треба відбирати дані.

Необхідно замітити, що автори алгоритмів [1 – 3] застосовували варіант 2, але Алгоритм A_1, а не Алгоритм A_3.

4.4.2. Результати для генерації приватних даних.

Далі наведено результати на прикладі параметрів для генерації векторів s1, s2 для алгоритмів [2, 3]. В експериментах застосовувались:

Алгоритм A_1 для варіанту 2, саме такий метод застосовували автори відповідних стандартів;

Алгоритм A_3 для варіанту 2, саме такий метод забезпечує незалежність часу генерації від конкретної послідовності, що є особливо важливо для компонентів приватних ключів. Для алгоритму 3 застосовують значення l = 16 та l = 32.

Як і в попередніх експериментах генерується послідовність розміром 10000 елементів. Результати наведені в табл. 3.

Таблиця 3

Генерація приватних даних: Варіант 2

Алгоритм	Bytes	Tacts	Bytes	Tacts
	q = 15 (η = 2)		q = 9 (η = 4)	
Алгоритм A_1	79988	5082205	87500	4120856
Алгоритм A_3, l = 16	250000	368615	250000	368320
Алгоритм A_3, l = 32	450000	365166	450000	342589

Алгоритм A_1 потребує суттєво більшого часу, ніж Алгоритм 3 але вимагає послідовність значно меншого розміру, тобто більшого часу для її генерації, але цей алгоритм не забезпечує константність часу.

Значення l не впливає на розмір послідовності і практично не впливає на час генерації.

Р е к о м е н д а ц і я . Для генерації приватних даних застосовувати Алгоритм 3 замість алгоритму 1 при l = *32*.

5. Статистичне тестування послідовностей з довільним алфавітом

5.1. Методи тестування

Нехай задано алфавіт $\Sigma = \{\sigma_0, ..., \sigma_{k-1}\}$ і деяку послідовність $\gamma = \gamma_0, ..., \gamma_{n-1}$, де $\gamma_i \in \Sigma$. Тести призначені для перевірки гіпотези про рівномірний розподіл послідовності γ. Без втрати загальності надалі будемо вважати, що $\Sigma = \{0,1,...,\mathrm{k}-1\}$ для деякого k. Математичне очікування для рівномірного розподілу над Σ визначено як $\mu(\Sigma) = (k-1)/2$. Середньоквадратичне відхилення для рівномірного розподілу над Σ визначена як $\sigma(\Sigma) = \sqrt{(k^2-1)/12}$.

5.1.1. Монобітний тест.

Вхідні дані: послідовність $\gamma = \gamma_0, ..., \gamma_{n-1}$ з алфавіту $\Sigma = \{0,1,...,\mathrm{k}-1\}$, рівень значимості α.

Вихідні дані: 1, якщо послідовність має рівномірний розподіл, 0 інакше.

Алгоритм:

Крок 1: Обчислити $\mu(\Sigma) = (k-1)/2$ та $\sigma^2(\Sigma) = (k^2-1)/12$.

Крок 2: Обчислити $S_n = \sum_{i=0}^{n-1} \gamma_i$.

Крок 3: Обчислити $s_{obs} = \dfrac{|S_n - \mu(\Sigma)n|}{\sigma(\Sigma)\sqrt{n}}$.

Крок 4: Обчислити P-значення $p = erfc\left(\dfrac{s_{osb}}{\sqrt{2}}\right)$.

Крок 5: Повернути 1, якщо $p > \alpha$, інакше повернути 0.

Тест було реалізовано на мові програмування C++, код алгоритму монобітного тесту надано у лістингу 1:

```
double monobitTest(vector<int> seq, int q, double alpha) {
    cout << "\nMonobit testing in progress...\n";
    double mu = (q – 1) / 2;
    double sigma = (pow(q, 2) – 1) / 12;
    uint64_t sumSeq = 0;
    ofstream myfile, myFile2;
    myfile.open("HRNGIDQRandomSeq2_toQ.txt");
    for (int i = 0; i < seq.size(); i++) {
        sumSeq += seq[i];
        myfile << seq[i] << "\n";
    }
    myfile.close();
    double obsSeq = (fabs((sumSeq)-(mu * seq.size()))) / (sqrt(sigma) * sqrt(seq.size()));
    double beforeERFC = obsSeq / (sqrt(2));
    double p = erfc(beforeERFC);
    cout << "\n" << "p = " << p;
    return p;
}
```

Лістинг 1 – Код алгоритму монобітного тесту

5.1.2. Критерій узгодженості Колмогорова – Смирнова та Хі-квадрат.

Для статистичного тестування рівномірності розподілу у різних джерелах пропонується використовувати критерій узгодженості Колмогорова – Смирнова [11] чи критерій Хі-квадрат [12].

У NIST Engineering Statistics Book [13] зазначено, що хоча K-S тест зазвичай розробляється в контексті неперервних розподілів для нецензурованих і незгрупованих даних, його було поширено на дискретні розподіли, а також на цензуровані та згруповані дані. Приклад адаптації тесту на дискретні розподіли надано у роботі [14]. Там пропонується модернізована реалізація функції stats::ks.test() для мови програмування R [15]. Пакет містить запропоновану нову функцію ks.test(). Він не змінює існуючу поведінку ks.test(), за одним незначним винятком – додає можливості, необхідні для виконання тестів з гіпотетичними дискретними розподілами.

Для використання модернізованої версії функції необхідно підключити пакет, виконавши у коді команду: install.packages("ks.test", repos="http://R-Forge.R-project.org").

Для перевірки послідовностей довільного алфавіту з використанням критерію Колмогорова – Смирнова було вирішено зробити декілька тестів:

- перший: подібний до того, який показано у [14], тобто однозразковий тест Колмогорова – Смирнова;
- другий [16]: двозразковий тест, який перевіряє, чи походять два набори даних з одного розподілу.

У першому випадку на вхід тесту подається числовий вектор, який містить значення вибірки з одного з розподілів, та символьний рядок, який визначає функцію, що генерує p-значення для гіпотетичного розподілу, яка може бути однією з pnorm, pbeta, pcauchy, pchisq, pexp, pf, pgamma, plnorm, plogis, pt, punif, pweibull, pbinom, pgeom, phyper, pnbinom, ppois, pwilcox. Також можливим є явне задання розподілу, наприклад, для рівномірного дискретного розподілу в межах значень 0-14, параметр, який передаватиметься у функцію, матиме вигляд: ecdf(0:14).

У другому випадку на вхід подаються два числових вектори, для яких треба перевірити факт походження з одного розподілу.

Для того щоб перевірити, чи належать послідовності за заданим алфавітом рівномірному розподілу, генерується випадковий набір даних з дискретного рівномірного розподілу, що відповідає алфавіту послідовності з використанням функції rdunif з бібліотеки purrr [17]. Генерація відбувається наступним чином:

x <- rdunif(25557884, 0, 14).

У прикладі генерується набір з 25557884 чисел в межах 0-14, які відповідають рівномірному дискретному розподілу.

Для визначення успішності проходження тесту даними застосовується критичне значення для D [13] ($\max(D^+, D^-)$), де D^+ – статистика проходження тесту для alternative = "g", а D^- – статистика проходження тесту для alternative = "l". Критичне значення для D обчислюється за наступною формулою [18]:

$$D = \frac{\text{Константне значення для обраного } \alpha}{\sqrt{n}}$$

де n – довжина вибірки(вибірок), що перевіряється, а константне значення для вибірок понад 50 значень для різних рівнів значущості надається у [19]. У табл. 4 показано критичне значення для D для обраних рівнів значущості.

Таблиця 4

Критичні значення для D для різних рівнів значущості

Рівень значущості	Формула обчислення критичного значення
$\alpha = 0.01$	$\frac{1.62762}{\sqrt{n}}$
$\alpha = 0.05$	$\frac{1.35810}{\sqrt{n}}$
$\alpha = 0.1$	$\frac{1.22385}{\sqrt{n}}$

У якості альтернативи NIST пропонує використовувати тест хі-квадрат [20]. Тест хі-квадрат є альтернативою тестам Андерсона – Дарлінга та Колмогорова – Смірнова. Основною перевагою такого тесту в нашому випадку є те, що тест хі-квадрат може бути застосований до дискретних розподілів, а отже підійде для тестування послідовності довільного алфавіту.

Тест хі-квадрат визначено для перевірки гіпотез:

H_0: дані підпорядковуються заданому розподілу.

H_a: дані не відповідають вказаному розподілу.

Статистика тесту: для обчислення критерію хі-квадрат дані розбиваються на k груп, а тестова статистика визначається як

$$\chi^2 = \sum_{i=1}^{k} (O_i - E_i)^2 / E_i ,$$

де O_i – спостережувана частота для групи i, а E_i – очікувана частота для групи i.

Тестова статистика приблизно відповідає розподілу хі-квадрат з $(k-c)$ ступенями свободи, де k – кількість непорожніх груп, а c – кількість оцінюваних параметрів для розподілу + 1. Для рівномірного розподілу $c = 1$. Тобто, кількість ступенів свободи для рівномірного розподілу буде визначатися за формулою

$$df = k - 1$$

Отже, гіпотеза про те, що дані походять з генеральної сукупності із зазначеним розподілом, відхиляється, якщо $\chi^2 > \chi^2_{1-\alpha,k-c}$, де $\chi^2_{1-\alpha,k-c}$ – критичне значення критерію хі-квадрат з $(k-c)$ ступенями свободи і рівнем значущості α.

Для проведення статистичного тестування з використанням хі-квадрат було обрано двосторонній тест, який передбачає наступну реалізацію [21]:

- Для двостороннього тесту знайдіть стовпчик, що відповідає $1-\frac{\alpha}{2}$ у таблиці критичних значень верхньої межі, і відхиліть нульову гіпотезу, якщо тестова статистика більша за наведене в таблиці значення. Аналогічно, знайдіть у таблиці стовпчик, що відповідає $\frac{\alpha}{2}$, для нижніх критичних значень і відхиліть нульову гіпотезу, якщо тестова статистика менша за наведене в таблиці значення.

У табл. 5 наведено критичні значення нижньої та верхньої межі для обраних ступенів свободи – 14 та 2022 – та обраних рівнів значущості. Значення для ступенів свободи 2022 пораховані з використанням онлайн калькулятора – Critical Chi-Square Value Calculator [22] – оскільки таблиці, які присутні на сайті NIST, містять детальні дані тільки для ступенів свободи до 100 і стислі для ступенів до 1000.

Таблиця 5

Критичні значення розподілу хі-квадрат
для заданих ступенів свободи та рівнів значущості

Ступені свободи	Рівень значущості	Критичні значення (нижня межа – верхня межа)
14	0.1	6.571 – 23.685
	0.05	5.629 – 26.119
	0.01	4.074 – 31.319
2022	0.1	1918.549 – 2127.724
	0.05	1899.266 – 2148.522
	0.01	1861.954 – 2189.557

Далі буде виконане статистичне тестування з використанням наведених критичних значень для послідовностей довільного алфавіту, отриманих з використанням методів, описаних раніше з двійкових послідовностей генератора /dev/random. Буде наведено отримане значення хі-квадрат, а також зроблено висновок про рівномірність розподілу послідовності на основі отриманого значення.

Тест було реалізовано на мові програмування C++, код алгоритму тесту хі-квадрат надано у лістингу 2:

```
double chiSquareTest(vector<int> seq, int q) {
   cout << "\nChi-square testing in progress...\n";
   int* values = new int[q];
   for (int k = 0; k < q; k++) {
      values[k] = 0;
   }
   for (int i = 0; i < seq.size(); i++) {
      values[seq[i]]++;
   }
   double e_i = (double)seq.size() / BASE;
   double part = 0.0;
   double chi = 0.0;
   for (int k = 0; k < q; k++) {
      part = 0.0;
      part = pow((double)values[k] – e_i, 2) / e_i;
      chi += part;
   }
   cout << "\nchi = " << fixed << setprecision(3) << chi;
   return chi;
}
```

Лістинг 2 – Код алгоритму тесту хі-квадрат

Тестування з використанням критерію Колмогорова – Смирнова проводилося мовою програмування R з використанням IDE PyCharm 2023.3.3 [23]. Графіки розподілів послідовностей створено вбудованими засобами IDE.

5.2. Результати тестування

Результати тестування наводяться для значень $q = 15$ та $q = 2023$.

5.2.1. Дослідження послідовностей, отриманих методом відбору.

Послідовності до взяття за основою проходять статистичне тестування, а отже мають проходити тестування і при взятті за обраною основою. Отримані результати підтверджують це припущення.

5.2.1.1. Послідовність за основою 15.

- Дослідження з використанням монобітного тесту.

Таблиця 6

Результати тестування для dev_random_Seq_C1 за основою 15

Розмір вибірки після представлення за основою	239000000
p-значення	0.359225
$\alpha = 0.1$	Тестування пройдено успішно
$\alpha = 0.05$	Тестування пройдено успішно
$\alpha = 0.01$	Тестування пройдено успішно

Отже, як видно з отриманих результатів, послідовність за обраною основою успішно проходить статистичний тест.

- Дослідження з використанням тесту хі-квадрат

Таблиця 7

Результати тестування хі-квадрат для dev_random_Seq_C1 за основою 15

Значення хі-квадрат	16.259	
$\alpha = 0.1$	6.571 < <u>16.259</u> < 23.685	Тестування пройдено успішно
$\alpha = 0.05$	5.629 < <u>16.259</u> < 26.119	Тестування пройдено успішно
$\alpha = 0.01$	4.074 < <u>16.259</u> < 31.319	Тестування пройдено успішно

Послідовність успішно проходить тест хі-квадрат, що підтверджує дані минулих статистичних тестів.

- Дослідження з використанням критерію Колмогорова – Смирнова.

Однозразковий тест.

Таблиця 8

Результати однозразкового тесту Колмогорова-Смирнова для dev_random_Seq_C1

Довжина послідовності, що тестується (n)	23900000
D^+	0.000033529
D^-	0.00014358
D	0.00014358
Критичне значення для $\alpha = 0.01$	$Crit_{0.01} = \frac{1.62762}{\sqrt{n}} = 0.0003329$
Критичне значення для $\alpha = 0.05$	$Crit_{0.05} = \frac{1.35810}{\sqrt{n}} = 0.0002778$
Критичне значення для $\alpha = 0.1$	$Crit_{0.1} \frac{1.22385}{\sqrt{n}} = 0.0002503$
Оскільки $D < (Crit_{0.01}, Crit_{0.05}, Crit_{0.1})$ – послідовності походять з одного розподілу	

Однозразковий тест для послідовності за основою 15 показує, що послідовність походить з рівномірного дискретного розподілу для меж 0:14, а отже послідовність є рівномірною.

Двозразковий тест.

Таблиця 9

Результати двозразкового тесту Колмогорова – Смирнова
для dev_random_Seq_C1

Довжина послідовності, що тестується (n)	23900000
D^+	0.00024615
D^-	0.000060167
D	0.00024615
Критичне значення для $\alpha = 0.01$	$Crit_{0.01} = \frac{1.62762}{\sqrt{n}} = 0.0003329$
Критичне значення для $\alpha = 0.05$	$Crit_{0.05} = \frac{1.35810}{\sqrt{n}} = 0.0002778$
Критичне значення для $\alpha = 0.1$	$Crit_{0.1} \frac{1.22385}{\sqrt{n}} = 0.0002503$
Оскільки $D < (Crit_{0.01}, Crit_{0.05}, Crit_{0.1})$ – послідовності походять з одного розподілу	

Двозразковий тест також показує рівномірність послідовності за основою 15, що можна спостерігати на рис. 1.

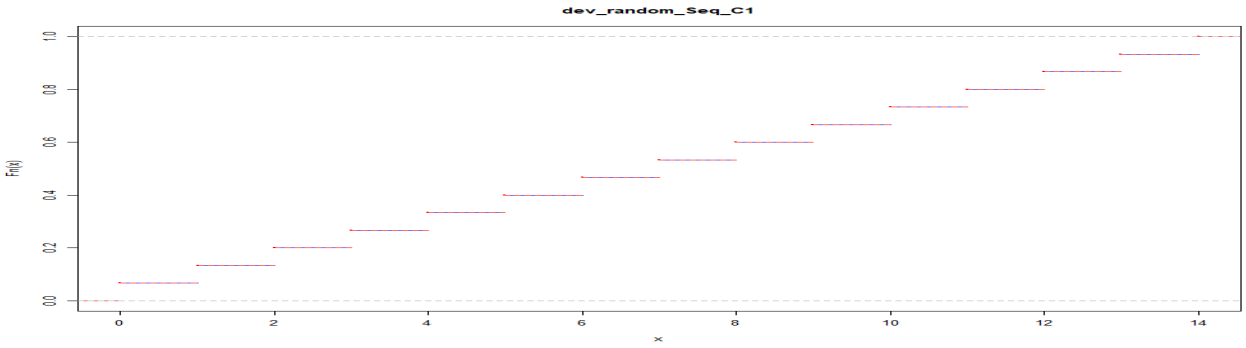


Рис. 1. Порівняння розподілів для послідовності dev_random_Seq_C1 за основою 15
та послідовності з рівномірного дискретного розподілу

Як видно з отриманих графіків, розподіл послідовності майже повністю накладається на рівномірний розподіл для значень з такими ж межами, що означає рівномірність послідовностей довільного алфавіту.

5.2.1.2. Послідовність за основою 2023.

- Дослідження з використанням монобітного тесту

Таблиця 10

Результати тестування для dev_random_Seq_C1 за основою 2023

Розмір вибірки після представлення за основою	90000000
p-значення	0.85315
$\alpha = 0.1$	Тестування пройдено успішно
$\alpha = 0.05$	Тестування пройдено успішно
$\alpha = 0.01$	Тестування пройдено успішно

Послідовність за обраною основою успішно проходить статистичний тест.

- Дослідження з використанням тесту хі-квадрат.

Таблиця 11

Результати тестування хі-квадрат для dev_random_Seq_C1 за основою 2023

Значення хі-квадрат	2032.124	
$\alpha = 0.1$	1918.549 < 2032.124 < 2127.724	Тестування пройдено успішно
$\alpha = 0.05$	1899.266 < 2032.124 < 2148.522	Тестування пройдено успішно
$\alpha = 0.01$	1861.954 < 2032.124 < 2189.557	Тестування пройдено успішно

Послідовність успішно проходить тест хі-квадрат.

- Дослідження з використанням критерію Колмогорова – Смирнова.

Однозразковий тест.

Таблиця 12

Результати однозразкового тесту Колмогорова – Смирнова для dev_random_Seq_C1

Довжина послідовності, що тестується (n)	9000000
D^+	0.00016463
D^-	0.00018614
D	0.00018614
Критичне значення для $\alpha = 0.01$	$Crit_{0.01} = \frac{1.62762}{\sqrt{n}} = 0.0005425$
Критичне значення для $\alpha = 0.05$	$Crit_{0.05} = \frac{1.35810}{\sqrt{n}} = 0.0004527$
Критичне значення для $\alpha = 0.1$	$Crit_{0.1} \frac{1.22385}{\sqrt{n}} = 0.00040795$
Оскільки $D < (Crit_{0.01}, Crit_{0.05}, Crit_{0.1})$ – послідовності походять з одного розподілу	

Однозразковий тест для послідовності за основою 2023 показує, що послідовність походить з рівномірного дискретного розподілу для меж 0:2022, а отже послідовність є рівномірною.

Двозразковий тест.

Таблиця 13

Результати двозразкового тесту Колмогорова – Смирнова для dev_random_Seq_C1

Довжина послідовності, що тестується (n)	9000000
D^+	0.00035444
D^-	0.000109
D	0.00035444
Критичне значення для $\alpha = 0.01$	$Crit_{0.01} = \frac{1.62762}{\sqrt{n}} = 0.0005425$
Критичне значення для $\alpha = 0.05$	$Crit_{0.05} = \frac{1.35810}{\sqrt{n}} = 0.0004527$
Критичне значення для $\alpha = 0.1$	$Crit_{0.1} \frac{1.22385}{\sqrt{n}} = 0.00040795$
Оскільки $D < (Crit_{0.01}, Crit_{0.05}, Crit_{0.1})$ – послідовності походять з одного розподілу	

Двозразковий тест також показує рівномірність послідовності за основою 2023.

Для більшої наочності і зрозумілості отриманих графіків було проведено додаткове тестування для 5000 значень. Графік такого тестування більш ясно показує розбіжності між розподілами, яких не видно на графіках для дуже великої кількості значень (рис. 2).

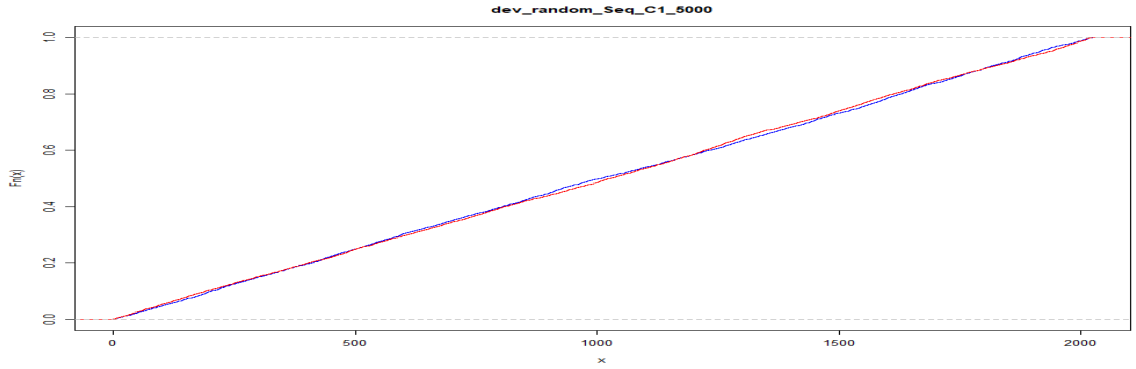


Рис. 2. Порівняння розподілів для послідовності dev_random_Seq_C1 та послідовності з рівномірного дискретного розподілу для 5000 значень

5.2.2. Дослідження послідовностей, отриманих методом «швидкої гральної кістки».

5.2.2.1. Послідовність за основою 15.

- Дослідження з використанням монобітного тесту.

Таблиця 14

Результати тестування для dev_random_Seq_C2 за основою 15

Розмір вибірки після представлення за основою	239000000
p-значення	0.143497
$\alpha = 0.1$	Тестування пройдено успішно
$\alpha = 0.05$	Тестування пройдено успішно
$\alpha = 0.01$	Тестування пройдено успішно

- Дослідження з використанням тесту хі-квадрат.

Таблиця 15

Результати тестування хі-квадрат для dev_random_Seq_C2 за основою 15

Значення хі-квадрат	16.277	
$\alpha = 0.1$	6.571 < 16.277 < 23.685	Тестування пройдено успішно
$\alpha = 0.05$	5.629 < 16.277 < 26.119	Тестування пройдено успішно
$\alpha = 0.01$	4.074 < 16.277 < 31.319	Тестування пройдено успішно

- Дослідження з використанням критерію Колмогорова – Смирнова

Однозразковий тест.

Таблиця 16

Результати однозразкового тесту Колмогорова – Смирнова для dev_random_Seq_C2

Довжина послідовності, що тестується (n)	23900000
D^+	0.000005509
D^-	0.00024991
D	0.00024991
Критичне значення для $\alpha = 0.01$	$Crit_{0.01} = \frac{1.62762}{\sqrt{n}} = 0.0003329$
Критичне значення для $\alpha = 0.05$	$Crit_{0.05} = \frac{1.35810}{\sqrt{n}} = 0.0002778$
Критичне значення для $\alpha = 0.1$	$Crit_{0.1} \frac{1.22385}{\sqrt{n}} = 0.0002503$
Оскільки $D < (Crit_{0.01}, Crit_{0.05}, Crit_{0.1})$ – послідовності походять з одного розподілу	

Однозразковий тест для послідовності за основою 15 показує, що послідовність походить з рівномірного дискретного розподілу для меж 0:14, а отже послідовність є рівномірною.

Двозразковий тест.

Таблиця 17

Результати двозразкового тесту Колмогорова – Смирнова
для dev_random_Seq_C2

Довжина послідовності, що тестується (n)	23900000
D^+	0.00020715
D^-	0.00013912
D	0.00020715
Критичне значення для $\alpha = 0.01$	$Crit_{0.01} = \frac{1.62762}{\sqrt{n}} = 0.0003329$
Критичне значення для $\alpha = 0.05$	$Crit_{0.05} = \frac{1.35810}{\sqrt{n}} = 0.0002778$
Критичне значення для $\alpha = 0.1$	$Crit_{0.1} \frac{1.22385}{\sqrt{n}} = 0.0002503$
Оскільки $D < (Crit_{0.01}, Crit_{0.05}, Crit_{0.1})$ – послідовності походять з одного розподілу	

Двозразковий тест також показує рівномірність послідовності за основою 15, що можна спостерігати на графіку (рис. 3).

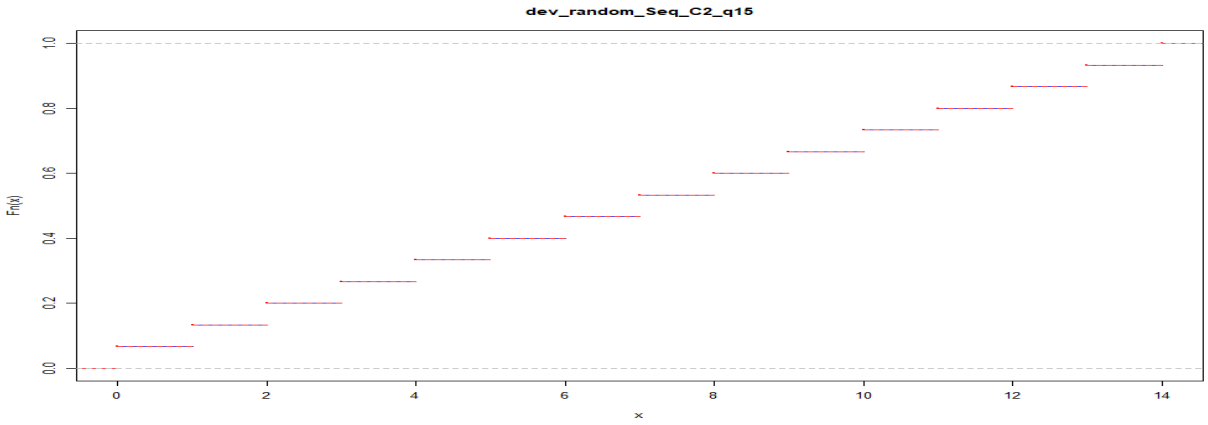


Рис. 3. Порівняння розподілів для послідовності dev_random_Seq_C2 за основою 15
та послідовності з рівномірного дискретного розподілу

5.2.2.2. Послідовність за основою 2023.

- Дослідження з використанням монобітного тесту.

Таблиця 18

Результати тестування для dev_random_Seq_C2 за основою 2023

Розмір вибірки після представлення за основою	90000000
p-значення	0.297884
$\alpha = 0.1$	Тестування пройдено успішно
$\alpha = 0.05$	Тестування пройдено успішно
$\alpha = 0.01$	Тестування пройдено успішно

- Дослідження з використанням тесту хі-квадрат.

Таблиця 19

Результати тестування хі-квадрат для dev_random_Seq_C2 за основою 2023

Значення хі-квадрат	2098.735	
$\alpha = 0.1$	1918.549 < 2098.735 < 2127.724	Тестування пройдено успішно
$\alpha = 0.05$	1899.266 < 2098.735 < 2148.522	Тестування пройдено успішно
$\alpha = 0.01$	1861.954 < 2098.735 < 2189.557	Тестування пройдено успішно

- Дослідження з використанням критерію Колмогорова – Смирнова

Однозразковий тест.

Таблиця 20

Результати однозразкового тесту Колмогорова – Смирнова для dev_random_Seq_C2

Довжина послідовності, що тестується (n)	9000000
D^+	0.000028918
D^-	0.00025623
D	0.00025623
Критичне значення для $\alpha = 0.01$	$Crit_{0.01} = \frac{1.62762}{\sqrt{n}} = 0.0005425$
Критичне значення для $\alpha = 0.05$	$Crit_{0.05} = \frac{1.35810}{\sqrt{n}} = 0.0004527$
Критичне значення для $\alpha = 0.1$	$Crit_{0.1} \frac{1.22385}{\sqrt{n}} = 0.00040795$
Оскільки $D < (Crit_{0.01}, Crit_{0.05}, Crit_{0.1})$ – послідовності походять з одного розподілу	

Однозразковий тест для послідовності за основою 2023 показує, що послідовність походить з рівномірного дискретного розподілу для меж 0:2022, а отже послідовність є рівномірною.

Двозразковий тест.

Таблиця 21

Результати двозразкового тесту Колмогорова – Смирнова для dev_random_Seq_C2

Довжина послідовності, що тестується (n)	9000000
D^+	0.00039344
D^-	0.000086889
D	0.00039344
Критичне значення для $\alpha = 0.01$	$Crit_{0.01} = \frac{1.62762}{\sqrt{n}} = 0.0005425$
Критичне значення для $\alpha = 0.05$	$Crit_{0.05} = \frac{1.35810}{\sqrt{n}} = 0.0004527$
Критичне значення для $\alpha = 0.1$	$Crit_{0.1} \frac{1.22385}{\sqrt{n}} = 0.00040795$
Оскільки $D < (Crit_{0.01}, Crit_{0.05}, Crit_{0.1})$ – послідовності походять з одного розподілу	

Двозразковий тест також показує рівномірність послідовності за основою 2023, що можна спостерігати на рис. 4.

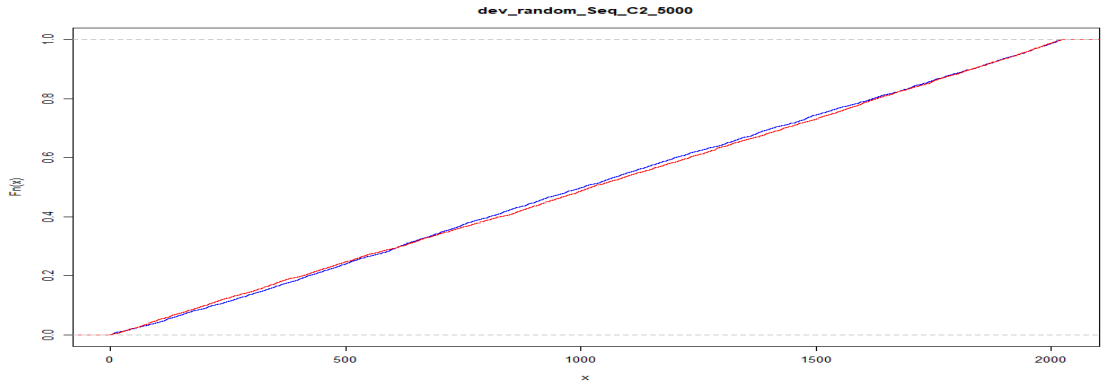


Рис. 4. Порівняння розподілів для послідовності dev_random_Seq_C2
та послідовності з рівномірного дискретного розподілу для 5000 значень

5.2.3. Дослідження послідовностей, отриманих методом Уокера.

5.2.3.1. Послідовність за основою 15.

- Дослідження з використанням монобітного тесту.

Таблиця 22

Результати тестування для dev_random_Seq_C3 за основою 15

Розмір вибірки після представлення за основою	239000000
p-значення	0.706594
$\alpha = 0.1$	Тестування пройдено успішно
$\alpha = 0.05$	Тестування пройдено успішно
$\alpha = 0.01$	Тестування пройдено успішно

- Дослідження з використанням тесту хі-квадрат

Таблиця 23

Результати тестування хі-квадрат для dev_random_Seq_C3 за основою 15

Значення хі-квадрат	10.969	
$\alpha = 0.1$	6.571 < 10.969 < 23.685	Тестування пройдено успішно
$\alpha = 0.05$	5.629 < 10.969 < 26.119	Тестування пройдено успішно
$\alpha = 0.01$	4.074 < 10.969 < 31.319	Тестування пройдено успішно

- Дослідження з використанням критерію Колмогорова – Смирнова.

Однозразковий тест.

Таблиця 24

Результати однозразкового тесту Колмогорова – Смирнова
для dev_random_Seq_C3

Довжина послідовності, що тестується (n)	23900000
D^+	0.000060767
D^-	0.00010215
D	0.00010215
Критичне значення для $\alpha = 0.01$	$Crit_{0.01} = \frac{1.62762}{\sqrt{n}} = 0.0003329$
Критичне значення для $\alpha = 0.05$	$Crit_{0.05} = \frac{1.35810}{\sqrt{n}} = 0.0002778$
Критичне значення для $\alpha = 0.1$	$Crit_{0.1} \frac{1.22385}{\sqrt{n}} = 0.0002503$
Оскільки $D < (Crit_{0.01}, Crit_{0.05}, Crit_{0.1})$ – послідовності походять з одного розподілу	

Однозразковий тест для послідовності за основою 15 показує, що послідовність походить з рівномірного дискретного розподілу для меж 0:14, а отже послідовність є рівномірною.

Двозразковий тест.

Таблиця 25

Результати двозразкового тесту Колмогорова – Смирнова
для dev_random_Seq_C3

Довжина послідовності, що тестується (n)	23900000
D^+	0.00018473
D^-	0.000006736
D	0.00018473
Критичне значення для $\alpha = 0.01$	$Crit_{0.01} = \frac{1.62762}{\sqrt{n}} = 0.0003329$
Критичне значення для $\alpha = 0.05$	$Crit_{0.05} = \frac{1.35810}{\sqrt{n}} = 0.0002778$
Критичне значення для $\alpha = 0.1$	$Crit_{0.1} \frac{1.22385}{\sqrt{n}} = 0.0002503$
Оскільки $D < (Crit_{0.01}, Crit_{0.05}, Crit_{0.1})$ – послідовності походять з одного розподілу	

Двозразковий тест також показує рівномірність послідовності за основою 15, що можна спостерігати на рис. 5.

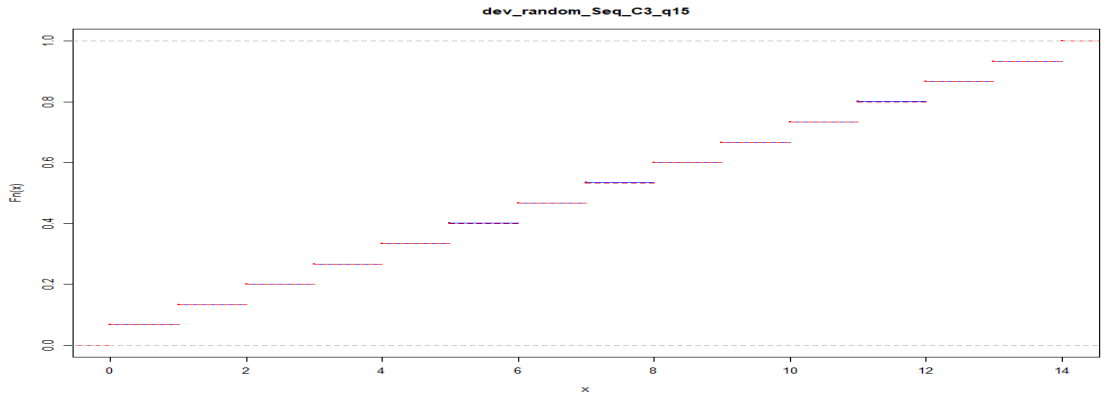


Рис. 5. Порівняння розподілів для послідовності dev_random_Seq_C3 за основою 15 та послідовності з рівномірного дискретного розподілу

5.2.3.2. Послідовність за основою 2023.

- Дослідження з використанням монобітного тесту.

Таблиця 26

Результати тестування для dev_random_Seq_C3 за основою 2023

Розмір вибірки після представлення за основою	90000000
p-значення	0.638141
$\alpha = 0.1$	Тестування пройдено успішно
$\alpha = 0.05$	Тестування пройдено успішно
$\alpha = 0.01$	Тестування пройдено успішно

- Дослідження з використанням тесту хі-квадрат.

Таблиця 27

Результати тестування хі-квадрат для dev_random_Seq_C3 за основою 2023

Значення хі-квадрат	2067.994	
$\alpha = 0.1$	1918.549 < 2067.994 < 2127.724	Тестування пройдено успішно
$\alpha = 0.05$	1899.266 < 2067.994 < 2148.522	Тестування пройдено успішно
$\alpha = 0.01$	1861.954 < 2067.994 < 2189.557	Тестування пройдено успішно

- Дослідження з використанням критерію Колмогорова – Смирнова.

Однозразковий тест.

Таблиця 28

Результати однозразкового тесту Колмогорова – Смирнова для dev_random_Seq_C3

Довжина послідовності, що тестується (n)	9000000
D^+	0.00020297
D^-	0.00024453
D	0.00024453
Критичне значення для $\alpha = 0.01$	$Crit_{0.01} = \frac{1.62762}{\sqrt{n}} = 0.0005425$
Критичне значення для $\alpha = 0.05$	$Crit_{0.05} = \frac{1.35810}{\sqrt{n}} = 0.0004527$
Критичне значення для $\alpha = 0.1$	$Crit_{0.1} \frac{1.22385}{\sqrt{n}} = 0.00040795$
Оскільки $D < (Crit_{0.01}, Crit_{0.05}, Crit_{0.1})$ – послідовності походять з одного розподілу	

Однозразковий тест для послідовності за основою 2023 показує, що послідовність походить з рівномірного дискретного розподілу.

Двозразковий тест.

Таблиця 29

Результати двозразкового тесту Колмогорова – Смирнова для dev_random_Seq_C3

Довжина послідовності, що тестується (n)	9000000
D^+	0.00018144
D^-	0.00038344
D	0.00038344
Критичне значення для $\alpha = 0.01$	$Crit_{0.01} = \frac{1.62762}{\sqrt{n}} = 0.0005425$
Критичне значення для $\alpha = 0.05$	$Crit_{0.05} = \frac{1.35810}{\sqrt{n}} = 0.0004527$
Критичне значення для $\alpha = 0.1$	$Crit_{0.1} \frac{1.22385}{\sqrt{n}} = 0.00040795$
Оскільки $D < (Crit_{0.01}, Crit_{0.05}, Crit_{0.1})$ – послідовності походять з одного розподілу	

Двозразковий тест також показує рівномірність послідовності за основою 2023 (рис. 6).

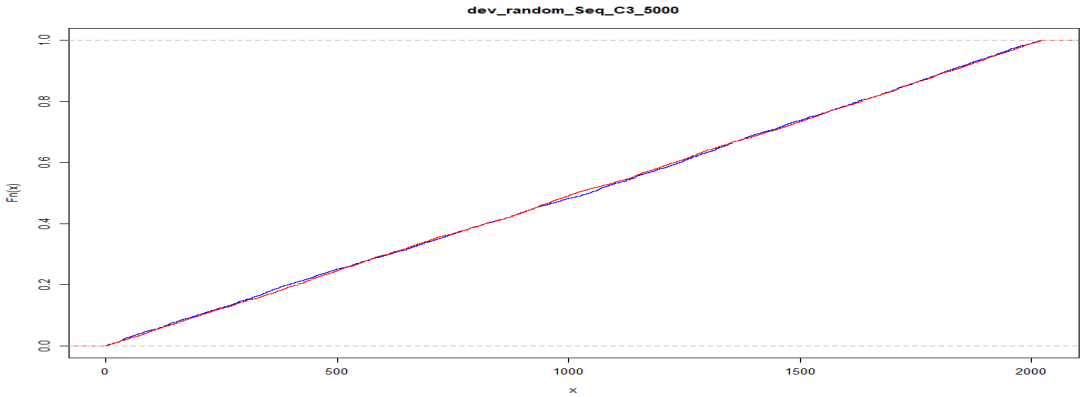


Рис. 6. Порівняння розподілів для послідовності dev_random_Seq_C3 та послідовності з рівномірного дискретного розподілу для 5000 значень

На рис. 7 показано значення хі-квадрат для послідовностей з різних методів отримання послідовностей довільного алфавіту для різних основ.

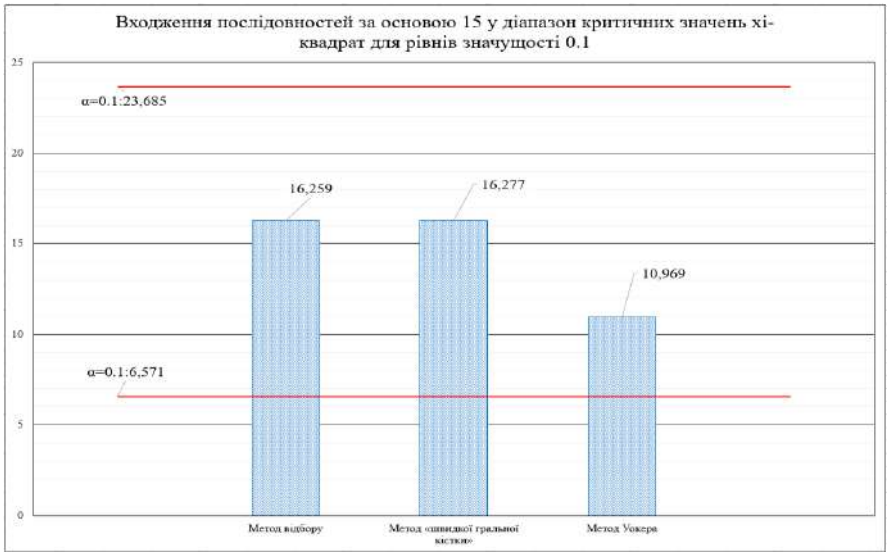


Рис. 7. Входження послідовностей за основою 15 у діапазон критичних значень хі-квадрат для рівня значущості 0.1

Рис. 8. Входження послідовностей за основою 2023 у діапазон критичних значень хі-квадрат для рівня значущості 0.1

Як видно з отриманих результатів, послідовності довільного алфавіту, отримані кожним з методів успішно проходять статистичне тестування з використанням різних критеріїв.

Висновки

Твердження 5 надає можливість будувати обґрунтовано стійки (у загальновизнаному сенсі цього слова [5 – 7]) генератори (псевдо)випадкових послідовностей над довільним алфавітом, виходячи з аналогічних генераторів двійкових послідовностей та допустимих алгоритмів, визначених в п. 3.

Виконано порівняння наведених методів генерації послідовностей за швидкодією та обсягом необхідних даних для параметрів, які застосовують в алгоритмах [1 – 3]. Для практичного застосування за швидкодією їхніх програмних реалізацій і обсягом вхідних даних, що ними застосовуються, доцільно застосовувати алгоритм A_3 замість алгоритму A_1

Послідовності довільного алфавіту, отримані кожним з методів, успішно проходять статистичне тестування з використанням різних критеріїв.

Список літератури:
1. FIPS.203. https://csrc.nist.gov/pubs/fips/203/ipd
2. FIPS.204. https://csrc.nist.gov/pubs/fips/204/ipd
3. ДСТУ 9212-2023. ДСТУ 9212:2023 Інформаційні технології. Криптографічний захист інформації. Алгоритм електронного підпису на модульних решітках
4. Олексійчук А.М., Курінний О.В. Методи криптоаналізу потокових шифрів : навч. вид. Київ : КПІ ім. Ігоря Сікорського, 2023. 172 с.
5. Blum M., Micali S. How to generate cryptographically strong sequences of pseudo-random bits // SIAM Journal of Computing. 1984. Vol. 13(4). P. 850–864.
6. Yao A.C. Theory and application of trapdoor functions // The 23-th. Annual Symposium on Foundations of Computer Science. IEEE, 1982. P. 80–91.
7. Katz J., Lindell Y. Introduction to modern cryptography. CRC Press, 2015. 598 p.
8. Lumbroso J. Optimal discrete uniform generation from coin flips, and application // arXiv.1304.1916v1 [cs.DS] 11 Apr 2013.
9. Кнут Д. Искусство программирования. Т. 2. Получисленные алгоритмы. 3-е изд. ; пер. с англ. Москва : Изд. дом “Вильямс”, 2000. 832 с.
10. Алексейчук А.Н. Неасимптотические нижние границы информационной сложности статистических атак на симметричные криптосистемы // Кибернетика и системный анализ. 2018. №. 1. С. 93–104.
11. Zvi Drezner,Ofir Turel & Dawit Zerom. A Modified Kolmogorov – Smirnov Test for Normality. 2010. URL: https://www.tandfonline.com/doi/citedby/10.1080/03610911003615816?scroll=top&needAccess=true (дата звернення: 12.03.2024).
12. William G. Cochran. The χ2 Test of Goodness of Fit. 1952. URL: https://www.jstor.org/stable/2236678 (дата звернення: 12.03.2024).
13. NIST Engineering Statistics Handbook. Kolmogorov – Smirnov Goodness-of-Fit Test. URL: https://www.itl.nist.gov/div898/handbook/eda/section3/eda35g.htm (дата звернення: 12.03.2024).
14. Taylor B. Arnold and John W. Emerson. Nonparametric Goodness-of-Fit Tests for Discrete Null Distributions. 2011. URL: http://www.stat.yale.edu/~jay/EmersonMaterials/DiscreteGOF.pdf (дата звернення: 12.03.2024).
15. R Development Page. Proposed Revision to stats::ks.test(). URL: https://r-forge.r-project.org/R/?group_id=802 (дата звернення: 12.03.2024).
16. Docs Tibco. Kolmogorov-Smirnov Tests. URL: https://docs.tibco.com/pub/enterprise-runtime-for-R/6.0.0/doc/html/Language_Reference/stats/ks.test.html (дата звернення: 12.03.2024).
17. Purrr: Functional Programming Tools. URL: https://uribo.github.io/rpkg_showcase/programming/purrr.html (дата звернення: 12.03.2024).
18. S. Massa. Lecture 13: Kolmogorov Smirnov Test & Power of Tests. Department of Statistics, University of Oxford. 2016. URL: https://www.ime.unicamp.br/~dias/Lecture%2013.pdf (дата звернення: 12.03.2024).
19. Kolmogorov-Smirnov Test Critical Values. URL: https://people.cs.pitt.edu/~lipschultz/cs1538/prob-table_KS.pdf (дата звернення: 12.03.2024).
20. NIST Engineering Statistics Handbook. Chi-Square Goodness-of-Fit Test. URL: https://www.itl.nist.gov/div898/handbook/eda/section3/eda35f.htm (дата звернення: 12.03.2024).
21. NIST Engineering Statistics Handbook. Critical Values of the Chi-Square Distribution. URL: https://www.itl.nist.gov/div898/handbook/eda/section3/eda3674.htm (дата звернення: 12.03.2024).
22. Soper D.S. Critical Chi-Square Value Calculator. 2024. URL: https://www.danielsoper.com/statcalc (дата звернення: 12.03.2024).
23. Jetbrains. PyCharm 2023.3.3. URL: https://www.jetbrains.com/pycharm/whatsnew/ (дата звернення: 12.03.2024).
24. Генератор рівномірно розподілених ймовірних чисел: пат. 33361 Україна : G06F7/58, 07C15/00. №99020855; заявл. 16.02.1999; опубл. 15.02.2001 Бюл. №1
25. Офіційний сайт КГВЧ Quantis RNG від швейцарської компанії ID Quantique (IDQ) [Електроний ресурс]. Режим доступу: https://www.idquantique.com/random-number-generation/overview/.

Надійшла до редколегії 14.01.2024

Відомості про авторів:

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

Олексійчук Антон Миколайович – д-р техн. наук, доцент, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України “Київський політехнічний інститут імені Ігоря Сікорського”, професор спеціальної кафедри № 1; Україна; e-mail: alex-dtn@ukr.net

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

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

УДК 004.056.5 **DOI:10.30837/rt.2024.1.216.02**

Д.Ю. ГОЛУБНИЧИЙ, канд. техн. наук, С.О. КАНДІЙ, М.В. ЄСІНА, канд. техн. наук, Д.Ю. ГОРБЕНКО

МЕТОДИ ТА ЗАСОБИ АНАЛІЗУ, ОЦІНКИ ТА ПОРІВНЯННЯ ВЛАСТИВОСТЕЙ ВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ ТА ВИПАДКОВИХ ЧИСЕЛ

Вступ

Наразі випадкові послідовності (ВП) та випадкові числа (ВЧ), що виробляються фізично справжніми (PT RNG) та нефізично справжніми (NPT RNG) генераторам, широко застосовуються на практиці – вони по суті законодавчо визначають механізми генерування ключів у криптографічних системах [1 – 11]. У залежності від криптографічних перетворень, вони застосовуються для генерації довгострокових ключів та ключів сеансу симетричних криптоперетворень, довгострокових асиметричних пар ключів та пар сеансових ключів, загальних параметрів криптоперетворень та криптографічних протоколів, специфічних одноразових значень (nonces), викликів (challenges), засліплення та маскування значень тощо [2 – 6, 9, 12 – 18].

Серед множини вимог до таких генераторів є забезпечення у ряді, а можливо і більшості, криптографічних застосунків максимально можливого значення початкової ентропії. По суті, критерій максимуму початкової ентропії криптографічних застосунків є безумовним, і, при обґрунтовано вибраних розмірах ключових даних та параметрів, дозволяє забезпечити необхідні та достатні умови їх криптографічної живучості та криптографічної стійкості. Вказане однозначно визначає необхідність генерування ключів та параметрів криптографічних перетворень на основі тільки PT RNG та NPT RNG джерел шуму [2 – 5, 10, 11]. Іншими обов'язковими вимогами є обов'язковість стандартизації та сертифікації методів та засобів генерування ВП та ВЧ [2 – 6, 10 – 18] на основі відповідних джерел шуму.

Аналіз міжнародних та національних нормативно-правових документів щодо вимог до PT RNG та NPT RNG джерел та відповідно до генераторів показав, що вони, з урахуванням суттєвих викликів, що пов'язані з розширенням можливостей криптоаналізу на основі застосування, крім класичних, квантових та атак бічними каналами, в суттєвій мірі повинні бути удосконаленими [14 – 18] та оцінені з використанням комплексних методик з використанням системи безумовних критеріїв.

В подальшому у цій статті в якості основних будемо дотримуватись таких основних визначень [19]:

- випадкова послідовність (ВП) – послідовність незалежних та однаково розподілених змінних (з рівномірного розподілу);
- випадкові числа (ВЧ) – це дискретні значення (зазвичай біти, рядки бітів або цілі числа), які отримують у окремі моменти часу з джерела шуму генератори випадкових послідовностей;
- псевдовипадкова послідовність (ПВП) – послідовність символів, що обчислювально не відмінна від випадкової послідовності і згенерована детермінованим алгоритмом.

Пошук новітніх теоретичних та практичних досліджень та результатів щодо методів та засобів генерування ВП та ВЧ дозволив зупинитися на перспективній програмі німецьких загальних критеріїв (CC) протягом приблизно двох десятиліть – AIS 20 і AIS 31, що визначають як удосконалювати та оцінювати різні RNG генератори [21, 17 – 19]. Вони визначають класи функціональності для різних типів RNG. Щоб бути сумісним з певним класом функціональності, RNG мають відповідати всім вимогам класу. Крім того, AIS 20 і AIS 31 окреслюють методологію оцінювання детермінованих RNG (DRNG) і справжніх RNG (TRNG) [2 – 5].

Традиційно в ряді випадків вважається, що наявність статистичного тестування RNG генераторів та відповідність вимогам згідно з [6 – 8] вже гарантує випадковість. Але при застосуванні порушником класичних, квантових атак і атак бічними каналами, цього недостатньо. Однозначно визнано, що крім статистичного тестування, необхідно застосовувати і стохастичне тестування на основі аналізу та оцінки початкової ентропії ВП та ВЧ, наприклад на основі PTRNG та NPTRNG, в умовах застосування класичних, квантових атак та атак бічними каналами [12 – 18, 20].

Метою даної статті є обґрунтування, розробка та експериментальне підтвердження коректного застосування алгоритмів генерування ВП та ВЧ на основі PTRNG та NPTRNG, в тому числі при застосуванні класичної та квантової мікроелектроніки, а також розробка рекомендацій щодо їх застосування для генерування ключів та параметрів для квантово стійких методів та стандартів криптографічних перетворень.

1. Джерела шуму, що можуть застосовуватися для генерації ВП та ВЧ на основі PTRNG та NPTRNG

Наразі існує значне число ДШ, які можливо застосовувати для генерування ВП та ВЧ. Аналіз показав, що ДШ, які можуть задовольняти вимогам, можливо поділити на два класи [2, 4, 5, 10, 11]:

- фізичні ДШ, в основі таких лежить деяке непередбачуване ймовірнісне фізичне явище, яке містить певну кількість ентропії [2, 3];
- нефізичні ДШ, в основі яких також лежить в певній мірі передбачуване явище, кожне з яких містить певну кількість ентропії.

Причому на основі фізичних ДШ можливо генерувати фізично справжні PT RNG ВП та ВЧ, а на основі нефізичних ДШ можливо генерувати нефізичні справжні NPT RNG ВП ТА ВЧ [2, 10, 11].

Фізичні ДШ можливо класифікувати згідно з фізичним явищем, яке має ймовірнісний характер, що має значну кількість ентропії [2, 3]:

- ДШ на основі шуму, в цьому класі певний фізичний процес має ймовірнісний характер, який практично неможливо передбачити, та можливість генерувати фізично справжні PT RNG ВП та ВЧ;
- ДШ на основі хаосу, цей клас ДШ ґрунтується на наявності певної системи (можливо навіть детермінованої) з багатьох складових, що має хаотичну поведінку у цілому;
- ДШ на основі вільних осциляторів, що можуть мати ентропію, ця можливість ґрунтується на непередбачуваності явищ в цифровій електротехніці. Такі вільні осцилятори є популярним вибором фізично справжнього PT RNG генератора ВП чи ВЧ на основі різноманітних персональних пристроїв;
- ДШ на основі ефектів квантової мікроелектроніки, що складають відносно новий, перспективний клас ДШ, в ньому ентропія створюється з використанням квантових ефектів мікроелектроніки.

Джерелами нефізичного шуму, що можуть генерувати NPT RNG нефізично справжні ВП чи ВЧ можуть слугувати [2, 4, 5]:

- події, що ґрунтуються на процесах взаємодії з суб’єктом (наприклад, користувачем) чи об’єктом та які можливо завдати на основі ймовірнісного подання;
- події, що ґрунтуються на використанні переривання апаратних пристроїв (наприклад, мережевої карти), для яких можливо задати ентропію на основі ймовірнісного подання переривання тощо.

Більш детальні дані щодо цих ДШ та відповідно фізично справжніх PT RNG генераторів і нефізично справжніх генераторів ВП (ВЧ) можна знайти в [2, 3].

У табл. 1 наведено основні переваги, недоліки та особливості і результати порівняння фізично справжніх ДШ, що можуть застосовуватись для генерування ключових даних та

загальних параметрів для існуючих класичних та перспективних квантово стійких криптографічних перетворень та криптографічних протоколів.

Таблиця 1

Переваги, недоліки та особливості ДШ

Тип	Переваги	Недоліки	Особливості
На основі шуму	Багато конструкцій генераторів, практичних досліджень та наявних впроваджень	Рух частинок, які генерують шум, в певній мірі взаємокорельований. Шум не можна «перезапустити», щоб перервати кореляції між послідовними вимірюваннями генерування бітів. У них більшість процесів, наприклад у резисторах, стабілітронах та транзисторах, мають певний ефект пам'яті. Випадковість джерел шуму неможливо завдати, виміряти або навіть контролювати під час виготовлення пристрою. Щодо них необхідний захист від впливу зовнішніх електромагнітних полів та випромінювання генератора	Для таких конструкцій використовують переважно шуми електричної природи. Основні фізичні ефекти: ефект Джонсона та ефект Зенера
На основі хаосу	Різноманітність фізичних процесів, на яких ґрунтуються генератори	Важко довести, що система дійсно хаотична. ДШ на основі хаосу в довгостроковій перспективі не можуть виробляти нову ентропію, що неминуче закінчується виробленням не менше 1 біта ентропії на кожен новий згенерований випадковий біт	Основні типи конструкцій: оптичні, електричні, оптико-електричні та механічні
На вільних осциляторах	Перевірені та стандартизовані конструкції. Найрозповсюдженіший тип генераторів. RNG на основі вільних осциляторів є недорогими рішеннями, які можна легко реалізувати в звичайних програмованих або реконфігурованих логічних мікросхемах	Коли декілька осциляторів розташовані близько один до одного (наприклад, на одній мікросхемі), вони, як правило, синхронізуються через електромагнітну взаємодію, що сприяє високому посиленню підсилювачів вільних осциляторів, що робить ДШ вразливими до атак із зовнішнім електромагнітним випромінюванням. Якщо такі ДШ синхронізуються або принаймні частково синхронізуються, з'явиться шаблон зі стохастичним відхиленням (шумом). Окрім цього, ще одна дуже важлива проблема щодо ДШ на вільних осциляторах полягає в тому, що амплітуда вихідного сигналу ДШ залежить від деталей блукаючих реактивних опорів і затримок у ланцюзі. Складність процедур постобробки, необхідних для проходження статистичних тестів, у RNG на основі вільних осциляторів часто така, що будь-який доказ випадковості ускладнений	Часткове вирішення проблем було знайдено в новій синергетичній комбінації регістра зсуву лінійного зворотного зв'язку (LFSR), а також вільних осциляторів, яка називається кільцевим осцилятором Фібоначчі (FIRO) і кільцевим осцилятором Галуа (GARO)
Радіоактивний розпад	Дійсно випадковий квантовий процес. Добре досліджені конструкції. Доказова випадковість	Оскільки випадкове джерело є радіоактивним, воно вимагає особливої обережності (покращених заходів безпеки) та знань. Обмеженням є також «мертвий час» детектора через накопичення іонів усередині детектора. Низька швидкість генерації	Одне із перших квантових явищ, що були використані для генерації випадкових бітів та чисел. Можливо використовувати два основні методи – метод швидкої синхронізації та метод повільного годинника. Деякі сучасні генератори випадкових чисел, засновані на радіоактивному розпаді. У них замість GM-трубок використовують напівпровідникові пристрої

Продовження табл. 1

Тип	Переваги	Недоліки	Особливості
Атомарні системи	Використовується квантовий ефект. Забезпечується доказова випадковість	Експериментальні установки, необхідні для генерації випадкових чисел з використанням захоплених іонів, набагато складніші, генерація з дуже низькою швидкістю	Використовують спіновий ефект (шум)
Фотонні детектори	Використовуються квантові ефекти. Велика швидкість генерації. Доказова випадковість.	Після кожної події виявлення, детектори неактивні протягом певного періоду, протягом якого вони не можуть виявити фотони. Це призводить до кореляції між згенерованими бітами та збільшує час, необхідний для їх отримання. Цього можна уникнути, використовуючи лише один детектор	Швидкість генерації випадкових бітів також може бути покращена, якщо генератор вимірює кілька шляхів проходження фотонів
Вакуумний шум	Використовуються квантові ефекти. Доказова випадковість. Практичні реалізації досягли швидкості генерації до 3 Гбіт/с	Швидкість генерації ВП та ВЧ у цих пристроях обмежена швидкістю детектора в зоні дробового шуму, коли в загальному спостережуваному шумі домінує вакуумний шум	Використовують випадковість вакуумних флуктуацій електромагнітного поля

2. Аналіз вимог щодо ДШ та їх ентропії

Основоположні вимоги до джерел шуму та його ентропії було запропоновано в стандарті NIST SP800-90B. Метою вимог NIST США до джерела ентропії [2, 4] є надання розробнику допомоги в розробці/впровадженні джерела ентропії, яке може надати вихідні дані з постійною кількістю ентропії, а також надати необхідну документацію для перевірки джерела ентропії.

Аналіз показує, що стандарт NIST SP800-90B [4] висуває наступні вимоги до ДШ у вигляді PTRNG та NPTRNG:

1. Наявність обґрунтованої стохастичної моделі вихідних сигналів ДШ. Модель повинна включати опис того, як працює ДШ та яким чином створюється непередбачуваність, а також і обґрунтування того, чому джерело шуму забезпечує прийнятну вихідну ентропію.

2. Поведінка джерела шуму має бути стаціонарною, коли розподіли ймовірностей вихідних сигналів джерела шуму не змінюються з часом при роботі джерела в нормальних умовах. Для цього повинне бути обґрунтовано, звідки походить непередбачуваність, і приблизно описано поведінку ДШ щодо стаціонарності його поведінки.

3. Модель ДШ повинна надавати чітке визначення очікуваної ентропії, що забезпечується вихідними сигналами джерела шуму, і надавати технічну аргументацію, чому джерело шуму може підтримувати таку швидкість ентропії.

4. Стан джерела шуму має бути максимально захищений від впливу. Методи, що використовуються для цього, повинні бути задокументовані, щодо межі безпеки захисту ДШ від впливу.

5. Незважаючи на те, що джерело шуму не зобов’язане створювати неупереджені та незалежні вихідні сигнали, воно повинно демонструвати випадкову поведінку, коли вихід не може бути визначений жодним відомим алгоритмічним правилом.

6. Джерело шуму має генерувати випадкові значення фіксованої довжини та має опис вихідного простору джерела шуму.

7. Якщо для підвищення безпеки використовуються додаткові ДШ, необхідно мати документ, який описує додаткові джерела шуму.

3. Методи оцінки ентропій ВП та ВЧ, що згенеровані PTRNG та NPTRNG

Ентропійні методи оцінки ґрунтуються на використанні узагальненого поняття ентропії Реньї [2, 21]. Нехай X – випадкова змінна, що у найбільш узагальненому виді визначає ентропію Реньї. Для випадкової змінної X ентропію Реньї можливо розрахувати за формулою

$$H_\alpha(X)=\frac{1}{1-\alpha}\log_2\sum_{i=1}^{k}(Pr[X=\omega_i])^\alpha, 0\le\alpha<\infty. \quad (1)$$

На практиці значеннями параметра α є 1, 2 та ∞. При α є 1 із (1) отримуємо співвідношення для оцінки ентропії Шеннона, при α є 2 – для оцінки колізійної ентропії, а при α є ∞ – для оцінки мінімальній ентропії.

За визначенням ентропія Реньї $H_\alpha(X)$ залежить тільки від розподілу μ випадкової змінної X, тому будемо використовувати також нотацію $H_\alpha(\mu)$, показуючи залежність $H_\alpha(X)$ як від α, так і від μ.

Розглянемо більш детально кожен випадок і покажемо, що у приватних випадках відповідних α маємо збіг.

Врахуємо, що ентропія Шеннона є границею ентропії Реньї $H_\alpha(X)$ в точці $\alpha=1$, в результаті отримуємо

$$H_1(x)=\lim_{\alpha\to1}H_\alpha(x)=\lim_{\alpha\to1}\frac{1}{1-\alpha}\log_2\sum_{i=1}^{k}(Pr[X=\omega_i])^\alpha.$$

Для того щоб отримати класичну формулу ентропії Шеннона з цієї границі скористаємося правилом Лопіталя, згідно з яким для двох дійсних функцій $f(x)=\log_2\sum_{i=1}^{k}(Pr[X=\omega_i])^\alpha$ та $g(x)=1-\alpha$, що мають похідні $f'(x), g'(x)$ в околиці точки δ, має місце вираз

$$\lim_{x\to\delta}\frac{f(x)}{g(x)}=\lim_{x\to\delta}\frac{f'(x)}{g'(x)}.$$

У цьому випадку $f(x)=\log_2\sum_{i=1}^{k}(Pr[X=\omega_i])^\alpha$, $g(x)=1-\alpha$ і $\delta=\alpha=1$.

Для отримання похідних скористаємося такими формальними правилами взяття похідних складної функції

$$\frac{d}{dx}\log_2(x)=\frac{1}{x\ln 2}, \frac{d}{dx}a^x=a^x\cdot\ln a.$$

Підставляючи відповідні значення у формулу (1), отримуємо:

$$\lim_{\alpha\to1}H_\alpha(x)=\lim_{\alpha\to1}\frac{\log_2\sum_{i=1}^{k}(Pr[X=\omega_i])^\alpha}{1-\alpha}=\lim_{\alpha\to1}\frac{\frac{d}{dx}\left(\log_2\sum_{i=1}^{k}(Pr[X=\omega_i])^\alpha\right)}{\frac{d}{dx}(1-\alpha)}=$$

$$=\lim_{\alpha\to1}\frac{\left(\sum_{i=1}^{k}(Pr[X=\omega_i])^\alpha\right)^{-1}\sum_{i=1}^{k}Pr[X=\omega_i]^\alpha\cdot\ln(Pr[X=\omega_i])}{-\ln 2}$$

Використовуючи властивість натурального логарифму $\frac{\ln b}{\ln c}=\log_c b$, перетворюємо $\frac{\sum_{i=1}^{k}\ln(Pr[X=\omega_i])}{-\ln 2}$ і отримаємо наступний вираз:

$$\lim_{\alpha\to1}H_\alpha(x)=-\sum_{i=1}^{k}Pr[X=\omega_i]\cdot\log_2(Pr[X=\omega_i]).$$

Звідки, маємо класичну формулу Шеннона:

$$H_1(X) = H(X) = -\sum_{i=1}^{k} Pr[X = \omega_i] \log_2 (Pr[X = \omega_i]). \quad (2)$$

Якщо $Pr[X = \omega_i] = 0$, то, за домовленістю, $Pr[X = \omega_i] \log_2 (\Pr[X = \omega_i]) = 0$. Позначення H зазвичай використовується замість H_1 для ентропії Шеннона. Ентропію Шеннона $H = H_1$ іноді називають загальною ентропією, або просто ентропією через її важливість в теорії інформації [1].

У (1) вказано, що мінімальна ентропія є спеціальним випадком для якого $\alpha = \infty$. На основі виразу (1) отримаємо аналітичне співвідношення для мінімальної ентропії. Так як $\alpha = \infty$, то на основі обчислення границі скористаємося тим фактом, що для усіх i=1,2, …k, $0 \le Pr[X = \omega_i] \le 1$. При збільшенні α сума $\sum_{i=1}^{k} Pr[X = \omega_i]^{\alpha}$ буде наближатися до $\max_i Pr[X = \omega_i]$.

Позначимо $p_i = Pr[X = \omega_i]$.

Розглянемо на основі ентропії Реньї альтернативний варіант отримання співвідношення для мінімальної ентропії. Враховуючи прийняте позначення, маємо

$$\lim_{\alpha \to \infty} H_\alpha(x) = \lim_{\alpha \to \infty} \frac{\log_2 \sum_{i=1}^{k} p_i^{\alpha}}{1-\alpha}.$$

Для виділення величини $\max_i p_i^{\alpha}$ виконаємо перетворення

$$\lim_{\alpha \to \infty} \frac{\log_2 \left(\sum_{i=1}^{k} \left(\left(\frac{p_i}{\max_i p_i} \right)^{\alpha} \cdot \max_i p_i^{\alpha} \right) \right)}{1-\alpha}.$$

Оскільки добуток під логарифмом дає суму двох логарифмів, то справедливо, що

$$\lim_{\alpha \to \infty} \frac{\log_2 \sum_{i=1}^{k} \left(\frac{p_i}{\max_i p_i} \right)^{\alpha} + \log_2 \left(\max_i p_i^{\alpha} \right)}{1-\alpha} =$$

$$= \lim_{\alpha \to \infty} \frac{\log_2 \sum_{i=1}^{k} \left(\frac{p_i}{\max_i p_i} \right)^{\alpha}}{1-\alpha} + \lim_{\alpha \to \infty} \frac{\log_2 \left(\max_i p_i^{\alpha} \right)}{1-\alpha}.$$

Позначимо, $\beta = \sum_{i=1}^{k} \left(\frac{p_i}{\max_i p_i} \right)^{\alpha}$, маємо:

$$\frac{\log_2 \beta}{1-\alpha} + \lim_{\alpha \to \infty} \frac{\log_2 \left(\max_i p_i^{\alpha} \right)}{1-\alpha}.$$

Оскільки, значення p_i пронормоване $\max_i p_i$, то під знаком суми одне $\max_i p_i = 1$, а сума всіх інших пронормованих ймовірностей – менше або дорівнює 1.

Тобто, $1 < \beta \le k$. Так як $\alpha \to \infty$, то значення $\beta \to \infty$:

$$\frac{\log_2 \beta}{\infty} + \lim_{\alpha \to \infty} \frac{\log_2 \left(\max_i p_i^{\alpha} \right)}{1-\alpha} = \frac{\log_2 \beta}{\infty} + \lim_{\alpha \to \infty} \frac{\alpha \log_2 \left(\max_i p_i \right)}{1-\alpha}.$$

Оскільки β – скінченна величина, то $\frac{\log_2 \beta}{\infty} = 0$. Тому можна записати для похідних

$$0 + \lim_{\alpha\to\infty} \frac{\alpha \log_2 (\max_i p_i)}{1-\alpha} = \lim_{\alpha\to\infty} \frac{\frac{d}{d\alpha}\left(\alpha \log_2 (\max_i p_i)\right)}{\frac{d}{d\alpha}(1-\alpha)} = \quad (3)$$

$$= \lim_{\alpha\to\infty} \frac{\frac{d}{d\alpha}(\alpha)}{\frac{d}{d\alpha}(1-\alpha)} \log_2(\max_i p_i) = \frac{1}{-1} \log_2(\max_i p_i) = -\log_2(\max_i p_i)$$

Отримаємо та перевіримо на основі використання виразу для ентропії Реньї вираз для ентропії колізій. Нехай H_2 позначає колізійну ентропію. Нехай також, X та X' – дві незалежні та однаково розподілені випадкові змінні з значеннями в деякій множині Ω. Тоді із виразу для ентропії Реньї (1), при $\alpha = 2$, маємо

$$H_2(X) = \frac{1}{1-2} \log_2 \left(\sum_{\omega\in\Omega} (Pr[X = \omega])^2 \right) = -\log_2 \left(\sum_{\omega\in\Omega} (Pr[X = \omega])^2 \right). \quad (4)$$

Практичні дослідження показують, що має місце таке співвідношення між енропією Шеннона, колізійною і мінімальною ентропією [2, 21]:

$$H_{min} \le H_2 \le H_1, \; H_{min} \le H_2 \le 2H_{min}. \quad (5)$$

Мінімальна ентропія є найбільш консервативною ентропією. На рис. 1 для прикладу зображені H_1, H_2 та H_∞ для бінарних випадкових змінних.

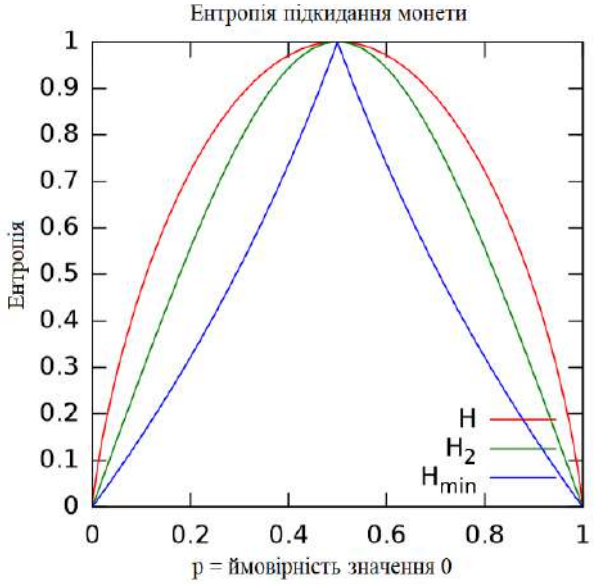


Рис. 1. Мінімальна ентропія, колізійна ентропія та ентропія Шеннона для випадкових бінарних змінних

Таким чином, задаючи значення ймовірностей $Pr[X = \omega_i]$, по кривим рис. 1 перевіряється, чи виконується практично співвідношення між $H_1, H_2, H_{\min}$ та $2H_{min}$. Якщо так, то приймається рішення, що послідовність відповідає ентропійним критеріям випадковості. Після цього етапу, для уточнення, рекомендується провести статистичне тестування, наприклад, з використанням NIST 800-22 [6] та DIEHARD [8].

4. Дослідження ентропій Шеннона, ентропії колізій та мінімальної ентропії ДШ згідно з NIST 800-90B

Методологічні основи оцінки ентропій ВП та ВЧ, що згенеровані PTRNG фізично справжніми генераторами, наведено в [2, 22 – 24]. Нижче наводяться обґрунтовані вище конкретизовані методики оцінки ентропій ВП та ВЧ – Шеннона, колізій та мінімальної ентропій. Вважається, що обґрунтовані та запропоновані нижче методики оцінки повинні (можуть) бути застосовані щодо ДШ (генераторів) як фізично справжніх (PTRNG), так і нефізично справжніх (NPT RNG) ДШ.

4.1. Оцінка ентропії Шеннона ДШ PT RNG та NPT RNG

Для дискретної випадкової змінної X з можливими значеннями $x_0, x_1, ..., x_{k-1}$ та відповідними ймовірностями появи символів ($p_0, p_1, ..., p_{k-1}$), ентропія Шеннона визначена як

$$H(\mathrm{X}) = -\sum_{i=0}^{k-1} p_i \cdot \log p_i \,. \tag{6}$$

Надалі позначатимемо частоту появи символу x_i у вибірці розміру n як $n(\mathrm{x}_i)$ та відповідну емпіричну ймовірність $p_i = n(x_i)/n$.

Якщо застосовувати формулу (6) напряму до реальних статистичних даних, то оцінка буде зміщеною [25, 26]. Щоб отримати незміщену оцінку, можливо використовувати корекцію, зокрема наступні методи корекції, що задані формулами (7) – (9) [27]:

$$\hat{H}(X) = H(X) + \frac{m-1}{2n}, \tag{7}$$

де m – кількість різних символів, що зустрілися в статистичних даних, n – розмір вибірки;

$$\hat{H}(X) = n \cdot H(X) - \frac{n-1}{n} H_{-i}(X), \tag{8}$$

де $H(\mathrm{X})_{-i}$ – це $H(X)$ без доданка $p_i \cdot \log p_i$;

$$\hat{H}(X) = -\sum_{i=0}^{n-1} a_i \cdot h_i \,. \tag{9}$$

Також $h_i = \sum_{j=1}^{k-1} [[p_j \cdot n == i]]$ та $a_i = -\frac{i}{n}\log\frac{i}{n} + \left(1 - \frac{i}{n}\right)$ (тут $[[\cdot]]$ позначає предикат).

Для зручності надалі будемо використовувати позначення MM для формули (8), JKF для формули (8) та BUB для формули (9).

Інший підхід до усунення зміщення полягає у використанні формули Баєса [28]:

$$\hat{H}(X) = -\sum_{i=0}^{k-1} \frac{p_i \cdot n + a_i}{n + A} \log\left(\frac{p_i \cdot n + a_i}{n + A}\right), \tag{10}$$

де $A = \sum_{i=0}^{k-1} a_i$, а значення a_i обираються в залежності від конкретного метода. Зокрема, часто $a_0 = a_1 = ... a_{k-1} = const$. Найбільш популярні вибори констант наступні [25, 28]:

- $a_i = 1/2$;
- $a_i = 1$;
- $a_i = 1/k$;
- $a_i = \sqrt{n}/k$.

З експериментальних досліджень у роботах [25, 29, 30] також варто виділити наступні три перспективні підходи до оцінки ентропії Шеннона:

- Підхід, що був запропонований у роботі [31] (надалі – SHU-оцінка). Значення ентропії визначається за формулою

$$\hat{H}(X) = \psi(n) - \frac{1}{n}\sum_{i=0}^{k-1}\left(\psi(p_i \cdot n) + (-1)^{p_i \cdot n}\int_0^{1/\xi-1}\frac{t^{p_i \cdot n-1}}{1+t}dt\right). \quad (11)$$

- Підхід, що був запропонований у роботі [32] (надалі – CS-оцінка). Значення ентропії визначається за формулою

$$\hat{H}(X) = -\sum_{i=0}^{k-1}\frac{\tilde{p}_i \log \tilde{p}_i}{1-(1-\tilde{p}_i)^n}, \quad (12)$$

де $\tilde{p}_i = \left(1-\frac{m}{n}\right)p_i$.

- Підхід, що був запропонований у роботі [33] (надалі – SHR-оцінка). Значення ентропії визначається за формулою

$$\hat{H}(X) = -\sum_{i=0}^{k-1}\tilde{p}_i \log \tilde{p}_i, \quad (13)$$

де $\tilde{p}_i = \lambda / k + (1-\lambda)\mathrm{p}_i$, причому

$$\lambda = \frac{1-\sum_{i=0}^{k-1}(p_i)^2}{(n-1)\sum_{i=0}^{k-1}(1/k - p_i)^2}.$$

Також можливо виділити ряд інших методів оцінки ентропії Шеннона, що використовують більш складні статистичні методи, проте вони не набули широкого поширення через складність реалізації.

4.1.1. Експериментальна перевірка ентропії Шеннона

Для тестування методів оцінки ентропії Шеннона було написане програмне забезпечення, що генерує випадкові послідовності із заданою мінімальною ентропією (і відповідною ентропією Шеннона). Для цього генерується випадкова бінарна послідовність з рівномірного розподілу і до послідовності застосовується вибірка з відхиленням. Нехай p позначає ймовірність появи 1. Тоді, мінімальна ентропія, згідно з визначенням буде

$$H_{min} = \max(p, 1-\mathrm{p}).$$

І відповідна ентропія Шеннона

$$H = -p \cdot \log_2 p - (1-p)\cdot \log_2(1-p).$$

На рис. 2 наведено експериментальні дані оцінки мінімальної ентропії бінарних послідовностей для $p = \{0.5, 0.6, 0.7, .0.8, 0.9\}$ на послідовності довжини 10^6 біт.

З рис. 2 видно, що усі методи дають гарну оцінку ентропії як для високоентропійних послідовностей, так і для низькоентропійних послідовностей.

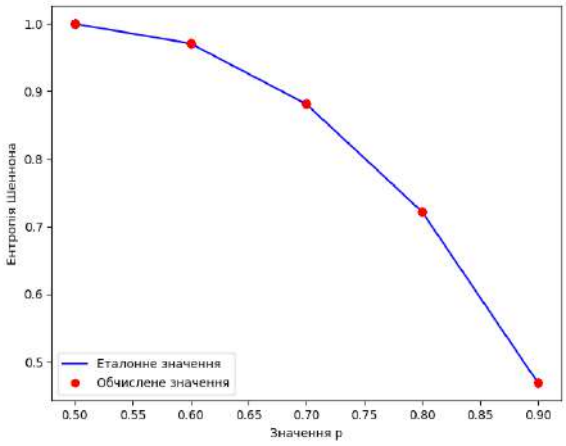


Рис. 2. Експериментальна оцінка ентропії Шеннона

4.2. Оцінка колізійної ентропії ДШ (ВП, ВЧ)

Колізійна ентропія визначена наступним чином:

$$H_2(X) = -\log\left(\sum_{i=0}^{k-1} p_i^2\right). \tag{14}$$

Для колізійної ентропії відомі наступні обмеження нерівностями:

$$H_{min} \le H_2 \le H\,, \tag{15}$$

$$H_{min} \le H_2 \le 2H_{min}\,. \tag{16}$$

Для практичних задач нерівностей, на нашу думку, достатньо, щоб оцінити значення колізійної ентропії, маючи оцінки мінімальної ентропії та ентропії Шеннона.

Для більш точних оцінок можливо скористатися методом, що описаний у роботі [34].

Метод залежить від двох параметрів – параметра точності оцінки δ та параметра статистичної помилки ò. Нехай деяка константа M, що гарантовано має значення більше за будь-яке можливе значення колізійної ентропії та довільна константа $c > 0$. Наприклад, $M = H(X)$ або $M = 2H_{min}(X)$. Тоді, можливо використовувати наступний алгоритм:

1. Обрати розмір блоку $N = \left\lceil c \cdot 2^{M/2} \delta^{-2} \right\rceil$
2. Обчислити кількість блоків $l = \lfloor n / N \rfloor$
3. Для $j = 1, \ldots, n/N$
   a. Для $i \in \{(j-1)N+1, \ldots, (j-1)N\}$
      i. $n(x_{i+1}) = n(x_i) + 1$
   b. $q_j = \dfrac{1}{m(m-1)}\left(\sum_{i=0}^{k-1} n(i)^2 - m\right)$
4. Знайти медіану q послідовності $q_1, \ldots, q_l$
5. Повернути $-\log q$

Метод доказово оцінює значення колізійної ентропії з похибками $(\delta, \grave{o})$, якщо $c \ge \log(1/\grave{o})$.

4.2.1. Експериментальна перевірка колізійної ентропії

Для експериментальної перевірки розглянутого методу для оцінки було використано таку ж методику, як і для ентропії Шеннона. Для заданого значення p колізійна ентропія визначається як

$$H_2 = -\log_2(\mathrm{p}^2 + (1-p)^2)\,.$$

На рис. 3 наведено експериментальні дані оцінки колізійної ентропії бінарних послідовностей для $p = \{0.5, 0.6, 0.7, .0.8, 0.9\}$ на послідовності довжини 10^6 біт.

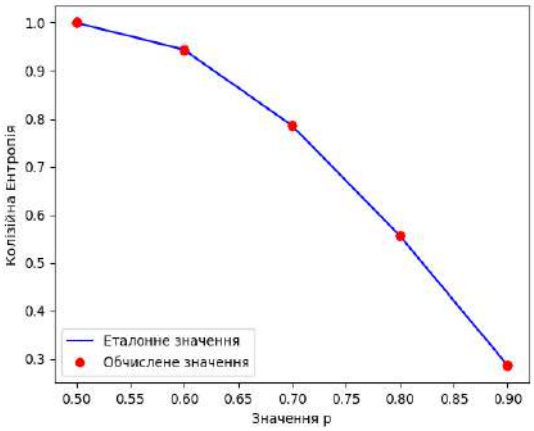


Рис. 3. Експериментальна перевірка оцінки колізійної ентропії

З рис. 3 видно, що усі методи дають гарну оцінку ентропії як для високоентропійних послідовностей, так і для низькоентропійних послідовностей.

4.3. Оцінка мінімальної ентропії ДШ (ВП, ВЧ)

Для дискретної випадкової змінної X з можливими значеннями $x_0, \mathrm{x}_1, ..., x_{k-1}$ (та відповідними ймовірностями $p_0, \mathrm{p}_1, ..., p_{k-1}$) мінімальна ентропія визначена як

$$H_{min}(X) = -\log_2\left(\max_{1\le i\le k}\{\mathrm{p}_i\}\right). \qquad (17)$$

Окрім позначення $H_{min}(\cdot)$ для мінімальної ентропії, також є популярним позначенням $H_\infty(\cdot)$.

Для оцінки мінімальної ентропії можливо виділити два основних підходи. Перший підхід базується на ентропійній статистиці, вперше описаний в [35]. Другий підхід базується на предикторах (англ. predictor) (на основі прогнозування), вперше описаних у [36].

Ентропійна статистика призначена для обчислення окремої статистики на вибірках. До методів, що використовують ентропійну статистику, належать:

- колізійний тест;
- тест на стиснення;
- тест Маркова.

Хоча оцінювачі ентропії (за винятком тесту Маркова) спочатку були розроблені для застосування до незалежних виходів, тести показали хороші результати при застосуванні до даних із залежностями.

Оцінювачі ентропії припускають, що розподіл ймовірностей описує вихід випадкового джерела шуму, але розподіл ймовірностей невідомий. Метою кожного оцінювача є виявлення інформації про невідомий розподіл на основі статистичних вимірювань.

Тести колізій та стиснення розв'язують рівняння для невідомого параметра, де рівняння є різними для кожного оцінювача. Ці рівняння походять із очікуваного значення цільової статистики з використанням майже рівномірного розподілу, який забезпечує нижню межу мінімальної ентропії. Майже рівномірний розподіл є прикладом однопараметричного сімейства розподілів ймовірностей, параметризованих p, P_p:

$$P_p(i) = \begin{cases} p, \text{ якщо i=0} \\ \dfrac{1-p}{k-1}, \text{ інакше} \end{cases}, \quad (18)$$

де k – кількість станів у вихідному просторі, а $p \geq \dfrac{1-p}{k-1}$, що має місце, коли $p \geq 1/k$. Іншими словами, один вихідний стан має максимальну ймовірність, а решта вихідних станів рівноймовірні.

Підхід на основі предикторів використовує два показники для отримання оцінки. Перший показник базується на глобальній продуктивності предиктора P_{global}, яка в літературі з машинного навчання називається точністю. По суті, предиктор фіксує частку правильних припущень. Це приблизно вказує на те, наскільки добре можна очікувати, що предиктор вгадає наступний вихід із джерела шуму на основі результатів довгої послідовності припущень. Другий показник P_{local} базується на найбільшій кількості правильних передбачень у рядку, який називається локальним показником ефективності. Ця метрика корисна для виявлення випадків, коли джерело шуму переходить у дуже передбачуваний стан протягом деякого часу, але предиктор може не працювати добре на довгих послідовностях. Розрахунки для оцінки локальної ентропії походять з теорії ймовірностей пробігів і повторюваних подій [37]. Для отримання додаткової інформації про оцінку мінімальної ентропії за допомогою предикторів див. [11].

Для того щоб оцінки предиктора схилялися до консервативної недооцінки мінімальної ентропії, P_{global} замінюється на P'_{global}, що відповідає 99-му квантилю кількості правильних прогнозів на основі спостережуваної кількості правильних прогнозів. Зауважимо, що порядок, у якому відбуваються правильні прогнози, не впливає на оцінку мінімальної ентропії на основі P_{global}. Наприклад, прогноз завжди може бути правильним для першої половини вихідних даних у наборі даних і завжди неправильним для другої половини вихідних даних. Оцінка мінімальної ентропії цієї послідовності на основі P_{global} становить половину довжини даних у бітах. З іншого боку, для іншої послідовності предиктор може мати 50 % шанс бути правильним для кожного зразка в цій послідовності. Мінімальна оцінка ентропії цієї другої послідовності, заснована на P_{global}, така ж, як і для першої послідовності. Однак типова тривалість успішного прогнозування для цих двох послідовностей дуже різна. Таким чином, цей підхід враховує ефективність локального передбачення, щоб консервативно зменшити оцінку мінімальної ентропії, якщо спостережувана поведінка локального передбачення є статистично значущою, враховуючи глобальний рівень успіху передбачення. Оцінки предикторів досягають цього, базуючи оцінку мінімальної ентропії на $\max(P'_{global}, P_{local})$, де P_{local} – це частка успішного прогнозу, для якої спостережуваний найдовший ряд правильних прогнозів становить 99 %. Фактично це одностороння перевірка гіпотези, яка відхиляє P'_{global} на користь P_{local}, якщо спостережуваний найдовший пробіг, враховуючи ймовірність успіху P'_{global}, перевищує 99 %.

4.3.1. Експериментальна перевірка методів оцінки мінімальної ентропії

Для експериментальної перевірки використовувалася така ж сама методологія як і для ентропії Шеннона та колізійної ентропії.

На рис. 4. наведено експериментальні дані оцінки колізійної ентропії бінарних послідовностей для $p = \{0.5, 0.6, 0.7, .0.8, 0.9\}$ на послідовності довжини 10^6 біт.

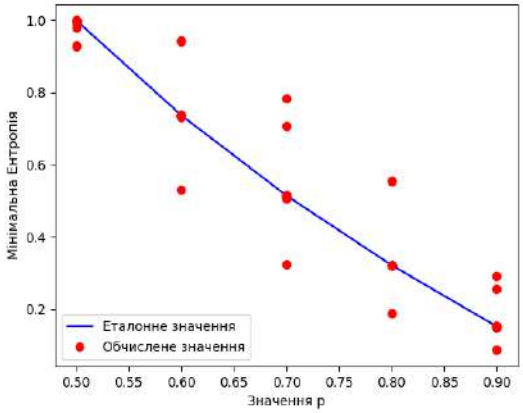


Рис. 4. Експериментальна перевірка оцінки мінімальної ентропії

З експериментальних даних видно, що для бінарних низькоентропійних даних оцінка стиснення може давати занижені значення мінімальної ентропії. У той же час тести оцінки прогнозування затримки та оцінки найдовшого повторюваного підрядка дають завищене значення ентропії. Причому ці зміщення в оцінках не зникають зі збільшенням вибірки.

4.4. Загальні рекомендації до оцінки ентропії Шеннона, колізійної мінімальної ентропії

На рис. 5 зведено дані експериментальних досліджень ентропії, що наведені вище на рис. 2 – 4.

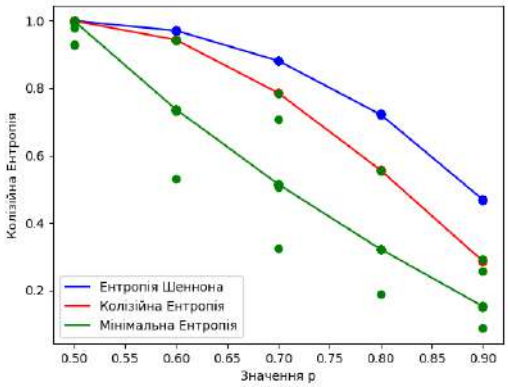


Рис. 5. Експериментальна оцінка ентропії

З отриманих даних випливає, що ентропію Шеннона та колізійну ентропію можливо оцінити доволі точно, у той час як мінімальну ентропію оцінити складніше. Проте, мінімальна ентропія є важливим показником для багатьох практичних застосувань, тому має сенс доповнювати оцінки мінімальної ентропії оцінками ентропії Шеннона та колізійної ентропії, якщо спостерігається розбіжність в отриманих оцінках мінімальної ентропії. Це є актуальним здебільшого для низькоентропійних джерел шуму.

Висновки

1. Ентропія Шеннона та колізійна ентропія можуть бути легше оцінені на практиці, ніж мінімальна ентропія. Проте, мінімальна ентропія має багато важливих застосувань. Тому для більш точних оцінок має сенс комбінувати оцінки мінімальної ентропії та ентропії Шеннона і колізійної ентропії.

2. Окремі статистичні тести NIST SP 800-90B на низькоентропійних даних можуть давати значно занижені або завищені значення. Проте, експериментальні оцінки показують, що зміщене значення не перевищує значення колізійної ентропії.

3. Для оцінки ентропії важливо, щоб кількість статистичного матеріалу була достатньо великою. Це важливо враховувати при тестуванні джерел шуму. Ентропія Реньї є найбільш загальною формою ентропії, проте для практичних застосувань є цікавими її властивості при значеннях параметра $\alpha = 1, 2, \infty$, що відповідають випадкам ентропії Шеннона, колізійної ентропії та мінімальної ентропії відповідно.

4. Існує два основних підходи до оцінки мінімальної ентропії: на основі ентропійної статистики та на основі передбачення. Тести ентропійної статистики призначені для обчислення окремої статистики на вибірках. До методів, що використовують ентропійну статистику, належать: колізійний тест, тест на стиснення, тест Маркова. Такі оцінювачі ентропії припускають, що розподіл ймовірностей описує вихід випадкового джерела шуму, але розподіл ймовірностей невідомий. Метою кожного оцінювача є виявлення інформації про невідомий розподіл на основі статистичних вимірювань.

5. Підхід прогнозування використовує два показники для отримання оцінки. Перший показник базується на глобальній продуктивності предиктора, яка в літературі з машинного навчання називається точністю. По суті, предиктор фіксує частку правильних припущень. Це приблизно вказує на те, наскільки добре можна очікувати, що предиктор вгадає наступний вихід із джерела шуму на основі результатів довгої послідовності припущень. Другий показник базується на найбільшій кількості правильних передбачень у рядку, який називається локальним показником ефективності. Ця метрика корисна для виявлення випадків, коли джерело шуму переходить у дуже передбачуваний стан протягом деякого часу, але предиктор може не працювати добре на довгих послідовностях.

6. Ентропія Шеннона та колізійна ентропія можуть бути легше оцінені на практиці, ніж мінімальна ентропія. Проте, мінімальна ентропія має багато важливих застосувань. Тому для більш точних оцінок має сенс комбінувати оцінки мінімальної ентропії та ентропії Шеннона і колізійної ентропії. Окремі статистичні тести NIST SP 900-80B на низькоентропійних даних можуть давати значно занижені або завищені значення. Проте, експериментальні оцінки показують, що зміщене значення не перевищує значення колізійної ентропії.

7. Головним завданням оцінок як PTRNG, так і NPTRNG є перевірка того, що (середня) ентропія на один біт внутрішнього випадкового числа перевищує задану нижню межу. Важливою відмінністю між PTRNG і NPTRNG, яка впливає на глибину оцінювання, є те, що джерело фізичного шуму в PTRNG знаходиться «під контролем» розробника RNG, а джерело нефізичного шуму NPTRNG зазвичай не може контролюватися.

8. Наразі, у більшості випадків застосування, перевага надається джерелам шуму на основі PTRNG, аніж на основі NPTRNG. По-перше, джерела шуму, які використовують NPTRNG, часто працюють добре лише за певних обставин, а NPTRNG часто не в змозі перевірити, чи виконуються ці умови. По-друге, оцінка ентропії зазвичай базується на складних припущеннях щодо знань і можливостей зловмисника і оперативного середовища.

9. Значення мінімальної ентропії, ентропії Шеннона та колізійної ентропії є основними критеріями якості джерела шуму. Причому, для визначення точних оцінок має сенс використовувати декілька різних оцінок.

10. Генератор ВП ОС Linux для генерації свіжої ентропії використовує події переривань, блочних пристроїв та пристроїв вводу. Основну ентропію містять мітки часу відповідних подій.

11. Набір статистичних тестів NIST STS 800-22 та методика проведення статистичного тестування, що орієнтовані на використання у задачах криптографічного захисту інформації, на даний момент найкраще відповідає потребам усіх сторін.

12. Набір статистичних тестів DIEHARD розроблений для аналізу якості послідовності випадкових чисел. Тести DIEHARD вважаються одним з найжорсткіших існуючих наборів тестів. Набір тестів DIEHARDER дозволяє прийняти однозначне рішення про відмову від «слабкого генератора» (наприклад, на рівні 0,0001 %), а не з ймовірністю відмови 1 або 5 %.

Список літератури:

1. Закон України «Про електронні довірчі послуги» від 1 січня 2024 року N 2155-VIII. [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/2155-19#Text.
2. BSI AIS 31. A Proposal for Functionality Classes for Random Number Generators, September 2022. Режим доступу: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Certification/Interpretations/AIS_31_Functionality_classes_for_random_number_generators_e.pdf?__blob=publicationFile&v=7.
3. NIST SP 800-90 A, Revision 1: E. Barker, J. Kelsey: Recommendation for Random Number Generators Using Deterministic Random Bit Generators. June 2015. Режим доступу: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf.
4. NIST SP 800-90 B: M. Turan, E. Barker, J. Kelsey, K. McKay, M. Baish, M. Boyle: Recommendation for the Entropy Sources Used for Random Bit Generation. January 2018. Режим доступу: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90B.pdf.
5. NIST SP 800-90 C, Third Draft: E. Barker, J. Kelsey: Recommendation for Random Bit Generator (RBG) Constructions. September 2022. Режим доступу: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90C.3pd.pdf.
6. Federal Information Processing Standard (FIPS) 140-2. Security Requirements for Cryptographic Modules 2002. Режим доступу: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf.
7. NIST SP 800-22, Revision 1a: A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, S. Vo, (revision) L. Bassham: A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, April 2010. Режим доступу: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-22r1a.pdf.
8. DIEHARDER – A testing and benchmarking tool for random number generators. [Електронний ресурс]. Режим доступу: https://manpages.ubuntu.com/manpages/focal/man1/dieharder.1.html.
9. Горбенко Ю. І. Побудування та аналіз систем, протоколів і засобів криптографічного захисту інформації : монографія. Ч. 1: Методи побудування та аналізу, стандартизація та застосування криптографічних систем ; за заг. ред. І. Д. Горбенко. Харків : Форт, 2016. 960 с.
10. Urandom – Linux main page. [Електронний ресурс]. Режим доступу: https://linux.die.net/man/4/urandom.
11. Microsoft Documentation. CryptGenRandom function (wincrypt.h). 2021. [Електронний ресурс]. Режим доступу: https://learn.microsoft.com/en-us/windows/win32/api/wincrypt/nf-wincrypt-cryptgenrandom.
12. ДСТУ ISO/IEC 14888-3:2019 Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Ч. 3. Механізми на основі дискретного логарифмування (ISO/IEC 14888-3:2018, IDT).
13. ДСТУ 4145-2002 Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння.
14. ДСТУ 7564:2014 Інформаційні технології. Криптографічний захист інформації. Функція гешування. З поправкою.
15. ДСТУ 7624:2014 Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення. З поправкою.
16. ДСТУ 8845:2019 Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного потокового перетворення.
17. ДСТУ 8961:2019 Інформаційні технології. Криптографічний захист інформації. Алгоритми асиметричного шифрування та інкапсуляції ключів.
18. ДСТУ 9212:2024 Інформаційні технології. Криптографічний захист інформації. Алгоритм електронного підпису на алгебраїчних решітках із відхилами.
19. Goldreich O. Foundations of Cryptography: Vol. 1. Cambridge University Press, September 2006. [Електронний ресурс]. Режим доступу: https://dl.acm.org/doi/10.5555/1202577.
20. «Меморандум про національну безпеку з просування лідерства США в галузі квантових обчислень при одночасному зниженні ризиків для вразливих криптографічних систем». [Електронний ресурс]. Режим доступу: https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/.
21. A. Rényi On measures of information and entropy // Proceedings of the 4th Berkeley Symposium on Mathematics, Statistics and Probability 1960, p. 547; Probability Theory, North-Holland, Amsterdam, 1970.
22. ISO/IEC 20543 Information technology – Security Techniques. Test and Analysis Methods for Random Bit Generators within ISO/IEC 19790 and ISO/IEC 15408. 2019.
23. Common Methodology for Information Technology Security Evaluation, Evaluation methodology, Version 3.1, Revision 4, September 2012. Режим доступу: https://www.commoncriteriaportal.org/files/ccfiles/CEMV3.1R4.pdf.
24. Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 2.3, August 2005. Режим доступу: https://www.commoncriteriaportal.org/files/ccfiles/cemv2.3.pdf.
25. Rodríguez L., Madarro-Capó E.,Legón-Pérez C., Rojas O., Sosa-Gómez G. Selecting an Effective Entropy Estimator for Short Sequences of Bits and Bytes with Maximum Entropy. [Електронний ресурс]. Режим доступу:

https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8147137/.
26. Skorski M. Improved Estimation of Collision Entropy in High and Low-Entropy Regimes and Applications to Anomaly Detection. Режим доступу: https://eprint.iacr.org/2016/1035.pdf.
27. Paninski L. Estimation of entropy and mutual information. Neural Comput. 2003;15:1191–1253. Режим доступу: doi: 10.1162/089976603321780272.
28. Trybula S. Some problems of simultaneous minimax estimation. Ann. Math. Stat. 1958;29:245–253. Режим доступу: doi: 10.1214/aoms/1177706722.
29. Hausser J., Strimmer K. Entropy inference and the james-stein estimator, with application to nonlinear gene association networks // J. Mach. Learn. Res. 2009;10:1469–1484.
30. Valiant G., Valiant P. Estimating the unseen: Improved estimators for entropy and other properties // J. ACM. 2017; 64:1–41. Режим доступу: doi: 10.1145/3125643.
31. Schürmann T. Bias analysis in entropy estimation // J. Phys. A. Math. Gen. 2004;37:L295. Режим доступу: doi: 10.1088/0305-4470/37/27/L02.
32. Chao A., Shen T.J. Nonparametric estimation of Shannon's index of diversity when there are unseen species in sample // Environ. Ecol. Stat. 2003;10:429–443. Режим доступу: doi: 10.1023/A:1026096204727.
33. Hausser J., Strimmer K. Entropy inference and the james-stein estimator, with application to nonlinear gene association networks // J. Mach. Learn. Res. 2009; 10:1469–148.
34. Skorski M. Improved Estimation of Collision Entropy in High and Low-Entropy Regimes and Applications to Anomaly Detection. Режим доступу: https://eprint.iacr.org/2016/1035.pdf.
35. P. Hagerty and T. Draper, Entropy Bounds and Statistical Tests, NIST Random Bit Generation Workshop, December 2012. Режим доступу: https://csrc.nist.gov/csrc/media/events/random-bit-generation-workshop-2012/documents/hagerty_entropy_paper.pdf.
36. J. Kelsey, Kerry A. McKay, M. Sonmez Turan, Predictive Models for Min-Entropy Estimation // Proceedings of the Workshop on Cryptographic Hardware and Embedded Systems 2015 (CHES 2015), France. Режим доступу: https://doi.org/10.1007/978-3-662-48324-4_19.
37. U. Maurer, A Universal Statistical Test for Random Bit Generators // Journal of Cryptology. 1992. Vol. 5, No. 2. P. 89–105.
38. C.E Shannon, Prediction and Entropy of Printed English // Bell System Technical Journal. Vol. 30, January 1951. [Електронний ресурс]. Режим доступу: https://archive.org/details/bstj30-1-50.
39. Quantis QRNG USB. [Електронний ресурс]. Режим доступу: https://www.idquantique.com/random-number-generation/products/quantis-random-number-generator/.

Надійшла до редколегії 15.01.2024

Відомості про авторів:
Голубничий Дмитро Юрійович – канд. техн. наук, доцент, АТ "Інститут Інформаційних Технологій", начальник наукового відділу; Україна; e-mail: goldim1971@gmail.com; ORCID: https://orcid.org/0000-0002-6873-7004
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", науковий співробітник-консультант; Україна; e-mail: sergeykandy@gmail.com
Єсіна Марина Віталіївна – канд. техн. наук, доцент, Харківський національний університет імені В. Н. Каразіна, доцент кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук, АТ «Інститут Інформаційних Технологій», науковий співробітник-консультант; Україна; e-mail: m.v.yesina@karazin.ua; ORCID: https://orcid.org/0000-0002-1252-7606
Горбенко Дмитро Юрійович – Харківського національного університету імені В. Н. Каразіна. студент факультету комп'ютерних наук, АТ "Інститут Інформаційних Технологій", молодший інженер-програміст; Україна; e-mail: jsciitua@gmail.com

УДК 004.05 **DOI:10.30837/rt.2024.1.216.03**

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

СУЧАСНІ ЗАГРОЗИ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИМ СИСТЕМАМ ТА МЕТОДИ ЗАХИСТУ ВІД НИХ

Вступ

У сучасному світі інформація стає одним з найважливіших ресурсів, а інформаційно-комунікаційні системи (ІКС) – невід'ємною частиною життя суспільства. Завдяки ІКС відбувається обробка, зберігання та передача інформації, що робить їх надзвичайно вразливими до різноманітних загроз.

Загрози для нормального функціонування ІКС постійно еволюціонують, стаючи все більш складними та небезпечними. Це робить актуальним дослідження та розробку нових методів та засобів захисту інформації, а також підвищення обізнаності користувачів ІКС щодо кіберзагроз.

Метою статті є дослідження сучасних загроз для нормального функціонування ІКС, а також розробка рекомендацій щодо підвищення рівня інформаційної безпеки (ІБ). Для досягнення поставленої мети необхідно виконати такі завдання:

- проаналізувати теоретичні основи інформаційної безпеки ІКС;
- вивчити та класифікувати сучасні загрози для інформації та ІКС;
- дослідити методи та засоби захисту інформації та ІКС;
- розробити рекомендації щодо підвищення рівня інформаційної безпеки ІКС.

Об'єктом дослідження є сучасні загрози для нормального функціонування ІКС. Предметом дослідження є методи та засоби захисту ІКС.

1. Класифікація і джерела загроз ІБ ІКС

Загрозу можна розглядати як атаку та можливість порушення ІБ і посягання на заволодіння інформацією, а той, хто посягає на інформацію, є зловмисником. Загрози проявляються через низький захист або знаходження вразливих місць у системі захисту ІКС [1]. Загрози інформаційної безпеки класифіковані за різними ознаками. Розглянемо це питання детальніше.

Рис. 1. Класифікація загроз для ІКС

На рис. 1 наведена класифікація загроз, що складається з п’яти основних класів, які включають в себе від двох до трьох підкласів. Першим з класів є загроза за основними принципами тріади з кібербезпеки: конфіденційності, цілісності й доступності. Очевидно, що загрози цього класу спрямовані на порушення нормального дотримання цих властивостей інформації.

Іншим, не менш цікавим класом, є визначення за джерелами загроз: внутрішніми (тими, що знаходяться всередині системи) й зовнішніми (знаходяться поза системою). Саме загрози цього класу розвиваються невпинно й постійно модернізуються.

Також виділяються загрози ІБ за розмірами нанесеної шкоди: від загальних (заподіяння шкоди об’єкту в цілому) до приватних (заподіяння шкоди деяким властивостям певного елемента об’єкта). Також ступінь впливу також підлягає таксономічним процесам: виділяють загрози пасивного й активного ступеню.

Останній з класів полягає в окресленні загрози за природою виникнення. Існують природні й штучні загрози, з природними все чітко й зрозуміло – загрози, викликані впливом на інформаційне середовище об’єктивних фізичних процесів або стихійних природних явищ, що не залежать від волі людини [1]. Щодо штучної природи виникнення – підклас розгалужується на ненавмисні й умисні загрози.

Стаття 1 Закону України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII надає чітку різницю між навмисними й ненавмисними загрозами, шляхом введення понять «кібератака» й «інцидент кібербезпеки (кіберінцидент)». Розглянемо ці визначення.

Кіберінцидент – подія або ряд несприятливих подій ненавмисного характеру та/або таких, що мають ознаки можливої кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем, ставлять під загрозу безпеку електронних інформаційних ресурсів [2].

Кібератака – спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об’єкти кіберзахисту [2].

Дійсно, визначення кіберінциденту й кібератаки повністю відповідають розгалуженням підкласу «штучні» класу загроз ІБ за природою виникнення.

2. Аналіз сучасних загроз

2.1. Внутрішні загрози

Основоположні вимоги до джерел шуму та його ентропії було запропоновано в Внутрішні загрози. Помилки та необережність персоналу, а також недосконаліть внутрішніх процесів та процедур можуть виникати через внутрішні недоліки управління, недостатню увагу до внутрішньої безпеки та недостатню освіченість персоналу щодо правил та процедур безпеки. Розглянемо внутрішні загрози ІБ у сучасному контексті детальніше.

Першим видом внутрішніх загроз є зловмисні інсайдерські загрози [3]. Основними цілями зловмисних таких загроз є шпигунство, шахрайство, крадіжка інтелектуальної власності та саботаж. Вони навмисно зловживають своїм службовим становищем, щоб викрасти інформацію або погіршити роботу системи з фінансових, особистих та/або зловмисних причин. Варто зазначити, що такі загрози можуть бути як колабораціоністського характеру, так і незалежного.

Спільники – це авторизовані користувачі, які працюють з третьою стороною, щоб навмисно завдати шкоди організації. Третьою стороною може бути конкурент, інша держава, організована злочинна мережа або фізична особа. Дії колаборациониста можуть призвести до витоку конфіденційної інформації або порушення бізнес-операцій. Під час незалежного характеру, навпаки, діють повністю самостійно і без зовнішніх маніпуляцій або впливу. Такі загрози можуть бути особливо небезпечними, оскільки зловмисники часто мають спеціальний доступ до ІКС.

Іншим видом сучасних внутрішніх загроз є загрози, що спричиняються недбалим ставленням. Вони часто є наслідком людської помилки, неправильного судження, ненавмисного сприяння та допомоги, фішингу, шкідливого програмного забезпечення (ШПЗ) і викрадених облікових даних. Співробітник несвідомо наражає корпоративні системи на зовнішню атаку. Таких співробітників також можна розділити на два види: пішаки (англ. Pawn) і дурні (англ. Goof) [3].

«Пішаки» – це авторизовані користувачі, якими маніпулюють, аби вони ненавмисно діяли зловмисно, часто за допомогою методів соціальної інженерії. Ці ненавмисні дії можуть включати завантаження ШПЗ на комп'ютер або розкриття конфіденційної інформації сторонній особі.

«Дурні» навмисно здійснюють потенційно шкідливі дії, але не мають злого наміру. Це зарозумілі, необізнані та/або некомпетентні користувачі, які не визнають необхідності дотримуватися політик і процедур безпеки. «Дурнем» може бути користувач, який зберігає конфіденційну інформацію про клієнтів на своєму персональному пристрої, навіть, якщо він знає, що це суперечить політиці організації.

Також, поза категорією знаходяться так звані «кроти». «Кроти» – це сторонні особи, які отримали інсайдерський доступ до систем організації. «Кріт» може видавати себе за постачальника, партнера, підрядника або працівника, отримуючи таким чином привілейовані повноваження, на які в іншому випадку він не мав би права претендувати. Загалом, такий вид внутрішньої загрози можна класифікувати як «неавторизований доступ». Узагальнений вигляд внутрішніх загроз у сучасному контексті наявний на рис. 2.

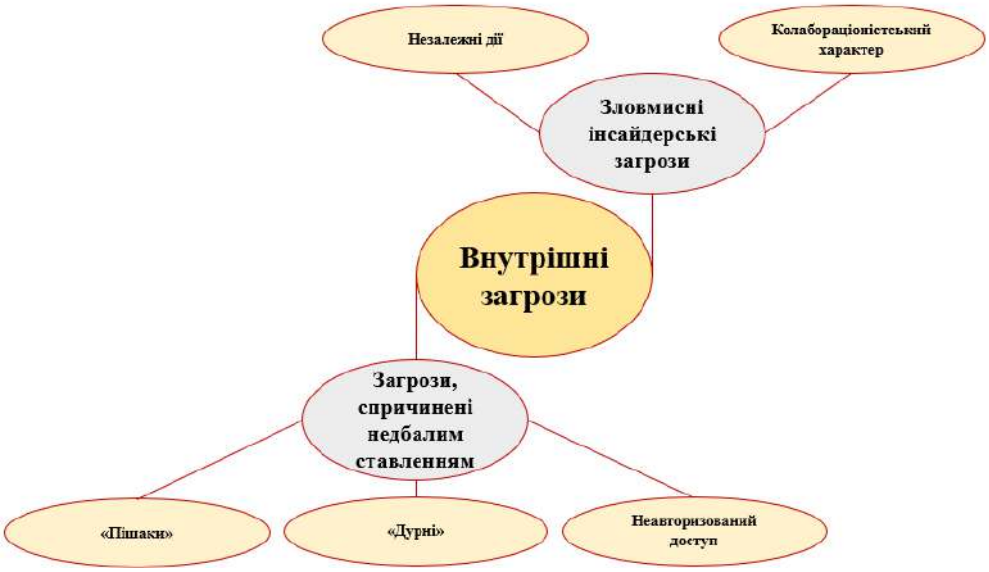


Рис. 2. Узагальнений вигляд внутрішніх загроз

2.2. Зовнішні загрози

Зовнішні загрози включають багато категорій, які виникають поза організацією та спричиняються кимось, хто не має відношення до неї. Зовнішні загрози також можуть бути спрямовані на окремих осіб. Злами або схеми викрадення паролів та онлайн-шахрайства, які спонукають нас добровільно ділитися обліковими даними, спрямовані як на особисті, так і на

корпоративні облікові записи. Зовнішні загрози включають фізичні загрози, такі як втручання в роботу пристроїв або мережі з метою порушення роботи. Зростаючий список хакерських практик, що використовуються для здійснення зовнішніх атак, включає в себе [4]:

• Фішинг.

Фішингова атака, часто у вигляді небажаного електронного листа, спрямована на те, щоб обманом змусити одержувача надати інформацію про свій обліковий запис або паролі. Деякі з них також містять посилання на небезпечні файли або веб-сайти;

• Атака методом грубої сили.

Ця поширена хакерська тактика використовує випадкові комбінації імен користувачів і паролів для спроб входу в ІКС, поки не буде знайдено збіг. Штучний інтелект (ШІ) і автоматизація дозволяють кіберзлочинцям легше здійснювати такі атаки;

• Атака «man in the middle».

Атаки типу MitM часто намагаються здійснити в місцях з незахищеним Wi-Fi з'єднанням, наприклад в аеропортах і готелях. Хоча цей тип атак зустрічається відносно рідко, кіберзлочинці можуть перехоплювати комунікації або перенаправляти користувачів на фальшиві веб-сайти, щоб викрасти їхню інформацію;

• Атаки на відмову в обслуговуванні.

Ця форма кіберзлочинності зазвичай спрямована на бізнес, використовує автоматизацію, щоб перевантажити веб-сайт трафіком, доки він врешті-решт не вийде з ладу. Розподілена атака на відмову в обслуговуванні (DDoS-атака) використовує той самий підхід, при цьому надходження трафіку в ІКС відбувається з декількох джерел, що ускладнює його блокування;

• SQL-ін'єкція.

Ін'єкція мовою структурованих запитів використовує шкідливий код, щоб обманом змусити базу даних відображати інформацію, яку не планувалося виставляти на загальний огляд. Ця складна зовнішня загроза вимагає від хакера ретельного вивчення своєї цілі та виявлення вразливих компонентів системи, з яких можна розпочати атаку;

• Атака «Drive-by».

Термін, запозичений з доцифрової епохи, така атака приховує шкідливі програми на, здавалося б, нешкідливих посиланнях або веб-сайтах. Якщо хтось несвідомо натискає на одне з таких посилань, на пристрій автоматично встановлюється ШПЗ без його відома. Можна провести зв’язок між цим підтипом зовнішньої загрози та підтипом внутрішньої загрози «пішак» з попереднього підрозділу.

Іншим великим підрозділом зовнішніх загроз інформації та нормальній роботі ІКС є ШПЗ. ШПЗ може описувати будь-який тип нав'язливого програмного забезпечення (ПЗ), яке призначене для крадіжки даних, пошкодження обладнання або іншого втручання в нормальну роботу комп'ютера. Найпоширенішими типами шкідливих програм є шпигунські програми та програми-вимагачі. Деякі шкідливі програми призначені для викрадення даних або виведення комп'ютерів і пристроїв з ладу [4]. Розглянемо деякі види атак, що спричиняють такі загрози:

• Шпигунські програми.

Ця небезпечна форма ШПЗ встановлюється на пристрій-складову ІКС і починає стежити за активністю користувача з подальшою передачею даних кіберзлочинцю. Шпигунські програми, які важко виявити, можуть використовуватися для збору конфіденційної інформації, наприклад, паролів і номерів кредитних карток;

• Програми-вимагачі.

Ця форма ШПЗ використовується для захоплення пристрою або всієї мережі в заручники, не даючи компаніям або приватним особам отримати доступ до власних файлів, поки не буде сплачено викуп, як правило, за допомогою кредитної картки або криптовалюти.

Варто зазначити, що повільна робота пристрою, незрозумілі спливаючі вікна, незвичні зміни в налаштуваннях браузера або безпеки – це тривожні ознаки атаки ШПЗ. Узагальнено зовнішні загрози наявні на рис. 3.

Рис. 3. Сучасні зовнішні загрози для інформації та ІКС

2.3. Технічні загрози

До технічних загроз можна віднести: атаки на апаратне та програмне забезпечення (розглянуті в попередньому підрозділі), мережеві атаки й атаки на криптографічні алгоритми. Розглянемо це питання детальніше.

Сучасна ІКС – це складна, тісно пов'язана екосистема обладнання, ПЗ, сервісів, комунікаційних протоколів, віртуальних ресурсів і людей. Нині такі системи є основою організацій в усьому світі, тому кібератаки, спрямовані на порушення мережевої безпеки, становлять величезну загрозу для компаній та зацікавлених сторін.

Атаки на мережеву безпеку стають все більш поширеними, дозволяючи зловмисникам пошкодити корпоративні системи та скомпрометувати конфіденційну інформацію. Після проникнення зловмисників через периметр комп'ютерної мережі відбуваються інші кіберзлочини, такі як запуск ШПЗ, атаки з вимогами викупу або атаки на кінцеві точки. Досвідчені кіберзлочинці можуть швидко розширити сферу та масштаб атаки, використовуючи всі вразливості ІКС. Мережеві атаки можуть бути [5]:

- активними: зловмисники отримують несанкціонований доступ до мережі, а потім змінюють дані (наприклад, за допомогою шифрування), щоб скомпрометувати їх і вплинути на їхню зручність та цінність;
- пасивними: кіберзлочинці атакують мережі для моніторингу або викрадення даних, не вносячи до них жодних змін.

Іншим доволі сучасним видом загроз для нормального функціонування ІКС є криптографічні атаки [6].

Криптографічна атака дозволяє зловмисникам обійти захист криптографічної системи, визначивши слабкі місця в її коді, шифрі, криптографічному протоколі або схемі управління ключами. Такий обхід також називається "криптоаналізом". Таким чином, криптографічні атаки націлені на криптографічні або шифрувальні системи, які приховують дані. Залежно від типу криптографічної системи та інформації, доступної зловмиснику, ці атаки можна умовно поділити на шість типів:

- Атаки грубої сили.

При атаці грубої сили зловмисник намагається розшифрувати зашифроване повідомлення або дані, використовуючи різні ключі. Якщо розмір ключа 8-бітний, то можливих ключів буде 256 (тобто 2^8). Для того щоб атака була успішною, зловмисник повинен знати алгоритм (як правило, у вигляді програм з відкритим вихідним кодом), щоб спробувати всі 256 можливих ключів у цій техніці атаки;

• Атака на зашифровані дані.

При цьому векторі атаки зловмисник отримує доступ до колекції зашифрованого тексту. Хоча зловмисник не може отримати доступ до відкритого тексту безпосередньо, він може успішно визначити зашифрований текст з колекції. Цей вид, як правило, менш ефективний, ніж його аналог грубого перебору;

• Атака за обраним відкритим текстом.

За допомогою атаки за обраним відкритим текстом зловмисник може вибрати дані відкритого тексту для отримання зашифрованого тексту, що, своєю чергою, спрощує його завдання з розгадування ключа шифрування;

• Атака за допомогою обраного шифрованого тексту.

У цьому методі зловмисник намагається отримати секретний ключ або дані про систему. Аналізуючи обраний шифрований текст і порівнюючи його з відкритим текстом, зловмисник намагатиметься вгадати ключ;

• Атака за відомим відкритим текстом.

Ця техніка застосовується, коли зловмисник вже знає відкритий текст деяких частин зашифрованого тексту, використовуючи методи збору інформації;

• Атака з використанням подвійного ключа та алгоритму.

Зловмисник намагається відновити ключ, який використовувався для шифрування або розшифрування даних, аналізуючи криптографічний алгоритм.

Окрім цих шести основних типів криптографічних атак, криптографічна атака може бути як пасивною, так і активною. Пасивні криптографічні атаки здійснюються з метою отримання несанкціонованого доступу до конфіденційних даних або інформації шляхом перехоплення або підслуховування загального зв'язку. У цій ситуації дані та комунікація залишаються недоторканими і не піддаються фальсифікації. Активні криптографічні атаки ґрунтуються на модифікації даних або комунікації. У цьому випадку зловмисник не тільки отримує доступ до даних, але й втручається в них. На рис. 4 узагальнена класифікація сучасних технічних загроз.

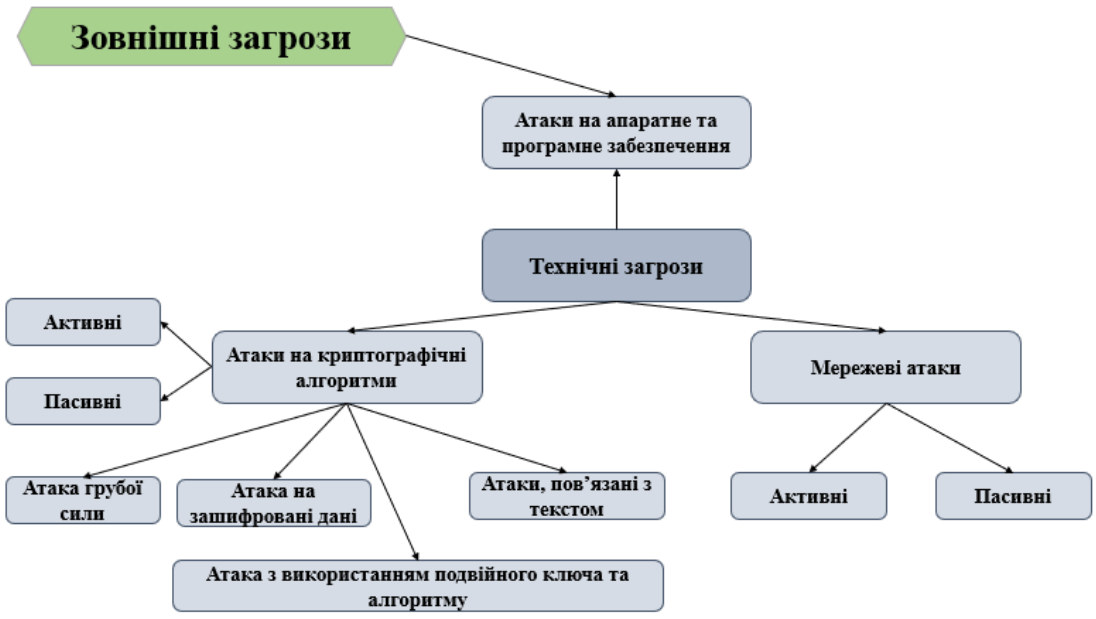


Рис. 4. Узагальнена класифікація сучасні технічних загроз

Варто зауважити, що на рис. 4 до атак на апаратне та програмне забезпечення під'єднані й зовнішні загрози з рис. 3. Ми вважаємо таке уточнення важливим, адже воно підтверджує факт пов'язаності всіх загроз тим чи іншим чином між собою.

Слід зазначити, що детально висвітлені внутрішні, зовнішні та технічні загрози. Також, у ході опису й аналізу стало зрозуміло, що всі три групи загроз тісно переплітаються між

собою: загроза несанкціонованого доступу в різних проявах наявна серед внутрішніх і технічних загроз; атака методом грубої сили входить до підгрупи «атаки на криптографічні алгоритми» технічних загроз й спільної групи «кіберзлочин» для технічних і зовнішніх загроз. Детальна мапа перетину груп, розглянутих загроз наведена на рис. 5.

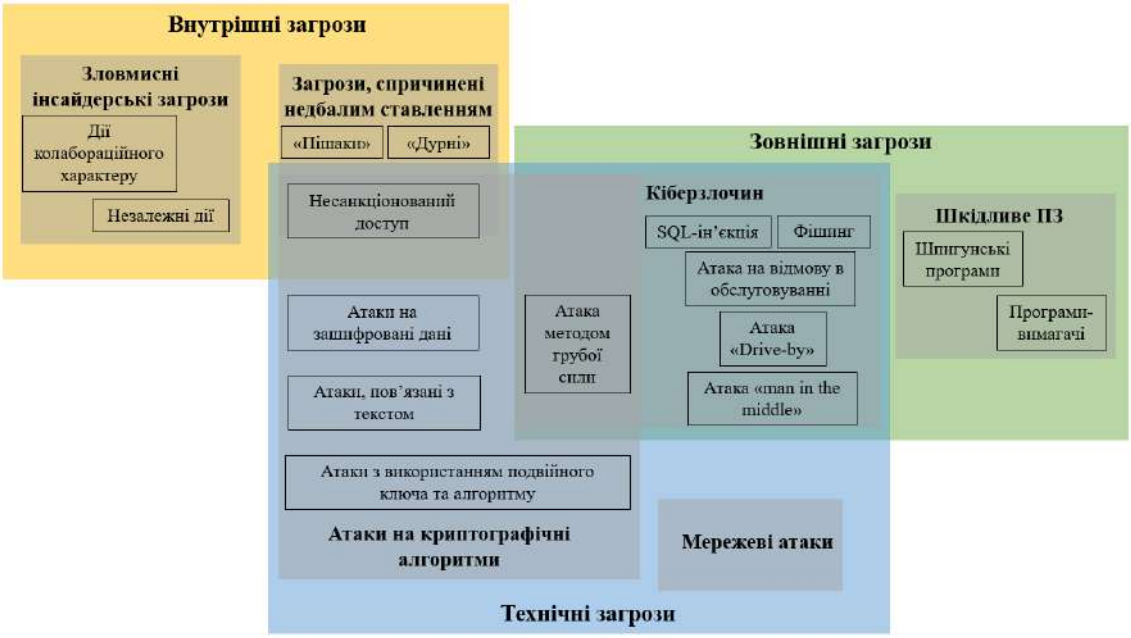


Рис. 5. Мапа перетину сучасних загроз для інформації та нормального функціонування ІКС

3. Методи та засоби захисту інформації

3.1. Класифікація методів та засобів захисту інформації

Класифікація методів та засобів захисту інформації може бути проведена за різними ознаками, такими як вплив на об'єкт захисту та рівень реалізації. Розглянемо ці дві ознаки більш детально. За ознакою впливу на об'єкт захисту, методи та засоби захисту інформації можна поділити на кілька категорій [7]:

1. Фізичні методи та засоби.

Ця категорія включає фізичні засоби захисту, такі як замки, двері, контроль доступу, відеоспостереження, бар'єри та інші заходи, спрямовані на захист фізичного доступу до інформаційних ресурсів та інфраструктури;

2. Програмні методи та засоби.

Ці методи та засоби включають в себе використання ПЗ для захисту інформації. Вони можуть включати у себе антивірусне ПЗ, файєрволи, системи виявлення та захисту від вторгнень (IDS/IPS), системи керування доступом та інші інструменти для запобігання, виявлення та виправлення кіберзагроз;

3. Криптографічні методи та засоби.

Ця категорія включає в себе використання криптографічних методів її алгоритмів для шифрування даних, захисту конфіденційності і цілісності інформації. Криптографічні методи використовуються для створення шифрів, електронних підписів та інших технік для забезпечення безпеки даних;

4. Правові методи та засоби.

Ця категорія включає в себе використання правових норм, законів та стандартів для захисту інформації. Такі методи та засоби можуть включати у себе створення та виконання політик безпеки, регулятивні вимоги до захисту даних, а також правові заходи для покарання осіб, які порушують безпеку інформації.

Кожна з цих категорій має свої особливості та призначення і може бути використана окремо або в поєднанні з іншими методами та засобами для ефективного захисту інформації

та інформаційних ресурсів. Загалом методи та засоби захисту інформації за ознакою впливу на об’єкт можна узагальнити наступним шляхом (рис. 6).

Рис. 6. Узагальнений вигляд методів та засобів захисту інформації за ознакою впливу

Кожен з цих видів методів та засобів захисту має свої особливості та призначення і може бути використаний в залежності від конкретних потреб ІКС чи організації.

3.2. Технічні та організаційні методи та засоби захисту інформації

Забезпечення безпеки інформації є важливим завданням для будь-якої організації чи підприємства в сучасному цифровому світі. Для досягнення цієї мети використовуються різні методи та засоби захисту, які можна розділити на технічні та організаційні. Розглянемо ці категорії з точки зору їх призначення, принципів дії та конкретних прикладів застосування. Почнемо з технічних методів та засобів захисту інформації, до них можна віднести наступне, в узагальненому виді інформація наведена на рис. 7:

- Системи автентифікації та авторизації.

Системи автентифікації та авторизації використовуються для контролю доступу до інформаційних ресурсів. Вони дозволяють перевірити особу користувача та надати йому доступ лише до тих ресурсів, на які він має право;

- Антивірусний захист.

Антивірусний захист використовується для захисту комп'ютерів від ШПЗ. Антивірусні програми сканують комп'ютер на наявність вірусів, троянів, шпигунських програм та інших шкідливих програм;

- Системи захисту даних.

Системи захисту даних використовуються для захисту даних від несанкціонованого доступу, модифікації, знищення або крадіжки;

- Системи виявлення та запобігання вторгнень.

Системи виявлення та запобігання вторгнень використовуються для виявлення та запобігання несанкціонованому доступу до комп'ютерних мереж;

- Мережеві екрани.

Мережеві екрани використовуються для захисту комп'ютерних мереж від несанкціонованого доступу. Мережеві екрани фільтрують трафік, який проходить через них, і дозволяють лише авторизований трафік;

- Системи криптографічного захисту.

Системи криптографічного захисту використовуються для захисту даних від несанкціонованого доступу, модифікації, знищення або крадіжки.

Використання цих методів та засобів може значно підвищити рівень безпеки ІКС. Важливо зазначити, що жоден метод або засіб не може забезпечити 100 % захисту. Тому слід використовувати комплексний підхід до захисту інформації, який включає в себе технічні, організаційні та правові методи.

Рис. 7. Узагальнений вигляд технічних методів і засобів захисту інформації

Наступним блоком є опис організаційних методів та засобів захисту інформації і ІКС. Перший і найважливіший метод – визначення політики безпеки ІКС. Політика інформаційної безпеки (ПІБ) – це набір правил, принципів і процедур, спрямованих на забезпечення дотримання всіма кінцевими користувачами та мережами в організації мінімальних вимог безпеки інформаційних технологій та захисту даних [8]. ПІБ повинна стосуватися всіх даних, програм, систем, об'єктів, інфраструктури, авторизованих користувачів і третіх осіб. ПІБ може бути дуже широкою. Вона може охоплювати ІТ-безпеку та/або фізичну безпеку, а також використання соціальних мереж, управління життєвим циклом і тренінги з ІБ.

Одним з підрозділів політики ІБ є регламентація доступу до інформації. Контроль доступу лежить в основі кібербезпеки. Для цього організації повинні завжди бути впевнені, що користувачі є тими, за кого себе видають, і, що вони мають дозвіл на використання певних мережевих ресурсів або доступ до зон з обмеженим доступом. Контроль доступу допомагає не лише захистити активи, але й, у разі порушення, відстежити дії та визначити причину.

Існує два види контролю доступу: фізичний і логічний. Фізичний контроль обмежує доступ до приміщень, робочих станцій та обладнання, в той час як логічний контроль обмежує доступ до критично важливих активів. Обидва види контролю є важливими для забезпечення кібербезпеки і виходять з того, що користувачі, пристрої та будь-які інші суб'єкти, які запитують доступ, невідомі доти, доки система не зможе їх ідентифікувати [9].

Слабкі та недостатні заходи – це, фактично, неминуча загроза виникнення надзвичайної ситуації. Найкращою міжнародною практикою є обмеження доступу до мережі до рівня, необхідного для виконання працівниками своїх службових обов'язків.

Принцип найменших привілеїв є одним з ключових заходів, рекомендованих стандартом IEC 62443-2-1 для захисту критично важливої інфраструктури та інших систем промислової автоматизації та управління від несанкціонованого доступу. Аналогічно, стандарт ISO/IEC 27001 рекомендує принцип найменших привілеїв для захисту даних: "Користувачам повинен бути наданий доступ до мережі та мережевих сервісів, на використання яких вони мають спеціальний дозвіл". Впровадження такої політики вимагає комплексного підходу до принципів управління ідентифікацією та активами. На додаток до обережного управління приві-

леями важливо також записувати всі дії користувачів, щоб мати можливість створити аудиторський слід у разі порушення.

Низка міжнародних стандартів стосується процесу автентифікації (перевірки пристрою та особи користувача) та авторизації, яка встановлює, чи може користувач отримати доступ до певного ресурсу з його або її рівнем привілеїв. До них відносяться, наприклад, серія стандартів IEC 62443 і згадана вище серія стандартів ISO/IEC 27000 [9].

IEC 60839-11-5 охоплює фізичні засоби контролю доступу, включаючи біометричні дані, такі як відбитки пальців і сканування райдужної оболонки ока, а також картки.

Також, варто зауважити, що організаційні заходи і методи забезпечення безпеки інформації та ІКС доволі чітко врегульовані й в українському законодавстві. Найголовнішим документом є Закон України «Про захист інформації в інформаційно-комунікаційних системах» [10]. Крім того, існує низка нормативних документів систем технічного захисту інформації, які допоможуть як з організаційними, так і з технічними методами забезпечення ІБ [11].

Висновки

1. Загрози інформаційної безпеки представлено як атаки, що можуть порушити ІБ та викликати заволодіння інформацією, і, зазвичай, походять з недостатньої захищеності чи вразливостей систем. Класифікація загроз включає основні категорії за принципами тріади кібербезпеки, джерелами, розмірами нанесеної шкоди та природою виникнення. У законодавстві України розрізняються кіберінциденти та кібератаки. Ця класифікація допомагає розуміти природу загроз та визначати відповідні заходи захисту.

2. У сучасному контексті внутрішні загрози ІБ можуть походити від різних джерел. Зловмисні інсайдери можуть намагатися викрасти інформацію або спричинити шкоду з метою особистої вигоди. Існують також загрози, що виникають внаслідок недбалого ставлення до безпеки, коли співробітники можуть навмисно або ненавмисно наражати системи на ризики. Категорії співробітників, які можуть бути втягнуті у ці загрози, включають «пішаків» та «дурнів», які можуть діяти ненавмисно або ненавмисно, а також «кротів», які отримують несанкціонований доступ до систем. Ідентифікація та усунення таких загроз вимагає комплексного підходу до безпеки організації.

3. Зовнішні загрози ІБ охоплюють різноманітні категорії, які походять зовні від організації і можуть бути спрямовані як на індивідуальні особи, так і на корпоративні системи. Серед них можуть бути атаки на особисті дані через викрадення паролів та онлайн-шахрайства, а також фізичні загрози, такі як втручання в роботу пристроїв або мереж з метою порушення їхньої роботи. Зараз розповсюджені різні види хакерських атак, такі як фішинг, атаки методом грубої сили, атаки "man in the middle", DDoS-атаки, SQL-ін'єкції та атаки "Drive-by". Крім цього, велика загроза існує від ШПЗ, таких як шпигунські програми та програми-вимагачі, які можуть призвести до крадіжок даних або втрати доступу до них.

4. Технічні загрози ІБ включають атаки на апаратне та програмне забезпечення, мережеві атаки та атаки на криптографічні алгоритми. Ці загрози становлять серйозну небезпеку для компаній та інших суб'єктів, оскільки можуть призвести до порушення конфіденційності, цілісності та доступності даних та інфраструктури.

5. Методи та засоби захисту інформації можна класифікувати за рівнем впливу на об'єкт захисту та рівнем реалізації. За першою ознакою вони поділяються на фізичні, програмні, криптографічні та правові. За другою ознакою – на організаційні, технічні та фізичні. Комбінація різних методів та засобів дозволяє створити ефективну систему захисту інформації, що враховує різні аспекти безпеки.

6. У сучасному цифровому середовищі захист інформації на підприємствах важливий для забезпечення безпеки даних. Для досягнення цієї мети використовуються технічні та організаційні методи і засоби. Технічні методи охоплюють системи автентифікації, антивірусний захист, системи захисту даних та інші. Організаційні заходи включають розробку полі-

тики безпеки, контроль доступу, принцип найменших привілеїв та інші. Загальний підхід до захисту інформації передбачає комплексне поєднання різних методів і засобів для максимальної ефективності.

Список літератури:

1. Основи управління інформаційною безпекою : навч. посіб. / А.М. Гребенюк, Л.В. Рибальченко. Дніпро : Дніпропетр. держ. ун-т внутр. справ, 2020. 144 с..
2. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII [Електронний ресурс] / Офіційний Вебпортал Парламенту України. Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19/ed20171005#Text.
3. What is an Insider Threat? Definition, Types, & Examples [Електронний ресурс]/ OpenText. Режим доступу: https://www.opentext.com/what-is/insider-threat.
4. Dashlane. (2024, Лютий 16) [Електронний ресурс] / A guide to External Security Threats in 2024. Режим доступу: https://www.dashlane.com/blog/guide-to-external-security-threats.
5. RiskOptics. (2022, Жовтень 31) [Електронний ресурс]/ Most Common Types of Network Security Attacks. Режим доступу: https://reciprocity.com/blog/most-common-types-of-network-security-attacks/.
6. What is a Cryptographic Attack? Your Comprehensive Guide. (2024, Січень 10) [Електронний ресурс] / Packetlabs. Режим доступу: https://www.packetlabs.net/posts/what-is-a-cryptographic-attack/.
7. Основи інформаційної безпеки : навч. посіб. / В. Б. Вишня, О. С. Гавриш, Е. В. Рижков. Дніпро : Дніпропетр. держ. ун-т внутр. справ, 2020. 128 с.
8. What is an Information Security Policy? (2023, Квітень 6) [Електронний ресурс]/ UpGuard. Режим доступу: https://www.upguard.com/blog/information-security-policy.
9. The important role of access control in cyber security. (2021, Квітень 21) [Електронний ресурс] / International Electrotechnical Commission. Режим доступу: https://www.iec.ch/blog/important-role-access-control-cyber-security.
10. Закон України «Про захист інформації в інформаційно-комунікаційних системах» від 05.07.1994 № 80/94-ВР [Електронний ресурс] / Офіційний Вебпортал Парламенту України. Режим доступу: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.
11. Нормативні документи системи ТЗІ. (2023, Березень 9). [Електронний ресурс] / Державна служба спеціального зв'язку та захисту інформації України. Режим доступу: https://cip.gov.ua/ua/news/normativni-dokumenti-sistemi-tzi.

Надійшла до редколегії 11.01.2024

Відомості про авторів:

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

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

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

УДК 004.065.5 **DOI:10.30837/rt.2024.1.216.04**

Є.О. ЛОГАЧОВА, М. В.ЄСІНА, канд. техн. наук

ПОРІВНЯЛЬНИЙ АНАЛІЗ УКРАЇНСЬКИХ ТА ЗАКОРДОННИХ БАНКІВСЬКИХ ЗАСТОСУНКІВ

Вступ

Банківські мобільні застосунки вже не перший рік спрощують життя клієнтам банківських установ. З кожним роком кількість користувачів збільшується, як і кількість операцій, які можна виконувати за допомогою застосунків. Проте банківські мобільні застосунки мають бути не тільки комфортними, а й убезпечувати своїх користувачів від різних видів шахрайств. Саме тому кібербезпека посідає важливе місце у розробці таких застосунків.

Розвиток мобільних банківських застосунків та загроз

Мобільні банківські застосунки можуть здаватись достатньо новою розробкою, проте насправді вони беруть свій початок з кінця минулого сторіччя. Початком зародження мобільних банківських застосунків можна вважати появу онлайн-банкінгів. У 1981 р. вперше з'являються послуги домашнього, себто онлайн банкінгу. Чотири найбільші міські банки, а саме Citibank, Chase Manhattan, Chemical and Manufacturers Hanover запропонували своїм клієнтам можливість використання системи Videotex [1]. Videotex – це загальний термін для систем, які передають текст і графіку діловому або домашньому користувачу за допомогою сигналів, що передаються по телефонній лінії, кабелю або будь-якому з каналів телевізійного або радіомовлення [2]. Наступним важливим кроком у розвитку онлайн-банкінгів стало те, що Stanford Federal Credit Union вперше надав усім своїм клієнтам можливість користуватись онлайн банкінгом [3].

Першим офіційним мобільним банківським застосунком вважається розробка The Bank of Scotland 2007 р. Пізніше у 2011 р. банк випустив повнофункціональний застосунок, доступний на пристроях Apple, пізніше застосунок адаптували і для BlackBerry та Android. Застосунок дозволяв отримати виписку з рахунку, перевірити останні транзакції та баланс [4].

Першим мобільним банківським застосунком в Україні став Приват24, який почав зароджуватись у 2001 р. Клієнти банку могли здійснювати авторизацію та проводити платежі за допомогою одноразових SMS-паролів. У 2008 р. була випущена перша версія повного мобільного застосунку Приват24 для iOS. А вже у 2010 р. була представлена версія застосунку для Android. У вересні 2019 р. було випущено версію Приват24 з оновленим дизайном та функціоналом, включаючи меню для підприємців, технологію FacePay24 та доступ для клієнтів інших банків до банківських операцій [5].

Разом із розвитком технологій, що з кожним разом все більше полегшувало користування фінансовими операціями, еволюціонували і можливості кіберзлочинів. Адже перші банківські застосунки не дозволяли виконувати настільки багато фінансових операцій, як сучасні. Це відбувається за рахунок роботи між пристроєм користувача та банківським сервером. І це відкриває більше можливостей для шахраїв, щоб незворотньо викрасти гроші або ж дані користувачів. До основних загроз належать [7]:

- атаки соціальної інженерії;
- фішинг;
- підробка банківських додатків;
- кейлогери;
- зловмисне програмне забезпечення;
- віруси трояни;
- фізична крадіжка пристрою;
- злам Wi-Fi;

- атаки на зв’язок;
- атаки на одноразові паролі та інше.

Характеристика досліджуваних застосунків

Для порівняльного аналізу було обрано п’ять українських застосунків та п’ять застосунків з різних країн. Перший досліджуваний банк згадувався раніше – Stanford FCU, який створили та використовують в США. Оновлений застосунок Stanford FCU випущено у вересні 2016 р., за цей час його завантажили понад 10 000 разів. Банк Stanford FCU пропонує своїм клієнтам два способи завантаження – з сайту банку та через PlayMarket [6].

Наступним досліджуваним банком є Fideuram – італійський банківський додаток. Fideuram з’явився у лютому 2015 р. Додаток налічує більше 100000 завантажень. Застосунок створено для пристроїв iPhone [8].

N26 – європейський мобільний банк, головний офіс якого розташований у Берліні. Додаток доступний для використання у країнах Європейського Союзу (ЄС), Великої Британії та США. N26 випустили у січні 2015 р., з того часу кількість клієнтів налічує понад 8000000 [9].

Banque populaire – французький банк, який презентував свій застосунок – Banque populaire du nord ще у 2010 р. Кількість завантажень перевищує 1000000. Застосунок використовують на території Франції. Для завантаження застосунку надано QR-коди, відсканувавши, які можна легко завантажити застосунок з різних платформ [10].

Останній досліджуваний закордонний банківський застосунок – Sparkasse. Sparkasse – німецький банк, який розробив свій додаток у 2014 р., з того часу кількість завантажень перевищує 10000000. Як правило, додатково завантажується і S-pushTAN – sichere Freigaben, який в подальшому буде використовуватись для покращення надійності автентифікації, проте його не рекомендують ставити на один пристрій із застосунком, адже у випадку зламу це може полегшити вхід шахраям [11].

Серед українських банків було обрано Monobank – перший український повноцінний мобільний банк, який не має фізичного відповідника, тобто банківського філіалу. Monobank існує з 2017 р. і надає своїм клієнтам широкий спектр послуг, завдяки якому у них не виникає необхідності звертатись до фізичної філії. Monobank не поступається своїм конкурентам, застосунок завантажили більше 10 мільйонів разів [12].

Приват24 – перший український мобільний банківський застосунок, який зароджувався ще у 2001 р., а у 2011 р. випустив застосунок, який використовується нині і налічує понад 10000000 завантажень [5].

Укрсиб-онлайн є менш популярним, проте його також використовує багато українців, застосунок розроблено у 2017 р., його використовують понад 1 мільйон користувачів. Укрсиббанк надає посилання для завантаження на своєму сайті [13].

Наступним для розгляду було обрано Ощадбанк. Оновлений застосунок випустили відносно нещодавно – у 2021 р., а він вже завантажений більше одного мільйону разів. Розробники стверджують, що застосунок має надійну безпеку, адже до нової версії додано верифікацію по PIN-коду картки. Завантажити застосунок можна за допомогою перевірених посилань на сайті Ощадбанк [14].

Банківський застосунок від ПУМБ було випущено у 2018 р., застосунок пропонує велику кількість послуг та вигідних пропозицій, наразі налічує понад 1000000 завантажень. Також застосунок підтримується на всіх пристроях, телефоні, комп’ютері чи планшеті [15].

Кожен з розглянутих банків надає посилання для завантаження на своєму сайті, адже однією з потенційних шахрайських дій є саме підробка застосунків. Додатковою перевагою є те, що банки, турбуючись про безпеку своїх клієнтів, нагадують користувачам правила безпеки при використанні мобільного банківського застосунку, розглядають потенційні загрози та надають необхідні контакти, до яких можна звернутись у разі виникнення загрози.

Порівняльний аналіз застосунків

У контексті сучасного фінансового ринку одними з найважливіших аспектів при виборі клієнтом банку є безпека та зручність. Банківські застосунки напряму пов'язані з персональними даними клієнтів, їх банківськими рахунками та серверами банку. Такі застосунки потребують особливих заходів безпеки, наприклад, наявності обов'язкової двофакторної автентифікації чи наявності можливості заміни паролю у застосунку. У табл. 1 та 2 наведено порівняльний аналіз досліджуваних банків за аспектами безпеки.

Таблиця 1

Аспекти безпеки закордонних застосунків

Безпека	Наявність двофакторної автентифікації	Наявність PUSH-повідомлень	Зміна PIN у застосунку	Вимикати посилену автентифікацію	Вибір власного CVV
Stanford FCU	+	-	-	-	-
Fideuram	+	-	+	-	-
N26	+	+	+	-	-
Banque populaire du nord	+	+	-	+	-
Sparkasse	+	+		-	-

Таблиця 2

Аспекти безпеки українських застосунків

Безпека	Наявність двофакторної автентифікації	Наявність PUSH-повідомлень	Зміна PIN у застосунку	Вимикати посилену автентифікацію	Вибір власного CVV
Monobank	+	+	+	-	+
Приват24	+	+	+	-	-
Укрсиб-онлайн	+	+	+	-	-
Ощадбанк	+	-	-	-	-
ПУМБ	+	+	-	-	-

За даними табл. 1 та 2 помітно, що лідерами за шкалою безпеки є N26, Banque populaire du nord, Monobank, Приват24 та Укрсиб-онлайн. Виходячи з результатів, можна помітити, що українські банки загалом намагаються не поступатись міжнародним.

Проте для того, щоб клієнт обрав певний застосунок, надійності може бути недостатньо. Адже стандарти зручності у користувачів підвищуються, а це значить, що розробники вимушені знаходити баланс між зручністю та безпекою. Так, наприклад, подовжена перевірка легітимності користувача чи відсутність миттєвих переказів може змусити клієнта обрати інший більш швидкий та зручний застосунок. Порівняльний аналіз аспектів зручності досліджуваних банків наведено у табл. 3 та 4.

Таблиця 3

Аспекти зручності закордонних застосунків

Зручність	Сплата будь-якого рахунку	Кредитна лінія у застосунку	Відкриття валютного депозиту	Аналіз витрат і доходів	Наявність страхування
Stanford FCU	-	-	-	-	-
Fideuram	+	-	-	+	-
N26	+	-	-	+	+
Banque populaire du nord	+	+	-	+	+
Sparkasse	+	-	-	+	-

Таблиця 4

Аспекти зручності українських застосунків

Зручність	Сплата будь-якого рахунку	Кредитна лінія у застосунку	Відкриття валютного депозиту	Аналіз витрат і доходів	Наявність страхування
Monobank	-	+	+	+	+
Приват24	+	+	+	+	+
Укрсиб-онлайн	-	-	-	+	-
Ощадбанк	-	-	-	+	+
ПУМБ	-	+	+	+	+

За даними табл. 3 та 4 лідируючі позиції за зручністю займають такі банки, як N26, Banque populaire du nord, Monobank, ПУМБ, найбільше відповідностей помічено у Приват24.

Банківські застосунки закордонного походження мають низку значних переваг над українською системою: структуровані вимоги до безпеки банківських мобільних застосунків, відповідність міжнародним нормам, більша увага безпеці, аніж зручності. Проте українські застосунки, хоч і зіштовхуються з певними проблемами – відсутність стандартів та єдиних правил в Україні щодо безпеки мобільних банківських застосунків; мала кількість точок доступу до якісного Інтернету, недостатність необхідного регулювання з боку держави, бажання догодити клієнтам новими покращеннями швидкості та зручності, все ж розвиваються і покращуються у плані кібербезпеки в тому числі. За останні роки було впроваджено нові норми та стандартизації, які наближають рівень безпеки українських мобільних банкінгів до європейських і тим самим допомагають Україні більше інтегруватись до ЄС [7].

Висновки

1. Враховуючи темп сучасного життя, мобільні банківські застосунки стають необхідністю для повноцінного комфорту. Кількість користувачів таких застосунків щорічно збільшується, а разом із тим прогресують можливості, які надають застосунки.

2. Рівень безпеки за обраними критеріями в українських банківських застосунках знаходиться на тому ж рівні, що і у міжнародних застосунках. При цьому Monobank показав навіть кращий результат, охопивши чотири пункти з п’яти. Проте, оглядаючи загальну картину відповідності міжнародним нормам, стає помітно, що українським системам ще необхідно розвиватись.

3. За обраними критеріями зручності найкращі результати отримав Приват24, серед міжнародних банківських застосунків найкраще показав себе Banque populaire du nord, натомість найгіршим виявився Stanford FCU. За отриманими результатами найкраще поєднання безпеки та зручності вдається N26, Banque populaire du nord, Monobank та Приват24.

Список літератури:

1. Dr. Yellaswamy Ambati // International Journal of Research in Management, Economics and Commerce. ISSN 2250-057X, Impact Factor: 6.384, Vol. 07 Is. 12, Dec.2017. P. 68–73. [Електронний ресурс]. Режим доступу: https://indusedu.org/pdfs/IJRMEC/IJRMEC_1468_22786.pdf
2. VI Deotex Systems and Services / L.R. Bloom, A.G. Hanson, R. F. Linfield, D.R. Wortendyke. u.s. Department of Commerce, Oct.1980. [Електронний ресурс]. Режим доступу: https://its.ntia.gov/umbraco/surface/download/publication?reportNumber=80-50_ocr.pdf
3. Stanford Federal Credit Union Transforms Member Experience with Digital Banking Innovations [Електронний ресурс]. Режим доступу: https://www.q2.com/blog/stanford-federal-credit-union-transforms-member-experience-with-digital-banking-innovations
4. Banking app, 2011. [Електронний ресурс]. Режим доступу: https://www.natwestgroup.com/heritage/history-100/objects-by-theme/going-the-extra-mile/banking-app-2011.html
5. Приват24 включив рейтинг діджитальності користувачів. [Електронний ресурс]. Режим доступу: https://privatbank.ua/news/2021/3/26/1401
6. Mobile app and Online Banking. [Електронний ресурс]. Режим доступу: https://www.sfcu.org/online-banking/

7. Аналіз особливостей забезпечення кібербезпеки у банківських мобільних додатках / Є. Логачова, М. Єсіна, В. Бобух // Computer science and cybersecurity. 2023. № 1(23). С. 63–73. [Електронний ресурс]. Режим доступу: https://periodicals.karazin.ua/cscs/article/view/23094/21104.
8. Fideuram Online. [Електронний ресурс]. Режим доступу: https://www.fideuram.it/prodotti-e-soluzioni-personalizzate/servizi-online/fideuram-online/
9. Open a bank account online in minutes. [Електронний ресурс]. Режим доступу: https://n26.com/en-eu/open-bank-account-online
10. Banque populaire du nord. [Електронний ресурс]. Режим доступу: https://www.banquepopulaire.fr/nord/votre-banque/choisir-une-region/?source_id=3494&wording=region
11. Онлайн-банкінг від шпаркаси App „Sparkasse“ [Електронний ресурс]. Режим доступу: https://www.berliner-sparkasse.de/content/dam/myif/berliner-sk/work/dokumente/pdf/allgemein/PushTan-und-OnlineBanking-UKR.pdf?stref=imagetextbox
12. Monobank. [Електронний ресурс]. Режим доступу: https://www.monobank.ua/cpa?lang=uk
13. UKRSIB online. [Електронний ресурс]. Режим доступу: https://online.ukrsibbank.com/ibank/
14. Мобільний додаток Ощад 24/7. [Електронний ресурс]. Режим доступу: https://www.oschadbank.ua/mobilnij-dodatok
15. ПУМБ Online – це моє! [Електронний ресурс]. Режим доступу: https://www.pumb.ua/pumbonline

Надійшла до редколегії 05.01.2024

Відомості про авторів:
Логачова Єлизавета Олегівна – студентка факультету комп’ютерних наук; Харківський національний університет імені В. Н. Каразіна; Україна; e-mail: lohachova2020kb11@student.karazin.ua; ORCID: https://orcid.org/0000-0002-9815-466X
Єсіна Марина Віталіївна – канд. техн. наук, доцент, доцент кафедри безпеки інформаційних систем і технологій, факультет комп’ютерних наук, Харківський національний університет імені В. Н. Каразіна; АТ «Інститут Інформаційних Технологій», науковий співробітник-консультант; Україна; e-mail: m.v.yesina@karazin.ua; ORCID: https://orcid.org/0000-0002-1252-7606

УДК 621.391:519.2 **DOI:10.30837/rt.2024.1.216.05**

Є.В. КОТУХ, канд. техн. наук, Г.З. ХАЛІМОВ, д-р техн. наук,
М.В. КОРОБЧИНСЬКИЙ, д-р техн. наук, М.М. РУДЕНКО, канд. техн. наук,
В.О. ЛЮБЧАК, канд. фіз.-мат. наук, С.М. МАЦЮК, канд. техн. наук, М.В. ЧАЩИН

ГОРИЗОНТИ ДОСЛІДЖЕНЬ В ГРУПОВІЙ КРИПТОГРАФІЇ В КОНТЕКСТІ РОЗРОБКИ ПОСТКВАНТОВИХ КРИПТОСИСТЕМ

Постановка задачі

Основним елементом криптографії з відкритим ключем є односторонні функції. У криптографії така функція використовується для шифрування, тоді як її інверсія – для дешифрування. Важливо, що дешифрування має бути простим лише для особи з секретним ключем, яка відкриває "люк" для легкого розшифрування. Цей секретний ключ відомий лише одержувачу та дозволяє легко розшифровувати повідомлення, зашифровані відкритим ключем. Відсутність інформації про "люк" у третіх осіб робить розшифрування обчислювально нездійсненним.

Інтуїтивно обґрунтованим припущенням є, що NP-повні проблеми в області теоретичної інформатики можуть бути ідеальними кандидатами для використання як односторонніх функцій у криптографії з відкритим ключем [1]. Проблема, що належить до множини NP-повних проблем, визначається тим, що перевірка правильності її рішення є простою, у той час як знаходження самого рішення є складним без наявності секретної інформації про "люк". Тут "простота" означає можливість обчислення за поліноміальний час, а "складність" – це неполіноміальний час обчислень, зазвичай експоненціальний.

Припускаючи, що $P \neq NP$, здається, що використання NP-повних проблеми задовольнило ці критерії. Загалом легко генерувати NP приклади належні до множини NP-повних проблем, але за умови, що $P \neq NP$ такі приклади залишаються такими, що важко розв'язуються.

Іншою привабливою особливістю NP-повних проблем є те, що, на відміну від задачі цілочисельної факторизації та проблеми дискретного логарифмування, вирішення NP-повних проблем є потенційно складним для квантового прискорення обчислень. Це залишається відкритим питанням, навіть за умови припущення, що $P \neq NP$. Таким чином, цікавою науковою задачею є розгляд можливості використання NP-повних проблем для побудови криптосистем відкритого ключа, стійких до атак, що реалізуються на квантових комп'ютерах [2].

Існують технічні складнощі для створення криптосистеми на основі NP-повних проблем, що завадило використанню цієї множини задач як основи для безпеки в таких криптосистемах. Концепція використання NP-повних проблеми для створення криптосистеми з відкритим ключем спочатку здавалася перспективною, але на практиці не продемонструвала результатів. Перша така криптосистема з відкритим ключем була побудована на базі проблеми цілочисельного рюкзака, яка згодом була скомпрометована за допомогою потужних універсальних атак. Зауважимо, що атаки були спрямовані на конкретну реалізацію люка, а не безпосередньо на проблему рюкзака. Задача побудови стійкої реалізації люка для криптосистеми на основі проблеми рюкзака залишається актуальною.

Проблема слова і проблема рюкзака мають схожість, оскільки обидві представляють собою "природні" задачі для криптосистем з відкритим ключем та можуть бути безпосередньо застосовані для побудови криптосистеми з відкритим ключем. Зрозуміло, що основною проблемою для розробки стійкої до атак конструкції є реалізація люка, що забезпечує розшифрування. Коли люк існує, він може стати вразливим місцем для криптоаналітичних атак [2].

Для розуміння ієрархії задач прийняття рішень запропонуємо візуалізацію множин складності проблем (рис. 1), що починається з проблем, які вирішуються за поліноміальний час,

проходить через множину NP-повних проблем і завершується NP-складними нерозв'язними проблемами, які є найскладнішими з усіх.

NP-повні проблеми вважаються такими, що знаходяться на грані розв'язності та є найпростішими з відомих "природних" проблем, які все ще вважаються нерозв'язними. Якщо NP-повна проблема буде трохи послаблена, вона може стати вже розв'язною.

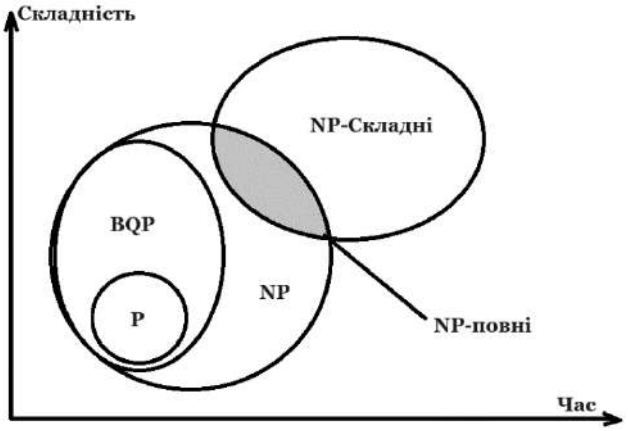


Рис. 1. Класи складності нерозв’язаних проблем

У контексті побудови квантово стійкої асиметричної криптосистеми необхідно враховувати саме дизайн люка. Це додає складності у використанні класичних NP-повних проблем та зумовлює, що NP-повна проблема може бути більш ускладнена задля забезпечення постквантових властивостей. Вважається, що більш складна проблема може ускладнити безпосередні атаки та надати більше можливостей для інтеграції люків, зберігаючи при цьому стійкість криптосистеми.

Аналіз поточного стану проблем, складних для розв’язання

Брассард в роботі [3] продемонстрував, що з певними обмеженнями, якщо б криптосистема була доведено NP-повною для атаки, це б теоретично означало, що NP=NP-повна. Однак ця теорія вважається невірною, хоч і доказів цьому немає. Тому криптоаналіз асиметричних криптосистем, що засновані на NP-повних проблемах, буде легшим, та, ймовірно, обчислено ймовірним.

Існує багато теорій про NP-повноту, але вони стосуються лише аналізу найгіршого випадку та певних прикладів проблеми. Наприклад, проблема цілочисельного рюкзака не є NP-повною за умов, якщо у проблемі не використовуються "експоненційно великі" числа. Для цього випадку для цієї проблеми існують алгоритми поліноміального часу [4].

Існують також розумні алгоритми наближення, що дозволяють обчислити приблизне рішення, яке не є точним. Також існують недетерміновані алгоритми, які можуть надати точну відповідь або з великою ймовірністю також можуть не дати відповіді зовсім. Хоча немає відомого алгоритму поліноміального часу для класичних обчислювачів, що вирішує найгірші випадки великих екземплярів, алгоритми, подібні до описаних, можуть запускати великі екземпляри NP-повної проблеми, які є неприйнятними, якщо асиметрична криптосистема має бути безпечною.

Проблема факторизації стала основою для декількох криптографічних систем, генерації криптографічно безпечних генераторів випадкових чисел та алгоритмів обміну секретними ключами без участі арбітра. Для цього випадку кожен протокол із повним підтвердженням безпеки базується на припущенні, що факторизація залишається складним завданням. Сама криптосистема RSA, хоча й не є прямо еквівалентною , все ж залежить від складності цього процесу для забезпечення своєї безпеки. Нові напрями в розробці та дослідженні криптосистем відкритого ключа, що використовують факторизацію, з’являються постійно.

В роботах [5 – 10] розглянуто використання логарифмічних підписів – особливого типу факторизації в групах. Факторизація залишається нерозв'язною проблемою для класичних

комп’ютерів. Проблеми, які можуть вирішити квантові комп'ютери за поліноміальний час, відносяться до класу BQP. До них відносяться всі проблеми P і багато проблем NP (див. рис. 1). В роботі [11] теоретично обґрунтовано можливість зниження криптографічної стійкості криптосистем, що використовують факторизацію чи проблему дискретного логарифму з використанням квантових обчислень. Отже, квантовому комп’ютеру потрібно більше ніж поліноміальна кількість кроків для вирішення NP-повної проблеми. Зрозуміло, що справжній статус складності завдання факторизації, особливо за умов факторизації в групах, залишається невизначеним.

Лю та Пас представили NP-повну задачу, складність випадку якої, у середньому, еквівалентна існуванню односторонніх функцій [1]. Отже, складна проблема в множині NP-повних проблем існує, якщо існує справжня одностороння функція та $P \neq NP$. Однак це не робить криптосистему, що використовує в основі таку проблему, криптографічно стійкою, бо реалізація функціональності люка матиме критичне значення.

Відповідно розгляд більш складних проблем як основи для криптосистем з відкритим ключем є важливим науково значущим підходом. Існують різноманітні проблеми, доведено нерозв'язні, а також задачі, для яких неможливо знайти загальне алгоритмічне рішення. Важливо , що для асиметричних криптосистем може бути застосований лише специфічний приклад однієї з цих складних задач. Складність криптоаналізу все одно залишиться в межах класу NP.

Розглянемо основні визначення та поняття. Перш за все, необхідно дослідити та обґрунтувати, за яких умов проблема, що визначається, належить до NP-повних проблем.

Визначення 1. Нехай A – детермінований алгоритм, який зупиняється на всіх входах. Функція $f: \mathbb{N} \to \mathbb{N}$, де $f(n)$ – максимальна кількість кроків, яка A використовується для будь-якого введення довжини n, є визначенням часу виконання (часової складності) A. Якщо $f(n)$ є час роботи A, вважаємо, що A виконується в часі $f(n)$, і це A є $f(n)$ часовим алгоритмом.

Визначення 2. Нехай f та g є функціями $f, g: \mathbb{N} \to \mathbb{R}^+$. Визначимо, що $f(n) = O(g(n))$, якщо існують такі позитивні цілі числа c і n_0, що для кожного цілого $n \geq n_0$, $f(n) \leq cg(n)$. Коли $f(n) = O(g(n))$, то $g(n)$ – це асимптотична верхня межа для $f(n)$.

Визначення 3. Нехай $t: \mathbb{N} \to \mathbb{R}^+$ функція. Визначимо клас часової складності, $TIME(t(n))$ як множину усіх проблем, які розв’язуються за допомогою $O(t(n))$ часового алгоритму.

Визначення 4. $P = \bigcup_{k \in \mathbb{N}} TIME(n^k)$ або P – це клас задач, які можна розв’язати за поліноміальний час за допомогою детермінованого алгоритму.

Визначення 5. NP – це клас задач, рішення яких може бути перевірено за поліноміальний час.

Визначення 6. Проблема A – це поліноміальне відображення часу, яке зводиться до проблеми B, визначеної як $A \leq_P B$, якщо існує функція f – поліноміальна обчислювана за часом, де для кожного w, $w \in A \Leftrightarrow f(w) \in B$. Функція f називається поліноміальним скороченням часу A до B.

Визначення 7. Проблема B є NP-повною, якщо вона задовольняє двом умовам: B знаходиться в NP, і будь-яке A в NP є обчислюваною за поліноміальний час, що зводиться до B.

З визначення NP-повноти випливає, якщо якась NP-повна проблема знаходиться в P, то всі ці проблеми належать до множини P. Маємо наступний висновок – якби алгоритм

вирішення проблеми за поліноміальний час можна було знайти для будь-якої NP-повної проблеми, то кожну NP-повну проблему можна вирішити за поліноміальний час.

Наразі не визначено жодної NP-повної проблеми, що можна вирішити за поліноміальний час. Також не доведено зворотне. Однак щоб це довести, треба довести, що $P \neq NP$; це наразі є найважливішою невирішеною проблемою в теоретичній інформатиці. Теоретично обґрунтовано, що класи P і NP не є рівними. Саме це обґрунтування лежить в основі припущення, що NP-повні проблеми не можуть бути розв'язані за поліноміальний час [12]. Хоча відсутність доказів цієї гіпотези може розглядатися як явна слабкість у використанні NP-повних проблем як основи для асиметричних криптосистем, важливо зазначити, що наразі не доведено, що факторизацію цілих чисел та обчислення дискретних логарифмів не можна виконати за поліноміальний час з використанням класичного обчислювача. Докази на користь $P \neq NP$ не наведено, але факт недоведеності $P \neq NP$ не є сильним запереченням проти використання NP-повних проблем як основи для криптосистем з відкритим ключем. Однак, навіть якщо це насправді так – $P \neq NP$, все ще не зрозуміло, чи можна використовувати NP-повні проблеми як платформу для криптосистем з відкритим ключем. Причиною цього є те, що класи складності P і NP визначаються в термінах найгіршого випадку часу роботи алгоритмів, які вирішують проблеми, що містяться в них. Отже, можливо, що за умов належності проблеми до NP з $P \neq NP$ є багато прикладів таких проблем, що можуть бути розв'язані за поліноміальний час. Саме з цих причин було проведено дослідження середньої складності NP-повних проблем [13].

За декілька десятиріч визначено перелік актуальних проблем, для яких переважна більшість прикладів таких проблем є простою для розв'язання. Наприклад, важливо зазначити, що проблема слова є NP-повною проблемою та є розв'язуваною для багатьох груп. Тільки незначна частина прикладів потребує часу, більшого за поліноміальний. Такі проблеми визначені як ті, що мають «чорну діру», та їх подальше використання у якості кандидатів для криптографії з відкритим ключем не розглядається. Вочевидь, існують проблеми, що мають «білу діру», де переважна більшість випадків є складною. Такі проблеми в множині NP-повних проблем мають перспективу для побудови постквантових криптосистем відкритого ключа.

Критерії належності проблеми слова в групах до NP-повних проблем

Наступні проблеми прийняття рішень були введені ще у 1911 р. та визначаються таким чином.

Проблема слова: для будь-якого $g \in G$ визначте, чи g є тотожним елементом G.

Проблема спряженості: для будь-якого $x, y \in G$ визначте, чи x та y спряжені, тобто чи існує елемент $c \in G$ (кон'югатор), такий, що $c^{-1}xc = y$.

Проблема ізоморфізму: Нехай G і G' – групи, задані кінцевими представленнями, визначте, чи G ізоморфна G'.

В 1912 р. Ден розробив алгоритм, що вирішує як проблему слова, так і проблему спряженості для фундаментальних груп замкнутих орієнтованих двовимірних многовидів роду, який більший або дорівнює 2. Такий підхід був значно розширений та адаптований для широкого спектру задач у теорії груп.

Проблема слова для загальних груп не класифікується як NP-повна, оскільки її властивості суттєво відрізняються в залежності від конкретної групи, для якої вона формулюється. Хоча для деяких специфічних класів груп проблема слова може бути розв'язана за поліноміальний час, для інших вона може бути нерозв'язною. Для того щоб проблема вважалася NP-повною, вона має задовольняти двом умовам: бути в множині NP (тобто для кожної вірної відповіді існує "свідок", який може бути перевірений за поліноміальний час), а також умові зведення кожної NP проблеми до NP-повної за поліноміальний час.

Проблема слова не завжди відповідає цим умовам, оскільки її складність може істотно варіювати залежно від структури групи. Проблема слова може бути NP-повною для певних

спеціальних класів груп або в певних умовах. Тому, проблема слова в контексті теорії груп не вважається NP-повною, хоча її варіанти для деяких конкретних груп або у спеціалізованих контекстах можуть мати різні обчислювальні властивості. Стислий аналіз таких класів груп допомагає визначити наступні конструкції.

Графові групи: для певних графових груп проблема слова може бути NP-повною. Це пов'язано зі структурою групи, яка визначається графом, та складністю визначення, чи можна рядок, сформований з генераторів та їх інверсій, звести до порожнього слова.

Групи з особливо складними відношеннями: у деяких групах, де визначення відношень між генераторами є особливо складним, проблема слова може стати NP-повною. Це стосується ситуацій, коли відношення в групі настільки складні, що перевірка еквівалентності двох рядків вимагає значних обчислювальних зусиль.

Специфічні конструкції: для деяких специфічних конструкцій груп, особливо тих, що штучно створені для демонстрації певних обчислювальних властивостей, проблема слова може бути NP-повною. Ці конструкції зазвичай розробляються так, щоб ілюструвати певні теоретичні аспекти проблеми слова.

Як було зазначено вище, проблема слова є розв'язуваною для багатьох груп G. Наприклад, для поліциклічних груп існують розв'язки проблеми слова, оскільки можна легко обчислити нормальну форму будь-якого слова в поліциклічному представленні; інші алгоритми також можуть вирішити проблему слова в певних умовах, зокрема алгоритм Тодда – Коксетера [14] і алгоритм завершення Кнута – Бендікса [15]. З іншого боку, неможливість розв'язання проблеми слова для конкретної групи деяким алгоритмом не означає, що в цій групі проблема слова є нерозв'язною. Наприклад, алгоритм Дена не розв'язує проблему слова для фундаментальної групи тора, але оскільки ця група є прямим добутком двох нескінченних циклічних груп, проблема слова для неї є розв’язною. У більш конкретних термінах проблему з уніфікованим словом можна виразити як питання про переписування літеральних рядків. Для представлення P групи G, P буде вказувати певну кількість генераторів $x, y, z, ...$ для G. Потрібно ввести одну букву для x і іншу (для зручності) – для елемента групи, представленого x^{-1}. Назвемо ці букви алфавітом $\sum$ нашої задачі. Тоді кожен елемент у G певним чином представляється добутком символів алфавіту $\sum$ певної довжини, помножених в G. Рядок довжиною 0 (нульовий рядок) означає одиничний елемент групи e з G. Суть усієї проблеми полягає в тому, щоб мати можливість розпізнати всі способи представлення e, враховуючи деякі співвідношення.

Вплив відношень у G полягає в тому, що вони дозволяють різним рядкам представляти один і той самий елемент групи. Відношення надають перелік рядків (слів), які можна вставляти або видаляти у виразі без зміни значення виразу, тобто елемента групи, що отримується в результаті множення слів. Це означає, що за наявності певних відношень можемо перетворити одне представлення елемента на інше, зберігаючи при цьому ідентичність елемента в контексті групової операції.

Для простого прикладу візьмемо презентацію $\{a \mid a^3\}$. Подання $\{a \mid a^3 = e\}$ описує циклічну групу порядку 3, де e – одиничний елемент групи. У цій групі кожен елемент можна представити як ступінь a та $a^3 = e$, тобто представити a як одиничний елемент групи. Записуючи A для зворотного до a, ми маємо можливі рядки, що поєднують будь-яку кількість символів a та A. Щоразу, коли бачимо aaa, або aA чи Aa, можемо їх викреслити. Ми також повинні пам’ятати про те, щоб викреслити AAA; це говорить, що оскільки куб a є одиничним елементом G, то таким же є і куб, обернений a. За цих умов проблема слова стає легкою. Спочатку скоротимо рядки до порожнього рядка a, aa, A або AA. Потім, щоб перетворити A в aa і перетворити AA в a, помножимо на aaa. Таким чином, проблема слова для циклічної групи третього порядку є розв’язною.

Однак це не типовий випадок, оскільки у якості прикладу маємо доступну канонічну форму, яка зменшує будь-який рядок з трьох до довжиною щонайбільше одного шляхом

монотонного зменшення довжини. В загальному випадку не можна отримати канонічну форму для елементів шляхом поетапного скорочення. Ймовірно, доведеться використовувати відношення для багаторазового розширення рядка, щоб зрештою знайти скорочення, яке зменшує довжину. У гіршому випадку відношення між рядками, що свідчить що вони рівні, в G є нерозв'язною проблемою .

Петро Новіков показав, що існує скінченно представлена група G, така що проблема визначення слова для G є нерозв'язною [16]. Звідси випливає, що проблема однорідного слова також є нерозв'язною. Інший доказ отримано авторами у [17] та досі не спростовано.

Існують нерозв'язні задачі для скінченно заданих груп і для напівгруп. В [18 – 20] розглянуто основні результати. Скінченно представлена група G складається з генераторів $x_1, x_2, ..., x_n$, які є просто абстрактними символами, і реляторів $r_1 \neq e\ r_1 \neq e, r_2 \neq e, ..., r_m \neq e$, які будуть визначені нижче. Кожному твірному відповідає x_i зворотний x_i^{-1}. Слово в G – це кінцевий рядок, що складається із символів x_i і x_i^{-1}. Порожній рядок e також є словом, ідентифікатором групи. Кожне з r_i перераховане вище, є словом. Груповою операцією об'єднання слів є конкатенація. Для кожного слова w зворотне слово w^{-1} складається з усіх символів w, записаних у зворотному порядку, де кожен x_i замінюється на x_i^{-1}, а кожен x_i^{-1} замінюється на x_i.

Група G складається з класів еквівалентності всіх можливих слів. Два слова w і v еквівалентні, якщо ми можемо перетворити w на v за допомогою кінцевої послідовності правил зміни форми.

Правило 1: зміна $x_i x_i^{-1}$ або $x_i^{-1} x_i$ на e, тобто виключення $x_i x_i^{-1}$ або $x_i^{-1} x_i$;

Правило 2: представлення $x_i x_i^{-1}$ або $x_i^{-1} x_i$ будь-який момент;

Правило 3: зміна r_j або r_j^{-1} на e, тобто виключення r_j або r_j^{-1};

Правило 4: представлення r_j або r_j^{-1}.

Існує більш формальний спосіб визначення цих понять. Спочатку вільна група F на генераторах $x_1, x_2, ..., x_n$ визначається як набір усіх слів у x_i і x_i^{-1}, які скорочуються шляхом повторної відміни $x_i x_i^{-1}$, $x_i^{-1} x_i$ доки подальші відміни не стануть можливими. Це дозволяє R бути нормальною підгрупою, породженою словами $r_1, r_2, ... r_m$ (R є перетином усіх нормальних підгруп, що містять r_j). Нарешті, G є фактор-групою F / R.

Проблема зі словом для групи G – це проблема з рішенням, яка запитує w, чи кожне слово w є еквівалентним тотожності G. Виявляється, що існують певні групи, для яких проблема зі словом є нерозв'язною. Як і будь-яка нерозв'язна проблема, проблема слова може бути нерозв'язною лише як питання, яке ставлять про нескінченну кількість слів, – будь-яка кінцева колекція слів повинна мати розв'язну проблему зі словами.

Таким чином, проблема слова в теорії груп може мати значний вплив на розробку криптографічно стійких алгоритмів в постквантову еру. Оскільки проблема слова може бути нерозв'язною для деяких груп, це створює потенціал для використання таких груп у розробці криптографічних систем, де визначення еквівалентності двох слів (або рядків) є критично важливим. Дослідження проблеми слова може сприяти створенню нових криптографічних схем, де безпека базується на складності обчислень у певних групах, а обґрунтування використання цих груп буде відігравати ключову роль у розробці алгоритмів, стійких до квантових атак.

Потенціал нерозв'язаних проблем у груповій криптографії

Групова криптографія все ще перебуває на ранніх етапах розвитку, хоча за останнє десятиліття продуктивно просувається вперед [21]. Більшість протоколів, що ґрунтуються на теорії груп, базуються на пошукових задачах, які походять з традиційних вирішувальних

задач в комбінаторній теорії груп. У наших застосуваннях ми використовуємо обидва типи цих задач. Задано властивість P та об'єкт O, вирішувальна задача для P та O полягає в визначенні, чи має O властивість P, тоді як пошукова задача для P полягає в знаходженні принаймні одного конкретного об'єкта O з властивістю P з множини об'єктів S, коли є інформація про те, що існують об'єкти з властивістю P. Наприклад, проблема пошуку спряженості, проблема пошуку гомоморфізму, проблема пошуку розкладу та проблема пошуку приналежності підгрупі є деякими з запропонованих примітивів на основі пошуку.

Проблема слова стала одним з перших прикладів нерозв'язної задачі, яка була виявлена не в області математичної логіки чи теорії алгоритмів, а у ключовій сфері класичної математики – алгебрі [22]. Через її нерозв'язність декілька інших задач у комбінаторній теорії груп також виявилися нерозв'язними. Важливо зазначити, що встановлення NP-повноти для проблеми слова в конкретних групах залежить від детального аналізу структури та властивостей цих груп.

Скінченно наведені групи є надзвичайно складними об'єктами. Наприклад, вільна група на двох твірних без зв’язків містить у собі як підгрупу вільну групу на злічено нескінченній кількості твірних. З такими групами та проблемою слова пов’язано багато структур і теорій.

Проста група – це нетривіальна група, єдиними нормальними підгрупами якої є сама тривіальна група. Практичний інтерес також мають деякі квазіпрості групи: G є квазіпростою, якщо вона є досконалою, тобто дорівнює власній підгрупі-комутатору $G=[G,G]$, а її група внутрішніх автоморфізмів $Inn(G)$ – проста. Для практичного застосунку в криптографії прикладне значення мають скінченні групи, оскільки перспективні напрями вимагають кінцевих структур даних. Існує класифікація [23] всіх скінченних простих груп, докази якої було завершено в 2000-х роках після багатьох років роботи великої кількості математиків. Для розуміння скористаємось Теоремою 1.

Теорема 1. Якщо G є скінченною простою групою, то або G є абелевою, у цьому випадку вона є циклічною групою простого порядку, або G є неабелевою, у цьому випадку виконується одна з умов:

- або $G \cong A_n$ – знакозмінна група на $n > 5$ символів;
- або G – група типу Лі;
- або G – одна з 26 спорадичних груп.

Групи типу Лі, які включають як класичні, так і виняткові групи, є важливим елементом сучасної алгебраїчної теорії. Вони визначені над скінченними полями із характеристикою поля p, яка є простим числом, та порядком поля q, що є степенем p. Основною особливістю цих груп є порядок групи. Використання неабелевих груп у криптографії має декілька переваг порівняно з абелевими групами. Неабелеві групи мають більш складну структуру, ніж абелеві, оскільки в них порядок виконання операцій є суттєвим. Ця додаткова складність робить процес аналізу і розкриття приватних ключів у криптосистемах більш складним.

Властивість некомутативності неабелевих груп ускладнює певні види атак, такі як атаки з використанням методів лінійної алгебри, які можуть бути ефективними проти криптосистем, заснованих на абелевих групах [24]. В неабелевих групах можливе використання більшої кількості операцій для конструкції криптосистем, що надає додаткову гнучкість у дизайні криптографічних протоколів.

Неабелеві групи можуть використовуватися у протоколах обміну ключами, де складність обчислення оберненого елемента або вирішення проблеми кон'югації може забезпечити додатковий рівень безпеки. Загалом, використання неабелевих груп в криптографії дозволяє розробляти складніші та потенційно більш безпечні криптографічні схеми, які можуть пропонувати кращий захист від різноманітних типів криптоаналітичних атак. Дослідження в області постквантової криптографії також виявили, що певні криптосистеми, засновані на неабелевих групах, можуть бути стійкими до атак з використанням квантових комп'ютерів. Всебічний аналіз та опис цих унікальних алгебраїчних структур наведено в [25].

Класичні групи – це групи природних матриць. Існує чотири типи для кожного цілого числа $n \geq 2$ і ступеня простого числа q. Наприклад, проективна спеціальна лінійна група $n \times n$ матриць над полем порядку q, позначена $PSL_n(q)$, має ранг $n-1$ і є простою, за винятком випадків, коли $n=2$ і $q=2,3$. Інші класичні групи – це групи унітарних, ортогональних і симплектичних матриць над скінченними полями. Інтерес мають також скінченні квазіпрості класичні групи, наприклад спеціальна лінійна група $SL_n(q)$. З $n=2$ маємо, що $SL_n(2^k) = PSL_n(2^k)$, що є простим для $k>1$. Виняткові групи не мають таких природних представлень, як групи матриць, і всі мають порядок не більше 8. Існує 10 нескінченних сімейств, індексованих ступенями простого числа q, одним з цих сімейств є групи Сузукі, що визначені над полями порядку 2^{2n+1}, які ми позначаємо $Sz(2^{2n+1})$.

З огляду на розв'язання проблеми групової факторизації автори в [26] припустили, що короткі шляхи існують у графах Кейлі кінцевих простих груп. Гіпотеза Бабая полягає в тому, що існує константа $c>0$ така, що для будь-якого h у скінченній простій неабелевій групі G і будь-якій породжуючій множині S існує шлях від 1 до h у $\Gamma(G,S)$ довжиною не більше $(\log|G|)^c$. Тобто кожен елемент G може бути записаний як слово довжини щонайбільше $(\log|G|)^c$ в елементах S. Гіпотеза Бабая для груп Лі обмеженого рангу була доведена. В інших випадках гіпотеза залишається недоведеною. Існують часткові результати, що підтверджують гіпотезу Бабая для певних генеруючих наборів. Зокрема, було доведено гіпотезу Бабая для більшості генеруючих множин знакозмінних груп та продемонстровано що гіпотеза Бабая вірна для груп великого рангу типу Лі з майже всіма достатньо великими множинами S. Гіпотеза Бабая передбачає, що для кожного елемента $h \in G$ існує шлях довжиною $(\log|G|)^{O(1)}$ від 1 до h на графі Кейлі. Важливість цієї гіпотези полягає в її наслідках для криптоаналізу в завданні пошуку таких коротких шляхів.

У області дослідження генеративних наборів, що ускладнюють пошук коротких шляхів, в останні роки отримано багато результатів: оптимізовано алгоритм Шраєра – Сімса для вирішення проблеми факторизації в групах перестановок; запропоновано алгоритм Лас-Вегас, заснований на випадковому блуканні, здатний розкладати на множники елементи A_n для майже всіх множин, а також запропоновано алгоритм, який припускається та експериментально надає ще коротші слова [27].

Було доведено, що кожна скінченна проста неабелева група G має генеруючий набір S розміром не більше семи. Для цього набору існує алгоритм, здатний знайти слова довжиною $O(\log|G|)$ за час, що дорівнює $O(\log|G|)$. Цей результат доводить необхідність пошуку таких генеруючих наборів, які роблять процес побудови коротких шляхів складнішим, збільшуючи складність криптоаналізу.

Групи Лі $PSL_n(q)$ і $SL_2(2^k)$ детально розглянуто в [25], де розроблено ефективні алгоритми для декількох спеціально вибраних генеруючих наборів. Інший підхід включає представлення класичних груп як "груп чорного ящика" та використання алгоритму Лас-Вегас для спроби побудови стандартних генеруючих наборів, які дозволяють вирішувати проблему факторизації. Для всіх генеруючих наборів $SL_2(2^k)$ існує субекспоненціальний алгоритм, що забезпечує слова субекспоненціальної довжини.

Вже було зауважено, що проблема слова може бути NP-повною для певних спеціальних класів груп або в певних умовах, але важливо зазначити, що у загальному випадку для абстрактних груп проблема слова не класифікується як NP-повна. Прикладами скінченно породжених лінійних груп є: скінченно породжені поліциклічні групи, групи Кокстера, групи кіс і групи графів. Отже, для всіх цих груп проблему зі словом можна розв'язати в логарифмічно-

му просторі. Це мотивує зазначити групи, як напрями досліджень, де проблема слова представляє практичний інтерес та може бути NP-повною:

Групи Дена: введені Максом Деном у 1910-х роках. Вони є прикладами фундаментальних груп певних 2-вимірних многовидів і мають властивість, що для деяких з них проблема слова розв'язна, тоді як для інших – ні. Ці групи дозволили глибше зрозуміти, як структура групи впливає на обчислювальні аспекти проблеми слова.

Групи Григорчука: введені у 1980-х роках Ростиславом Григорчуком, ці групи є прикладами груп, що мають властивість проміжного росту. Проблема слова для груп Григорчука була розв’язана.

Групи Баумслага – Солітара: ці групи задаються дуже простими відношеннями, але мають складну структуру та багато властивостей, що забезпечують складність реалізації. Для деяких параметрів конструкції групи Баумслага – Солітара проблема слова є розв'язною, тоді як для інших – вона залишається відкритою або нерозв'язною.

Коксетерові групи: це групи, що генеруються відбиттями, які задовольняють певним відношенням. Для деяких класів Коксетерових груп проблема слова розв'язна.

Групи Тарського: це незліченні групи, введені Альфредом Тарським, для яких проблема слова є нерозв'язною. Складність відношень у цих групах призводить до того, що не існує загального алгоритму для визначення, чи дорівнюють один одному два дані слова.

Гіперболічні групи: визначені Громовим, ці групи мають складні відношення, які відображають їх геометричні властивості. Проблема слова в гіперболічних групах наразі досліджена недостатньо.

Автоматні групи: ці групи можуть бути представлені за допомогою автоматів, що дозволяє моделювати динаміку групових операцій. Складність відношень у таких групах є предметом інтенсивного дослідження, оскільки вона має важливі наслідки для розуміння динамічних систем в математиці.

Спорадичні групи: особливий клас скінченних простих груп, які не належать до жодного з великих сімейств скінченних простих груп, таких як циклічні групи, альтернативні групи або групи Лі. Всього існує 26 спорадичних груп, і вони є досить рідкісні та особливі у світі алгебраїчних структур.

Кожна з цих спорадичних груп має унікальні властивості та структуру, і вивчення цих груп дозволило математикам зробити значний прогрес у розумінні скінченних простих груп та їх застосуваннях у різних областях математики та фізики.

Однак єдиного ефективного алгоритму, який би працював для всіх груп і генераторних наборів, наразі не знайдено. Дослідження груп переважно як комбінаторних структур, що використовують представлення груп через генератори та релятори, є відгалуженням теорії груп, відомої як комбінаторна теорія груп.

Вагнер та Маджарік [28] розробили протокол відкритого ключа, заснований на нерозв’язності проблеми слова для скінченно представлених спорадичних Сузукі 2-груп. Це демонструє, що ідея використання складності неабелевих груп у криптографії не нова. В останні роки ця ідея отримує нові напрями досліджень [5 – 10].

Кілька протоколів некомутативної криптографії, наприклад некомутативний протокол Діффі – Хеллмана Ко-Лі, протокол обміну ключами Аншеля – Аншеля – Голдфельда (AAG Commutator), схема цифрового підпису Кахробай – Коуппаріс і Кахробай – Хан – схема некомутативного шифрування з відкритим ключем Ель-Гамаля базуються на складності проблеми пошуку спряженості в певних запропонованих групах. У [30] автори стверджують, що ця криптосистема з відкритим ключем безпечна, оскільки немає достатньо інформації для визначення ключа w. Криптосистема, представлена вище, була вперше атакована Гофхайнцем і Стейнвандтом у [31]. Однак їхній алгоритм в основному заснований на грубій силі. Пізніше в 2003 р. Петрідес [32] заявив, що цей протокол вразливий, оскільки наданий відкритий ключ дає занадто багато інформації та дозволяє зловмиснику легко отримати закритий ключ. Схема узгодження ключів на основі задачі одночасного пошуку спряженості. Протокол Аншеля – Аншеля – Голдфельда добре відома і базується на складності проблеми одно-

часного пошуку спряженості. У 2019 р. Григорчук і Григор'єв запропонували певні класи груп автоматів для протоколу AAG. Конкретними прикладами, які вони запропонували, є перша група Григорчука та група Базиліка. Безпека цієї системи в цілому полягає в складності варіації проблеми пошуку сполученості в певних групах. Наприклад, Ко-Лі запропонував групи кіс, а Ейк та Кахробай в [33] запропонували поліциклічні групи.

Висновки

Асиметрична криптографія використовує односторонні функції. NP-повні задачі вважаються оптимальними для таких функцій, оскільки вони дозволяють відносно легко генерувати складні для вирішення приклади для яких рішень є складним. Однак, застосування NP-повних задач у криптографії обмежене через труднощі у створенні задач, які би були обґрунтовано складними. У статті детально розглянуто класи NP проблем, визначено основні терміни та концепції, проаналізовано властивості та критерії NP-повноти. Особлива увага приділяється складності NP-повних проблем в контексті квантових обчислень, а також визначенню неабелевих груп, в яких проблема слова вважається NP-повною. Дослідження підкреслює потенційні переваги використання неабелевих груп у криптографії, оскільки проблема слова для цих груп відноситься до класу NP-повних проблем. Проведено огляд останніх досліджень у галузі розробки асиметричних криптографічних примітивів, заснованих на використанні складних для розв'язання проблем у кінцевих групах. Обґрунтовано перспективність цього напрямку в груповій криптографії.

Список літератури:

1. Liu, Yanyi, and Rafael Pass. On one-way functions from NP-complete problems // Cryptology ePrint Archive (2021).
2. Luckow, Andre, Johannes Klepsch, and Josef Pichlmeier. Quantum computing: Towards industry reference problems // Digitale Welt 5 (2021): 38–45.
3. Gilles Brassard. Relativized cryptography // Proceedings of the 20th Annual Symposium on Foundations of Computer Science. 1979. pp. 383–391.
4. Baldo A., Boffa M., Cascioli L., Fadda E., Lanza C., & Ravera A. The polynomial robust knapsack problem // European Journal of Operational Research. 2023. 305(3). 1424–1434.
5. 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.
6. 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.
7. 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
8. 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.
9. 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
10. 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.
11. Suo J., Wang L., Yang S., Zheng W., & Zhang J. Quantum algorithms for typical hard problems: a perspective of cryptanalysis // Quantum Information Processing. 2020. 19. P. 1–26.
12. Vega F. (2023). On Feasibly Solving NP-complete Problems.
13. Causey C. J. (2023). NP-Complete Problems and Public Key Cryptography.
14. Todd J.A., Coxeter H.S.M. A practical method for enumerating cosets of a finite abstract group // Proc. Edinb. Math. Soc., II. Ser. 5, 26-34 (1936). Zbl 0015.10103, JFM 62.1094.02
15. Ball W. W. R., & Coxeter H. S. (2022). Knuth-Bendix Completion Algorithm.
16. Novikov P. S. Algorithmic Unsolvability of the Word Problem in Group Theory.. L. Britton, 1958 // Journal of Symbolic Logic 23 (1):50–52.
17. William W. Boone, Frank B. Cannonito, Roger C. Lyndon, Word Problems, Decision Problems and Burnside Problem in Group Theory. C. R. J. Clapham, 1976 // Journal of Symbolic Logic 41 (4):785–788.

18.Nyberg Brodda, Carl-Fredrik. The word problem and combinatorial methods for groups and semigroups. Diss. University of East Anglia, 2021.
19.Rybalov A. (2020, May). A generic algorithm for the word problem in semigroups and groups // Journal of Physics: Conference Series (Vol. 1546, No. 1, p. 012100). IOP Publishing.
20.Hooshmand M. H. Basic results on an unsolved problem about factorization of finite groups // Communications in Algebra 49.7 (2021): 2927–2933.
21.Alamati, Navid, et al. Cryptographic group actions and applications // Advances in Cryptology–ASIACRYPT 2020: 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7–11, 2020, Proceedings, Part II 26. Springer International Publishing, 2020.
22.Verschaffel L., Schukajlow S., Star J., & Van Dooren W. (2020). Word problems in mathematics education: A survey. ZDM, 52, 1-16.
23.van Veldhuizen, Toon, and Hans Cuypers. Investigating finite simple groups. Master Thesis
24.Singh, Priyanka, Manju Khari, and Nikhil S. Kaundanya. Impact of group theory in cryptosystem // Functional encryption. Cham: Springer International Publishing, 2021. 19–36.
25.Lanel G. H., Jinasena T. M. K. K., & Welihinda, B. A. (2021). A survey of public-key cryptography over non-abelian groups.
26. Kahrobaei D., Flores R., & Noce, M. (2023). Group-based cryptography in the quantum era. Not. Am. Math. Soc, 70(5), 752–763.
27.Vasco, María Isabel González, Delaram Kahrobaei, and Eilidh McKemmie. Applications of Finite non-Abelian Simple Groups to Cryptography in the Quantum Era // arXiv preprint arXiv:2308.14725 (2023).
28.Wagner N.R. and Magyarik M.R. A public-key cryptosystem based on the word problem // Proc. Advances in Cryptology–CRYPTO 1984, LNCS 196, Springer-Verlag (1985), pp. 19–36.
29.Sconza S., & Wildi, A. (2024). Knot-based Key Exchange protocol // Cryptology ePrint Archive.
30.Kahrobaei D., Khan B. A non-commutative generalization of ElGamal key exchange using polycyclic groups // IEEE GLOBECOM Global Telecommunications Conference [4150920], 2006. doi: 10.1109/glocom.2006.
31.Hofheinz D., & Steinwandt R. (2002). A practical attack on some braid group based cryptographic primitives // Public Key Cryptography—PKC 2003: 6th International Workshop on Practice and Theory in Public Key Cryptography Miami, FL, USA, January 6–8, 2003 Proceedings 6 (pp. 187–198). Springer Berlin Heidelberg.
32.Petrides G. (2006). Cryptographic applications of non-commutative algebraic structures and investigations of nonlinear recursions. The University of Manchester (United Kingdom).
33.Eick B., & Kahrobaei D. (2004). Polycyclic groups: a new platform for cryptology? // arXiv preprint math/0411077.
34.Kuperberg G. (2005). A subexponential-time quantum algorithm for the dihedral hidden subgroup problem // SIAM Journal on Computing. 35(1). 170–188.

Надійшла до редколегії 10.03.2024

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 технічних видів розвідки та інформаційних технологій 2-го навчального інституту Воєнної академії імені Євгенія Березняка Міністерства оборони України; Київ, Україна; e-mail: mars_kor@ukr.net; ORCID: https://orcid.org/0000-0001-8049-4730,
Руденко Михайло Миколайович – канд. техн. наук, доцент, доцент 2-ї кафедри технічних видів розвідки та інформаційних технологій 2-го навчального інституту Воєнної академії імені Євгенія Березняка Міністерства оборони України; Київ, Україна; e-mail: ruminik33@ukr.net; ORCID:https://orcid.org/0000-0002-9180-1510
Любчак Володимир Олександрович – канд. фіз.-мат. наук, доцент, завідувач кафедри кібербезпеки Сумського державного університету; e-mail: v.liubchak@dcs.sumdu.edu.ua; ORCID: https://orcid.org/0000-0002-7335-6716
Мацюк Сергій Михайлович – канд. техн. наук, доцент, доцент кафедри кібербезпеки; Національний технічний університет «Дніпровська політехніка»; Дніпро, Україна; e-mail: matsiuk.s.m@nmu.one; ORCID: https://orcid.org/0000-0001-6798-5500
Чащин Максим В'ячеславович – аспірант; Національний технічний університет «Дніпровська політехніка»; Дніпро, Україна; e-mail: mchaschin@gmail.com; ORCID: https://orcid.org/0009-0004-4671-0443

УДК 621. 396:004.056.5 **DOI:10.30837/rt.2024.1.216.06**

А.М. ОЛЕЙНІКОВ, канд. техн. наук, Ю.В. ЛИКОВ, канд. техн. наук,
В. І. ЗАБОЛОТНИЙ, канд. техн. наук

ОЦІНКА ПОХИБКИ ЛОКАЛІЗАЦІЇ РАДІОАКУСТИЧНИХ ЗАКЛАДНИХ ПРИСТРОЇВ ЗАСОБАМИ АКУСТИЧНОЇ ДАЛЕКОМЕТРІЇ

Вступ

Локалізація радіоакустичного закладного пристрою (РАЗП) – це визначення його місця розташування у просторі. Локалізація РАЗП може здійснюватися як по електромагнітному полю, так і із застосуванням акустичних зондувальних сигналів [1 – 4]

Локалізація по електромагнітному полю здійснюється за допомогою рознесених у просторі антен. Може бути як пасивною, так і активною. При цьому антени розміщують у різних точках приміщення, після чого, вимірюючи рівень сигналу РАЗП на кожній антені, визначають антену з максимальним рівнем. Ділянка розташування антени досліджується або візуально, або за допомогою спеціальної техніки (індикаторів поля, нелінійних локаторів тощо). Слід зазначити, що цей метод надає приблизну оцінку місця розташування РАЗП, і подальші пошуки РАЗП спеціальними засобами може зайняти деякий час.

Метод локалізації за допомогою акустичних зондувальних сигналів дозволяє визначити координати точки (з деякою похибкою) у просторі, де розташовано РАЗП. При цьому використовується двовимірний або тривимірний тріангуляційний метод визначення місця розташування РАЗП. Подальшій пошук додатковими спеціальними засобами поблизу цієї точки може значно зменшити час на проведення пошукових операції.

Як метод локалізації радіоакустичного закладного пристрою із використанням акустичних сигналів може застосовуватися спосіб акустичної зав'язки, який у цій роботі не розглядається.

Локалізація із застосування акустичних зондувальних сигналів здійснюється за допомогою акустичного далекоміра (АД) у складі апаратно-програмного комплексу (АПК) для виявлення РАЗП (наприклад АПК «ОРТ»,«VOSTOK») [3,4]. Ця функція наявна не в усіх АПК.

Структурну схема акустичного далекоміра АПК «VOSTOK» і схему його увімкнення показано на рис. 1.

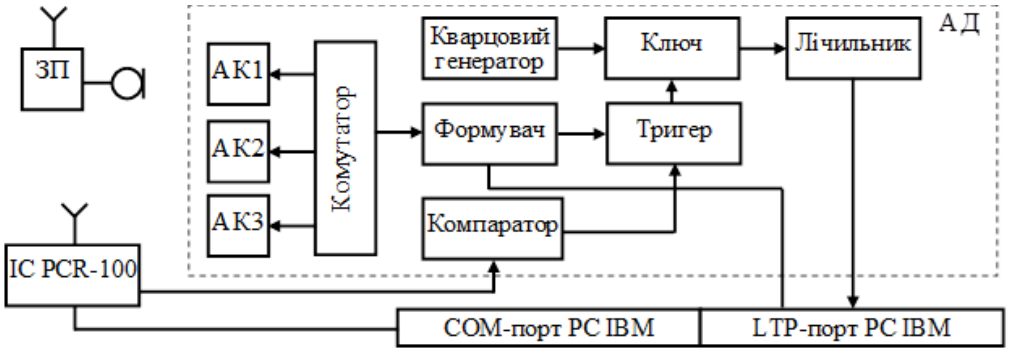


Рис. 1. Структурна схема акустичного далекоміра АПК «VOSTOK»

АД є окремим пристроєм, який формує акустичну хвилю і вимірює час поширення акустичного сигналу до РАЗП. Результат вимірювань вводиться до ПК для подальшої обробки.

Принцип роботи АД наступний. Акустична колонка (АК) відтворює звукове клацання (зондуючий акустичний сигнал). Акустична хвиля із сферичним фронтом, поширюючись у

просторі, через певний час t надходить до мікрофону РАЗП, який перевипромінює прийнятий імпульс по радіоетеру. Часом поширення радіохвилі до РАЗП нехтують. Сигнал приймається приймачем і демодулюється у відеоімпульс. Якщо вимірювати час *t* від клацання до появи цього відеоімпульсу на виході приймача і помножити час t на швидкість звуку, то вийде відстань до РАЗП. Причому чим точніше виміряно час, тим точніше обчислюється відстань.

Одне вимірювання дає радіус сфери, на будь-якій точці поверхні якої може перебувати РАЗП. Якщо вимірювання виконати з двох рознесених точок, то РАЗП буде розташована на колі, що є лінією перетинання цих двох сфер. Однозначно визначити місце розташування можна, вимірюючи відстань до РАЗП з трьох рознесених точок, що лежать, наприклад, на вершинах рівнобічного трикутника.

Розглянута методика апаратно реалізована у деяких АПК за допомогою звукової карти з використанням однієї рухомої колонки, що не надто зручно. При цьому одночасно відтворюється wave-файл і записується сигнал з лінійного входу звукової карти, але виникає проблема синхронізації часу між початком операції читання даних з приймача і часом початку звукового тесту. Обидві операції ініціюються програмно, і значення часового інтервалу між ними залежить від потужності комп'ютера, обсягу буфера драйверів звукової карти, мультизадачного середовища Windows тощо. Досвід свідчить, що цей інтервал у деяких комп'ютерах може досягати суттєвих значень, перераховуючи у відстань – до 20 м.

Щоб уникнути зазначених вище проблем, в АПК «VOSTOK» АД реалізовано апаратно як окремий пристрій, який виконує функції формування клацання і точного визначення часу поширення акустичного сигналу, а результат вводиться у комп'ютер для подальшої обробки. АД містить кварцовий генератор, лічильник, одновібратор (для формування клацання), компаратор (для формування прямокутного імпульсу зупинки лічення з відеоімпульсу на тлі шуму, що надходить з виходу приймача), три акустичні колонки. Керування пристроєм здійснюється від комп'ютера через стандартний паралельний порт.

Оцінка похибки локалізації РАЗП комплексом «VOSTOK»

Похибка вимірювання координат РАЗП акустичним далекоміром складається з апаратурної та випадкової похибок вимірювання дальності, а також методичної похибки визначення місця розташування РАЗП, яка обумовлена особливостями далекомірного методу визначення координат [3, 4].

Апаратурна похибка вимірювання дальності обумовлена, насамперед, скінченним значенням кроку дискретизації лічильних імпульсів кварцового генератора АД, яка не перевищує 1 см при вибраній частоті 40 кГц. Цю похибку можна зменшити на порядок, але у цьому немає сенсу через наявність значної випадкової похибки, яка викликана шумами. Апаратурна похибка вимірювання дальності через варіацію швидкості поширення звуку в повітрі у межах 332 – 344 м/с при змінюванні температури від 0° до 20° С надто мала і може не враховуватися.

Часова фіксація імпульсів за положенням одного з фронтів

Часова фіксація імпульсів за положенням фронтів є найбільш розповсюдженою.

В АД фіксація часового положення імпульсу може здійснюватися по передньому фронту прийнятого сигналу з використанням компаратора, який виявляє сигнал відносно порогової напруги порівняння. Внаслідок впливу шуму точка фіксації часового положення імпульсу зміниться, що спричинює появу випадкової похибки вимірювання дальності.

Середньоквадратичне значення шумової похибки σt1 прямо пропорційне діючому значенню шуму і обернено пропорційне крутості фронту імпульсу в точці порівняння сигналу та порогу. Середньоквадратичну помилку визначення часового положення імпульсу на виході лінійного амплітудного детектора можна знайти із виразу [5]

$$\Delta\tau_1 = \frac{\sigma_{t1}}{\sqrt{n}} = \frac{T_\text{ф}}{q\sqrt{2n}}, \qquad (1)$$

де q – відношення С/Ш на вході детектора; n – кількість імпульсів для лічення; $T_ф$ – тривалість фронту сигнального імпульсу.

Помноживши $\Delta\tau_1$ на швидкість звуку, можна знайти середньоквадратичну помилку σ_d визначення дальності до РАЗП:

$$\sigma_d = \frac{c}{\sqrt{2 \cdot n} \cdot q \cdot \Delta f}, \tag{2}$$

де Δf – смуга пропускання приймача; с – швидкість звука.

Точно визначити $T_ф$ складно, оскільки на його форму впливає АЧХ акустичного випромінювача, мікрофона РАЗП, кількість та взаємне розташування меблів у приміщенні, а також смуга пропускання приймача.

У програмі підтримки АД передбачена можливість оперативного регулювання рівня сигналу, який надходить зі сканувального приймача, а в апаратній частині використовують індикатор перевищення порогового рівня U_0, що дозволяє швидко адаптувати АД до конкретного РАЗП.

Розрахунки показують, що в найгіршому випадку середньоквадратична похибка визначення відстані від акустичної колонки до РАЗП при правильному настроюванні роботи АД становить декілька сантиметрів.

Зазвичай за часове положення сигналу беруть положення точки перетинання певного рівня порівняння U_0 з переднім фронтом імпульсу. Цей спосіб фіксації застосовують як в радіолокації, так і при імпульсному радіозв'язку. Розповсюдженість методу обумовлена його простотою.

Під впливом малого шуму виникає помилка фіксації часового положення імпульсу. Середньоквадратичну помилку відліку визначають за формулою (1).

Для розглянутого способу фіксації імпульсів обчислюють ширину смуги пропускання фільтра перед детектором Δf_0, яка забезпечує мінімум помилки (1) [5]:

$$\Delta f_0 \approx \frac{1}{T_{ф0}}, \tag{3}$$

де $T_{ф0}$ – тривалість фронту імпульсу на вході фільтра.

Формулу (1) при оптимальній смузі (3), враховуючи $\sigma_0 = \sqrt{N_0 \cdot \Delta f_0}$ можна записати:

$$\Delta\tau_1 = \frac{\sqrt{N_0 \cdot \Delta f_0}}{U_{c0}} \cdot \frac{T_ф}{T_{ф0} \cdot \sqrt{n}} \cdot \frac{1}{\sqrt{n}}, \tag{4}$$

де U_{c0} – амплітуда сигнальних імпульсів на вході приймача.

З порівняння виразів (1) і (4) видно, що помилка (4) більша ніж гранична у $\sqrt{2} \cdot T_Ф / T_{Ф0}$ разів. Якщо перед детектором увімкнено ідеальний смуговий фільтр зі смугою $\Delta f_0 = 1/T_{Ф0}$, тоді $T_Ф / T_{Ф0} = 1,2$ і збільшення становить $\sqrt{2} \cdot 1,2 = 1,7$. Для імпульсів, у яких тривалість фронту близька до повної тривалості ($T_{Ф0} \approx T_{c0}$), втрати точності відліку збільшуються. Так, для імпульсу дзвіноподібної форми обчислено, що часова помилка відліку за точкою перетинання переднього фронту з рівнем 0,607 від амплітуди імпульсу, виходить у 2,08 рази більшою ніж гранична (імпульс пройшов крізь дзвіноподібний фільтр зі смугою у $\sqrt{3}$ разів ширшою спектра сигналу).

Головний недолік методу фіксації імпульсів по фронту в тому, що навіть за відсутності шуму можуть виникати значні часові помилки внаслідок змінювання амплітуди сигнальних імпульсів. Для зменшення цих помилок необхідно разом із зміною амплітуди імпульсів відповідно змінювати і величину рівня порівняння U_0. Особливо негативно впливають швидкі зміни амплітуди сигнальних імпульсів. Існує кілька способів автоматичного встановлення рівня порівняння, наприклад:

- фіксація положення імпульсу за положенням заднього фронту, встановлюючи попередньо рівень за амплітудою чергового прийнятого імпульсу;

- фіксація положення імпульсу дзвіноподібної форми за точкою перетинання обвідної сигналу з її похідною.

Однак існують випадки, коли рівень порівняння не вдається встановити за амплітудою сигналу, а потрібно встановлювати за рівнем шуму, як наприклад, у випадку сигналу у вигляді кодованих груп імпульсів. У цих умовах метод фіксації імпульсів по фронту стає незадовільним.

Часова фіксація імпульсів за положенням обох фронтів

Часова фіксація імпульсів за положенням обох фронтів сигналу є більш досконалою.

Зручним є спосіб фіксації, при якому за часове положення сигналу беруть середину часового інтервалу між точками перетинання постійного рівня U_0 з фронтами сигнального імпульсу (рис. 2, точка t_0).

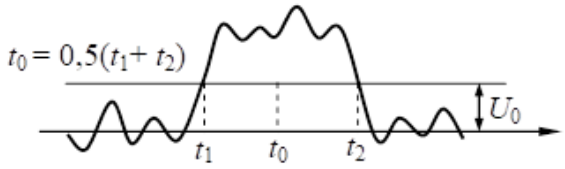


Рис. 2. Спосіб часової фіксації імпульсів
за положенням обох фронтів

Положення точки t_0 пов'язано із положенням фронтів t_1 і t_2 співвідношенням

$$t_0 = \frac{1}{2} \cdot (t_1 + t_2). \tag{5}$$

Якщо часові флуктуації точок t_1 і t_2 мають однакову дисперсію ($\sigma_{t1}^2 = \sigma_{t2}^2$), то дисперсія точки t_0:

$$\sigma_{t0}^2 = \frac{1}{2}\sigma_{t1}^2 \cdot (1 + R_{1,2}), \tag{6}$$

де $R_{1,2}$ – коефіцієнт взаємної кореляції точок t_1 і t_2.

У випадку, коли флуктуації точок обумовлені стаціонарним малим шумом з коефіцієнтом автокореляції $r(\tau)$, у формулу (6) замість $R_{1,2}$ потрібно підставляти $-r(T_c)$ (T_c – тривалість сигнального імпульсу на рівні U_0). Знак мінус враховує обставину, що при збільшенні миттєвого значення шуму на передньому і задньому фронтах точки t_1 і t_2 зміщуються в різних напрямах.

При визначенні часового положення імпульсів приблизно трапецеподібної форми, які виникають на виході лінійного амплітудного детектора і мають тривалість обох фронтів $T_Ф$, середньоквадратична помилка відліку на підставі співвідношень (1) і (6) становить

$$\Delta\tau_0 = \frac{T_\phi}{2q}\left[1 - r(T_c)\right] \cdot \frac{1}{\sqrt{n}}. \tag{7}$$

У випадку оптимальної смуги пропускання фільтра перед детектором (3) і достатньо великому значенні T_c, коли $r(T_C) \approx 0$, формулу (7) з урахуванням рівності $\sigma_0^2 = N_0 \cdot \Delta f_0$ записують у вигляді

$$\Delta\tau_0 = \frac{1}{\sqrt{2}} \frac{\sqrt{N_0 \cdot \Delta f_0}}{U_{c0}} \cdot \frac{T_\phi}{T_{\phi 0}} \cdot \frac{1}{\sqrt{n}}. \tag{8}$$

Помилка (8) перевищує граничну в $T_Ф / T_{Ф0}$ разів, тобто не більше ніж на 20 %. При розглянутому способі відліку приблизно такі ж втрати виходять і для сигналів, у яких $T_{Ф0} \approx T_{c0}$. Це пов'язано з урахуванням кореляції точок t_1 і t_2. Так, для згаданого під час обґрунтування

формули (4) випадку імпульсу дзвіноподібної форми, за тих самих умов, але при відліку за обома фронтами, помилка буде більшою, ніж гранична лише у $2,08\cdot\left[1-r(T_c)\right]/\sqrt{2}=2,08\cdot 0,8/\sqrt{2}=1,18$ разів.

Головна перевага фіксації імпульсів за обома фронтами порівняно із фіксацією за одним фронтом полягає у меншому впливі змінювань амплітуди сигналу на часове положення точки $t0$. Якщо сигнальні імпульси мають симетричну форму, то вплив змінювань амплітуди загалом виключається. Рівень порівняння можна встановлювати постійним і таким, щоб послабити вплив викидів шуму. Недоліком методу є певне ускладнення його технічної реалізації.

Часова фіксація імпульсів за положенням максимальних значень сигналу

Часова фіксація імпульсів за положенням максимальних значень сигналу є особливо цікавою. При узгодженій фільтрації сигнальних імпульсів часова помилка відліку стає сумірною із теоретично досяжною. Важливо також, що відношення сигналу до шуму на виході узгодженого фільтра, як відомо, є максимальним. Тому визначення положення сигналу за положенням максимальних значень дозволяє поєднувати граничну точність з найбільшою надійністю.

Положення максимуму реалізації сигналу і шуму, що виникає на виході узгодженого фільтра, іноді визначають за положенням нуля її похідної. При цьому складно відрізнити головний максимум від побічних, які обумовлені викидами шуму. Доводиться здійснювати попередню часову селекцію головного максимуму. Більш зручним є такий спосіб: сигнал, який пройшов узгоджений фільтр і детектор (рис. 3, *а*), обмежується знизу на рівні U0 і потім диференціюється (рис. 3, *б*).

Далі сигнал надходить на підсилювач та двобічний обмежувач. В результаті виходить імпульс виду рис. 3, *в*. Якщо від'ємною ділянкою цього імпульсу запустити генератор, на виході буде імпульс, передній фронт якого збігається з положенням максимуму сигнального імпульсу (рис. 3, *г*). Встановлюючи потрібний рівень обмеження U_0, при цьому способі можна простими технічними засобами ефективно послабити вплив викидів шуму, які не перевищують рівень обмеження, зберігаючи притаманну методу високу точність часової фіксації.

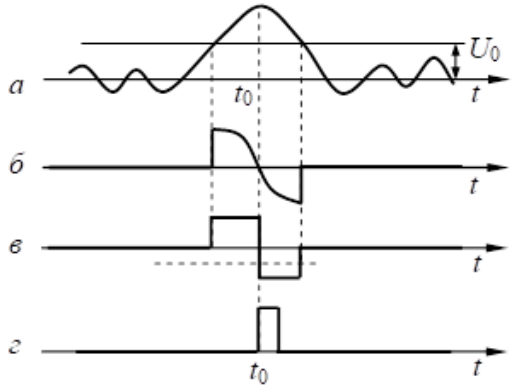


Рис. 3. Спосіб часова фіксації імпульсів за положенням максимальних значень сигналу

Переваги методу часової фіксації положенням максимальних значень по суті досягаються завдяки точним відомостям про форму та тривалість сигнальних імпульсів. Інакше неможливо побудувати узгоджений фільтр. При фіксації за фронтами можна загалом не мати попередньої інформації про тривалість сигнальних імпульсів, тому ці методи не виключають один одного.

Часова фіксація імпульсів кореляційним методом

Кореляційний метод фіксації часового положення імпульсів полягає у такому:

1) прийнятий сигнал демодулюється ;

2) визначається спектр прийнятого сигналу і акустичного сигналу, що надсилається;

3) обчислюється взаємна кореляційна функція (ВКФ) цих сигналів шляхом перемноження їхніх спектрів і застосування швидкого оберненого перетворення Фур'є;

4) визначення положення максимуму ВКФ, що і визначає положення імпульсу.

Головною перевагою цього методу є те, що при визначенні часового положення використовується енергія всього імпульсу, тому максимум ВКФ явно виражений. Працездатність методу зберігається і при достатньо низьких значень співвідношення сигнал/шум (с/ш). Фактично, граничне значення с/ш визначається величиною, яка необхідна для правильного детектування імпульсу.

Ще однією перевагою кореляційного методу є незалежність результату від флуктуацій амплітуди імпульсу, а отже – його висока стабільність та повторюваність результатів.

Недоліком методу є великий обсяг математичних обчислень, пов'язаних з перетворенням Фур'є. Але цей недолік легко усунути, застосовуючи сучасні комп'ютери.

Експериментальні дослідження похибки визначення розташування РАЗП

Для оцінки переваги кореляційного методу порівняно з пороговим проведено експериментальні дослідження та комп'ютерне моделювання похибки визначення місця розташування РАЗП. Експеримент був проведений на АПК "VOSTOK" з використанням цих двох методів [3, 4]. Комп'ютерне моделювання здійснювалось у математичному пакеті MathCAD.

Для порогового методу було змодельовано одиночний імпульс тривалістю 25 мс і тривалістю фронту 1 мс і взята вибірка обсягом 100. Пороговий рівень встановлено на 80 % от амплітуди імпульсу. Вибіркові значення змішувалися з нормальним шумом ($m_x = 0$, $\sigma_x = 1$), і реєструвалося часове положення зашумленого імпульсу залежно від співвідношення с/ш (по 100 «дослідів» на кожне значення с/ш). Співвідношення с/ш змінювалося від 1 до 20 з кроком 1. Для кожного значення с/ш визначалося середньоквадратичне відхилення оцінок місця розташування РАЗП.

Для моделювання кореляційним методом використано такий самий імпульс. Із нього отримано два імпульси (від РАЗП і комутатора) шляхом їх змішування з двома масивами нормально розподіленого шуму ($m_x = 0$, $\sigma_x = 1$). Далі обчислено ВКФ і визначено положення її максимуму залежно від співвідношення с/ш.

Залежності змінювання СКВ оцінок місця розташування РАЗП від співвідношення с/ш на вході приймача для двох методів визначення координат РАЗП (порогового (1) і кореляційного (2)) показано рис. 4.

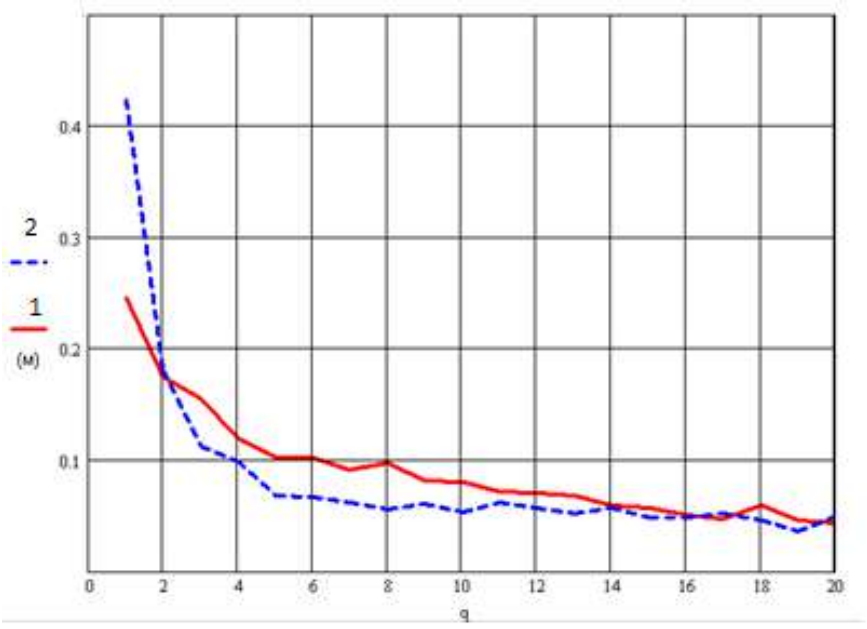


Рис. 4. Залежність СКВ оцінок місця розташування РАЗП від співвідношення с/ш

Із рис. 4 видно, що похибка кореляційного методу менше похибки порогового методу в діапазоні співвідношення с/ш від 2 до ~20. Це обумовлено тим, що у пороговому методі реєстрація часового положення імпульсу здійснюється по передньому фронту. При цьому незначні шумові флуктуації призводять до значних похибок. У кореляційному методі використовується енергія всього сигналу (розраховується ВКФ імпульсів, прийнятих по акустичному і радіоканалу), тому максимум імпульсу є явно вираженим, що дозволяє визначити його часове положення з малою похибкою. При великих співвідношеннях с/ш невеликі шумові флуктуації слабко впливають на точність фіксації часового положення імпульсу пороговим методом, тому результати обох методів стають практично ідентичними.

Експеримент проводився з використанням акустичного далекоміра АПК "VOSTOK" [3, 4].

Експериментальні залежності СКВ визначення місця розташування РАЗП від відстані від АД до РАЗП і кута між напрямком на РАЗП і перпендикуляром до площини АД для порогового (1) і кореляційного (2) способу фіксації часового положення імпульсу показано на рис. 5 і 6. (3 – розрахункова крива).

Як видно з рис. 5 і 6, експериментальні криві для порогового і кореляційного методів повторюють теоретичну криву (3) , яка розрахована згідно з формулою

$$\sigma_{\text{мп}} = \frac{\sqrt{\sigma_1^2 + \sigma_2^2}}{\sin\alpha}, \tag{9}$$

де σ_i – СКВ похибки визначення дальності від *i*-ї колонки; α – кут між лініями положення, який у свою чергу залежить від відстані від АД до РАЗП і кута між напрямком на РАЗП і перпендикуляром до площини АД.

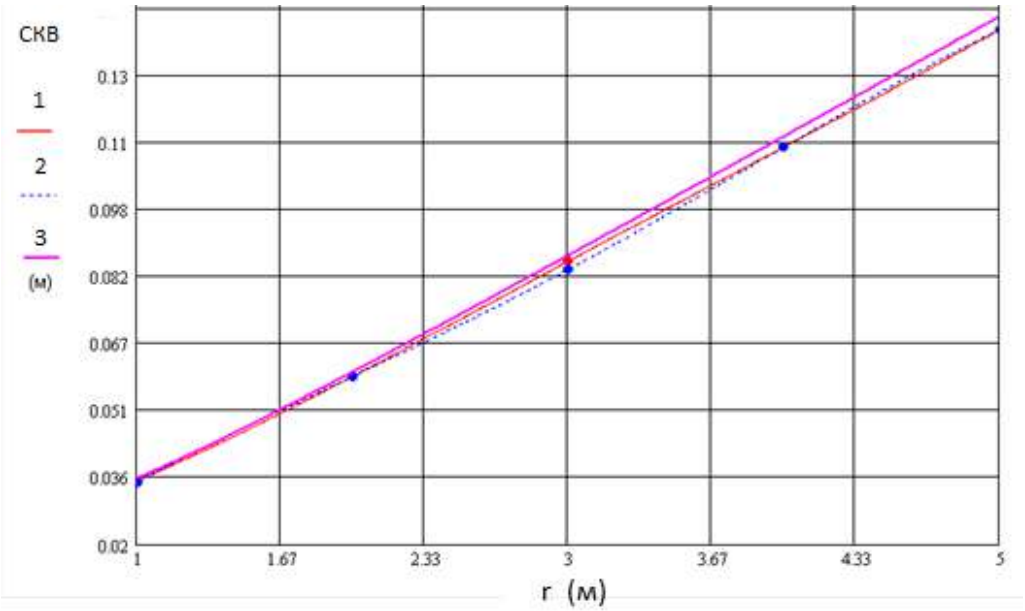


Рис. 5. Залежності СКВ похибки визначення місця розташування РАЗП від відстані від АД до РАЗП

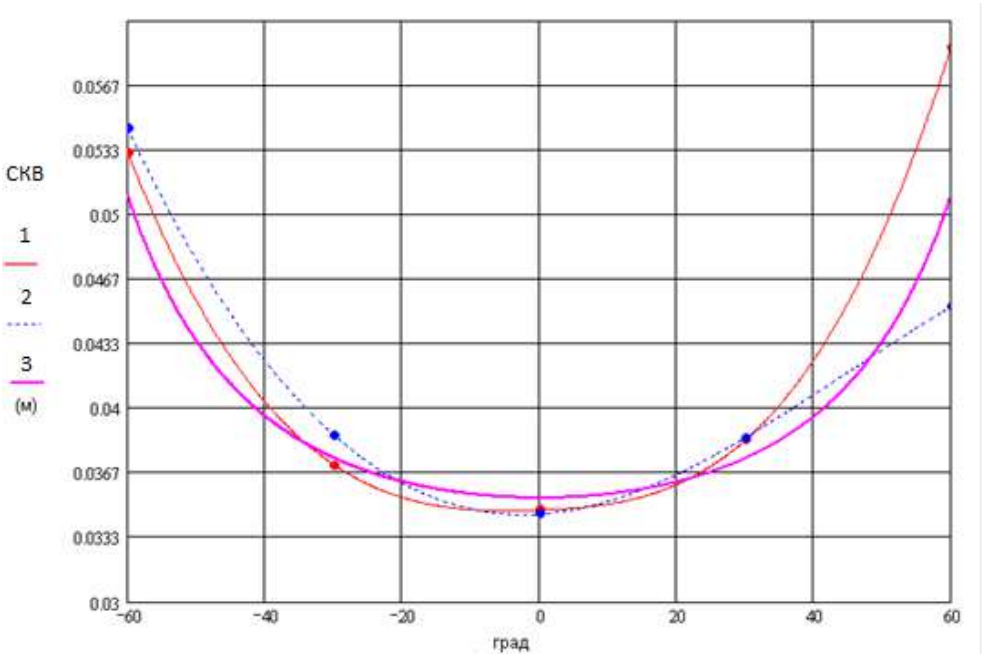


Рис. 6. Залежності СКВ похибки визначення місця розташування РАЗП від кута між напрямком на РАЗП і перпендикуляром до площини АД

Висновки

При локалізації закладних пристроїв, що використовують амплітудну або частотну модуляцію, за допомогою акустичного далекоміра доцільно використовувати кореляційний метод фіксації часового положення імпульсів. При цьому відмічається:

- зменшення середньоквадратичного відхилення похибки локалізації порівняно з пороговим методом на 15 % у діапазоні значень с/ш від 2 до 20;
- висока стабільність результатів;
- мала чутливість до змін амплітуди сигналу, що приймається

Список литературы:

1. Sathyamoorthy D., Jalis M., Md Jelas, Shalini Shafii. Wireless spy devices // A review of technologies and detection methods. November Defence S and T Technical Bulletin 7(2). 2014. 130–139 p. (https://www.researchgate.net/publication/267751871)

2. Пошук та локалізація радіозакладних пристроїв / В.О.Хорошко, О.Д.Азаров, Г.О.Максименко, Ю.Є.Яремчук. Вінниця : ВНТУ, 2007. 333 с.

3. Олейніков А.М., Коваль В.П. Особливості застосування апаратно-програмних комплексів для виявлення та локалізації закладних пристроїв // Захист інформації. Київ, 2002. N 3. С.28–36.

4. Засоби та системи технічного захисту інформації / І.Є. Антіпов, А.М. Олейніков, Ю.В. Ликов, В.Д. Кукуш, І.О. Милютченко. Харків : ХНУРЕ, 2019. 216 с.

5. Мітяшов Б.М. Визначення часового положення імпульсів за наявності перешкод. Москва : Рад. радіо, 1962. 200 с.

Надійшла до редколегії 07.02.2024

Відомості про авторів:

Олейніков Анатолій Миколайович – канд. техн. наук, професор, Харківський національний університет радіоелектроніки, професор кафедри комп'ютерної радіоінженерії та систем технічного захисту інформації, Україна; e-mail: anatoly.oleynikov@nure.ua; ORCID: https://orcid.org/0000-0002-4458-8833

Ликов Юрій Володимирович – канд. техн. наук, доцент, Харківський національний університет радіоелектроніки, доцент кафедри комп'ютерної радіоінженерії та систем технічного захисту інформації; Україна; e-mail: yurii.lykov@nure.ua; ORCID: https://orcid.org/0000-0001-7120-3276

Заболотний Володимир Ілліч – кандидат технічних наук, доцент, Харківський національний університет радіоелектроніки, професор кафедри безпеки інформаційних технологій, Україна; email volodymyr.zabolotnyi@nure.ua; ORCID:0000-0003-3258-8489

УДК 551.501.7 **DOI:10.30837/rt.2024.1.216.07**

В.В. СЕМЕНЕЦЬ, д-р техн. наук, О.В. ГРИГОР'ЄВ, канд. техн. наук

ПРОГРАМНО-АПАРАТНИЙ КОМПЛЕКС НА БАЗІ МІКРОКОНТРОЛЕРА STM32F407VG ДЛЯ ДОСЛІДЖЕННЯ ВІБРАЦІЙ АКСЕЛЕРОМЕТРОМ LIS3DSH

Вступ

Сучасні технологічні процеси потребують безперервного контролю за багатьма параметрами технологічного обладнання. Одними з найважливіших є механічні параметри, зокрема механічні вібрації досліджуваного об'єкта.

Подібний контроль необхідний в різних областях науки та техніки. Наприклад, в напівпровідниковій електроніці – для контролю вібрації установок вирощування кристалів, а в мікроелектроніці – для контролю вібрацій установок фотолітографії. В машинобудуванні такий контроль використовується для визначення вібрацій верстатів, а в автомобільній промисловості – щоб контролювати вібрації окремих вузлів автомобіля і всього автомобіля в цілому. На залізничному транспорті контролюють вібрації, щоб визначити наближення поїзда, в енергетиці – для контролю вібрації лопаток газових турбін та контролю вібрацій в газопроводах, а в авіабудуванні – щоб контролювати політ і т.д.

Отже, розробка систем, призначених для моніторингу та аналізу вібрацій технічних об'єктів, є актуальним питанням сьогодення.

Аналіз літературних джерел та постановка проблеми вібраційної діагностики обладнання

Розробленню систем моніторингу та аналізу вібрацій присвячено різні науково-технічні статті. Зокрема, в [1] розроблено систему моніторингу та аналізу вібрацій, що виникають в електромоторах. Система використовує п'єзоелектричний акселерометр (ICP 603C11) і плату збору даних від National Instruments (NI 6009). Вібраційні сигнали збираються з різних частин електричних моторів і передаються на комп'ютер через плату збору даних. Віртуальний інструмент, що дає змогу в реальному часі моніторити і проводити Фур'є аналіз отриманих сигналів з сенсора вібрацій реалізовано в LabVIEW [3]. В роботі [2] розроблено вбудовану систему для моніторингу вібрацій насосного агрегату на базі мікроконтролера від компанії Microchip. Програмне забезпечення (ПЗ) для збору і аналізу даних оптимізовано для тестування помп з турбонадувом з швидкостями обертання до 2000 об/хв. Автори провели велику кількість вимірювань за допомогою розробленої системи на різних турбоагрегатах для визначення експлуатаційних умов насосних агрегатів [2]. В статті [3] описано метод визначення перемішення та швидкості з сигналів прискорення отриманих з акселерометрів, а в [4] розроблено методику моніторингу надійності мостових конструкцій з використанням МЕМС акселерометри. В [4] побудовано систему моніторингу верстатів і процесів механічної обробки. Система збору вібраційного сигналу базується на мікроконтролері Arduino, який підключено до комп'ютера через USB порт. Спеціальне розроблене ПЗ під LabVIEW зчитує та опрацьовує дані в реальному масштабі часу. В [5] досліджена придатність мікроелектромеханічних (МЕМС) акселерометрів для моніторингу стану верстатів з ЧПК. Тести проведено на реально-діючому верстаті з ЧПК в типовому промисловому цеху. Показано, що МЕМС давачі можуть бути хорошою альтернативою до стандартних сенсорів вібрації, оскільки вони не потребують важких електрометричних підсилювачів. Вибір такого давача має бути зроблений відповідно до вимог застосування і результату тесту на придатність. Ряд авторів використовують мікроконтролери Arduino в апаратно-програмній системі для вимірювання механічних вібрацій [6]. В якості давачів вібрації використано акселерометри ADXL335. Розроблена система використовувалася для дослідження та моніторингу вібрацій вакуумної помпи. Дослідження показали можливість і доцільність розроблення вбудованих

систем моніторингу вібрацій в реальному масштабі часу з використанням недорогого апаратного та ПЗ. Використання іншого типу мікроконтролера наведено в роботах [7 - 8]. Зокрема, запропоновано систему моніторингу вібрацій ротаційних машин, верстатів, яка побудована на мікроконтролері PIC-18F6520 і акселерометрі ADXL322. Проведено дослідження на перевірку можливості реєструвати піки частот появи відмов для різних випадків несправностей. Найкращими підходами і технічними рішеннями серед описаних вище для розв'язання розглядуваного кола задач можна віднести методи, описані в роботах [1, 3]. Методи дослідження грунтувалися на проведенні експериментів з різними технічними об'єктами, що включали вимірювання параметрів вібрації, їх обробку та аналіз за допомогою власно розроблених апаратно-програмних систем. Розроблені системи є закритими та мають високу ціну, що не дає змоги розширювати їх функціональні можливості та модифікацію до відповідних потреб експлуатації. Отже, аналіз існуючих підходів та технічних рішень привів до розроблення якісно нової недорогої відкритої апаратно-програмної системи моніторингу вібрацій в реальному масштабі часу [9 - 14]. Така система має бути побудована на доступних і недорогих комплектуючих, відкритому ПЗ та з можливістю модифікації або розширення її функціональних можливостей відповідно до вимог та області застосування.

Попередні дані

Виходячи з аналізу, проведеного вище, найбільш підходящим варіантом є використання датчиків MEMS типу. Особливістю таких датчиків є малий розмір корпусу та низька ціна. Більшість таких датчиків підтримують інтерфейс SPI. З найбільш сучасних моделей можливо виділити LIS3DSH, який позиціонуються виробником як спеціалізоване рішення для розробки віброметрів промислового обладнання.

LIS3DSH - це датчик руху з цифровим виходом (виготовлений по технології MEMS).

Застосування:

Інтерфейс користувача для керуванням рухом, ігри та віртуальна реальність, крокомір, інтелектуальне енергозбереження для портативних пристроїв, орієнтація дисплея, розпізнавання клацання/подвійного клацання, розпізнавання та реєстрація ударів, контроль і компенсація вібрацій.

Опис

LIS3DSH - це високопродуктивний трьохосьовий лінійний акселерометр із наднизьким енергоспоживанням, що належить до сімейства «нано» з вбудованим кінцевим автоматом, який можна запрограмувати для реалізації автономних програм.

LIS3DSH має повні шкали ±2g/±4g/±6g/±8g/±16g і він здатний вимірювати прискорення зі швидкістю вихідних даних від 3,125 Гц до 1,6Кгц. Можливість самоперевірки дозволяє користувачеві перевірити роботу датчика в кінцевому застосуванні.

Самоперевірка

Самоперевірка дозволяє перевірити працездатність датчика, не переміщаючи його. Функція самотестування вимкнена, коли біт самотестування (ST) запрограмований на «0». Коли біт самотестування запрограмований на «1», до датчика прикладається сила приведення в дію, імітуючи певне прискорення вхідного сигналу. У цьому випадку вихідні сигнали датчика демонструють зміну своїх рівнів постійного струму. Коли самотестування активовано, вихідний рівень пристрою визначається алгебраїчною сумою сигналів, створених прискоренням, що діє на датчик, і електростатичною випробувальною силою.

Інтерфейс шини SPI

LIS3DSH для SPI є веденою шиною. SPI дозволяє записувати та читати регістри пристрою.

Послідовний інтерфейс взаємодіє із зовнішнім світом за допомогою 4 проводів: CS ,SPC, SDI та SDO.

CS - це активація послідовного порту, і вона контролюється головним SPI. Він знижується на початку передачі і повертається до високого в кінці. SPC - це таймер послідовного

порту, і ним керує головний пристрій SPI. Він зупиняється на високому рівні, коли CS є високим (немає передачі). SDI та SDO є відповідно вхідними та вихідними даними послідовного порту. Ці лінії проходять на спадаючому фронті SPC і повинні бути захоплені на наростаючому фронті SPC.

І команди регістру читання, і регістру запису виконуються за 16 тактових імпульсів або кратні 8 у разі читання/запису кількох байтів. Тривалість біта - це час між двома спадаючими фронтами SPC. Перший біт (біт 0) починається з першого спадаючого фронту SPC після спадаючого фронту CS, тоді як останній біт (біт 15, біт 23, ...) починається з останнього спадаючого фронту SPC безпосередньо перед наростаючим фронтом CS.

Біт 0: біт RW. Коли 0, дані DI(7:0) записуються в пристрій. Коли 1, дані DO(7:0) з пристрою зчитуються. В останньому випадку чіп керує SDO на початку біта 8.

Біт 1-7: адреса AD(6:0). Це поле адреси індексованого регістру.

Біт 8-15: дані DI(7:0) (режим запису). Це дані, які записуються на пристрій (спочатку MSb).

Біт 8-15: дані DO(7:0) (режим читання). Це дані, які зчитуються з пристрою (спочатку MSb).

У кількох командах читання/запису додаються додаткові блоки з 8 тактових періодів. Коли біт ADD_INC(CTRL_REG6) дорівнює «0», адреса, яка використовується для читання/запису даних, залишається незмінною для кожного блоку. Коли біт ADD_INC дорівнює «1», адреса, яка використовується для читання/запису даних, збільшується в кожному блоці.

Функції та поведінка SDI та SDO залишаються незмінними.

Опис програмно-апаратного комплексу

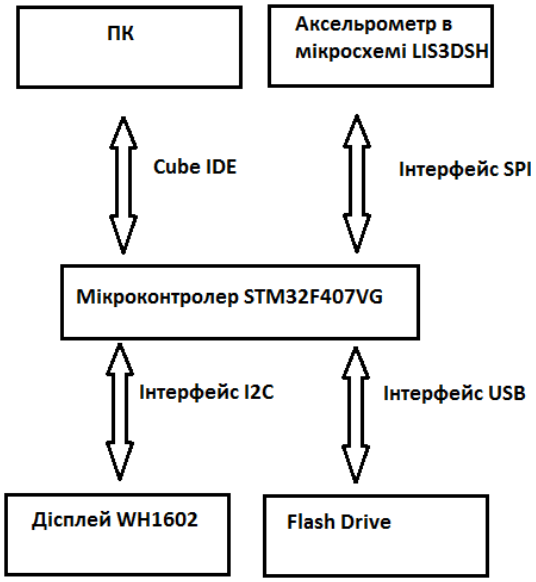


Рис. 1. Структурна схема програмно-апаратного комплексу

Апаратне забезпечення системи побудоване на МК STM32F407VG і трьохосьовому цифровому акселерометрі LIS3DSH (рис. 1). Акселерометр встановлюється на об’єкті моніторингу і підключається по шині SPI до МК. Мікроконтролер збирає дані з давача та їх опрацьовує. Акселерометр використано як давач для вимірювання вібрацій. LIS3DSH – це мініатюрний трьохосьовий цифровий акселерометр фірми STMicroelectronics з малим енергоспоживанням. LIS3DSH відносять до класу ємнісних акселерометрів. Цей прилад є ідеальний для вимірювання динамічних прискорень, низькочастотних вібрацій, статичних прискорень гравітації, руху і кутів нахилу. Смуга пропускання характеризує здатність давача помічати зміни прискорення, що відбуваються з високою частотою (наприклад, вібрація

з частотою 1000 Гц). На цю характеристику впливає частота дискретизації вбудованого АЦП акселерометра, яка повинна бути як мінімум в два рази більше смуги пропускання.

В LIS3DSH виміру максимум виміру – до 16 біт при вимірюванні рискорення ±16 g з постійною чутливістю – 4 mg/LSB у всіх діапазонах вимірювання g. Акселерометр має функції виявлення одиночного та подвійного поштовхів, контролю активності/не активності, функцію виявлення вільного падіння; є можливість гнучкого задання режимів переривання з вибором будь-якого (з 2-х можливих) виводів переривань; зміна діапазону вимірювання, як і смуги пропускання, вибирається подачею відповідної команди. Така вбудована система постійно відслідковує вібрацію, наприклад працюючого верстату, в режимі реального часу і аналізує параметри вібрації. Система видає попереджувальні повідомлення або зупиняє верстат у випадку виникнення неприпустимих вібрацій – запобігаючи таким чином можливі поломки і аварії. Система також має надавати достатню інформацію користувачу, щоб він зміг розпізнати можливі проблеми і прийняти профілактичні заходи на основі аналізу спектру вібрації характерного для конкретного виробу.

Система в змозі своєчасно попередити про ймовірну несправність, що дає можливість користувачу здійснити своєчасні профілактичні заходи.

Моніторинг сумарної вібрації має здійснюватися як в часовому, так і в частотному діапазонах. В часовому діапазоні система безперервно відслідковує стан виробу в режимі реального часу, на основі широкосмугового вимірювання вібро швидкостей, вібро прискорень і вібро переміщень.

В частотному діапазоні може бути встановлений ряд границь попереджуючих і аварійних сигналів для різних частотних діапазонів. Ці діапазони покривають весь спектр вібрації і дають змогу провести аналіз рівня вібрацій в контрольованій області на предмет перевищення допустимих границь по всьому частотному спектрі.

Розроблений алгоритм функціонування системи включає такі кроки:

Крок 1. Ініціалізація акселерометра LIS3DSH на шині SPI;

Крок 2. Зчитування значення з регістра WHO_AM_I і перевірка номера акселерометра;

Крок 3. Налаштування акселерометра LIS3DSH;

Крок 4. Встановлення значень дискретизації та режиму переривань;

Крок 5. Встановлення діапазону вимірювання та розподільної здатності;

Крок 6. Старт вимірювання;

Крок 7. Запис значень у буфер з переривання та очікування заповнення буферу;

Крок 8. Після заповнення буферу використання FIFO для переведення ряду у частотне представлення;

Крок 9. Передача за допомогою USB;

Крок 10. Після передачі початок виконування з кроку 6.

Розроблені наступні функції:

void Accel_Ini (void) – функція ініціалізації датчика;

static void Error (void) – функція-обробник помилки;

Accel IO_Read (uintl6_t DeviceAddr. uint8_t RegisterAddr) – функція читання даних за адресами датчика та регістру;

void Accel_IO_Write (uint16_t DeviceAddr, uint8_t RegisterAddr, uint8_t Value) функція запису даних за адресами датчика та регістру;

uint8_t Accel_ReadID (void) – функція читання адреси мікросхеми;

void Accel_AccFilterConfig(uint8_t FilterStruct) – функція підключення фільтру;

void AccInit(uintl6_t InitStruct) – функція ініціалізації налаштувань;

void Accel_GetXYZ (intl6_t* pData) – функція зчитування показників аксельрометра;

static uint8_t SPIx_Write Read (uint8_t Byte) – функція для прийому та передачі даних по інтерфейсу SPI;

AccInit (ctrl) функцію основної ініціалізації акселерометра.

З DATASHEET отримуємо константи для налаштування системи:

LIS3DSH_DATARATE_100: значення 0x60: даним значенням ми включимо біти ODR1 та ODR2, тим самим налаштуємо швидкість передачі даних 100 герц;

LIS3DSH_XYZ ENABLE: значення 0x07: включимо біти всіх осей, тим самим скажем датчику про те, щоб він нам зчитував дані всіх трьох осей (x, y та z);

LIS3DSH_SERIALINTERFACE_4WIRE: значення 0x00: цей біт відповідає за включення режиму інтерфейсної шини. Залишаємо 0, тим самим ми включимо 4-провідний SPI;

LIS3DSH_SELFTEST_NORMAL: значення 0x00: тут ми позначимо, що не включатимемо біти 1 і 2 (ST1 і ST2), тим самим включимо режим само тестування (звичайний режим);

LIS3DSH_FULLSCALE_2: значення 0x00: біти FSCALE ми також не включаємо, тим самим скажемо акселерометру, щоб він вимірював показання по всіх осях в межах від -2G до +2G;

LIS3DSH_FILTER_BW800 : значення 0x00: біти ширини смуги пропускання фільтра згладжування. Ми їх не встановлюємо, тому ширина смуги пропускання у нас буде 800 герц;

LIS3DSH_SENSITIVITY_0_06G. Тут ми налаштовуємо чутливість датчика до 0.06 mg.

Висновки

Спроєктовано та реалізовано фізичну модель системи, яка включає мікроконтролер, трьохосьовий цифровий акселерометр LIS3DSH, яка характеризується низькою ціною технічного рішення.

Розроблено та реалізовано спеціалізоване ПЗ системи, яке включає драйвер для налаштування, збору і опрацювання даних з акселерометра та відповідне ПЗ для побудови графіків сигналів вібро прискорення в часовій і частотній областях. Побудоване ПЗ дає змогу реалізувати широкі функціональні можливості та є вільно використовуваним.

Побудована система дає можливість проводити аналіз параметрів вібрації з метою передбачення і запобігання можливих аварій, зменшуючи таким чином затрати, пов’язані з виходом із ладу дорогих деталей і вузлів.

Список літератури:

1. Raă G. System for Monitoring and Analysis of Vibrations at Electric Motors / G. Rață, M. Rață // Intern. Journal of Emerging Technology and Advanced Engineering. 2014. Vol. XXI, Is. 3. P. 97–104.
2. Milovančević M. Embedded Systems for Vibration Monitoring / M. Milovančević, A. Veg, A. Makedonski, J. Stefanović Marinović // Facta Universitatis. Series: Mechanical Engineering. 2014. Vol. 12, Is. 2. P. 171–181.
3. Rocha S. M. S. Method to Measure Displacement and Velocity from Acceleration Signals / S. M. S. Rocha, J. F. S. Feiteira, P. S. N. Mendes, U. P. B. Da Silva, R. F. Pereira // Intern. Journal of Engineering Research and Applications. 2016. Vol. 6, Is. 6. P. 52–59.
4. Sekiya H. Technique for Determining Bridge Displacement Response Using MEMS Accelerometers / H. Sekiya, K. Kimura, C. Miki // Sensors. 2016. Vol. 16, Is.2. P. 257. doi: 10.3390/s16020257
5. Goyal D. Development of non-contact structural health monitoring system for machine tools / D. Goyal, B. S. Pabla // Journal of Applied Research and Technology. 2016. Vol. 14, Is.4. P. 245–258. doi: 10.1016/ j.jart.2016.06.003
6. Albarbar A. Suitability of MEMS Accelerometers for Condition Monitoring: An experimental study / A. Albarbar, S. Mekid, A. Starr, R. Pietruszkiewicz // Sensors. 2008. Vol. 8, Is. 2. P. 784–799. doi: 10.3390/ s8020784
7. Hjort, A. Measuring mechanical vibrations using an Arduino as a slave I/O to an EPICS control system / A. Hjort, M. Holmberg. Uppsala University, 2015. 25 p. Not a reprint
8. Chaudary, S. B. Vibration Monitoring of Rotating Machines Using MEMS Accelerometer/ S. B. Chaudary, M. Sengupta, K. Mukherjee // Intern. Journal of Sceintific Engineering and Research. 2014. Vol. 2, Is. 9.
9. Semenetz V.V., Leonidov V.I. Model-structural analysis of combination interference in the problems acoustic sounding of the atmosphere // Telecommunications and Radio Engineering. 2019. Vol. 78, Is. 12. P. 1078–1095. DOI: 10.1615/TelecomRadEng.v78.i12.60
10. Leonidov V.I. Analysis of the models and structure of echo signals of the atmospheric acoustic sounding // Telecommunications and Radio Engineering. 2014. 73(16). P. 1497–1502.
11. Семенець В.В., Леонідов В.І. Використання мікроконтролера stm32f407vg для дослідження амплітудно-частотних характеристик біологічних тканин // Радіотехніка: 2023. Вип. 214. С. 93–99.
12. Програмування мікроконтролерів STM32 в середовищі STM32CubeIDE в прикладах і задачах : навч. посіб. / О. В. Зубков, І. В. Свид, О. В. Воргуль, В. В. Семенець. Дніпро : ЛІРА ЛТД, 2022. 144 с.

13. Аврунін О.Г., Запорожець О.В., Носова Т.В., Семенець В.В // Мікропроцесоры в інформаційно-вимірювальних системах : навч. посіб. Харків : ХНУРЕ, 2015. 180 с. http://openarchive.nure.ua/handle/document/5291

14. Основи реєстрації та аналізу біосигналів : навч. посіб. / О.Г. Аврунін, В.Г. Абакумов, З.Ю. Готра, С.М. Злепко, А.В. Кіпенський, С.В. Павлов, В.В. Семенець. Харків : ХНУРЕ, 2019. 400 с. https://doi.org/10.30837/978-966-659-257-9

15.02.2023

Відомості про авторів:

Семенець Валерій Васильович – д-р техн. наук, професор. Харківський національний університет радіоелектроніки, професор кафедри біомедичної інженерії, Україна; e-mail: valery.semenets@nure.ua; ORCID: https://orcid.org/0000-0001-8969-2143

Григор'єв Олександр Вікторович – канд. техн. наук, доц., Харківський національний університет радіоелектроніки; Україна; e-mail: oleksandr.hryhoryev@nure.ua; ORCID: https://orcid.org/0000-0001-6467-7983

MEANS OF TELECOMMUNICATIONS
ЗАСОБИ ТЕЛЕКОМУНІКАЦІЙ

УДК 621.396.677.49 **DOI:10.30837/rt.2024.1.216.08**

Ю.Ю. КОЛЯДЕНКО, д-р техн. наук, В.О. БАДЕЄВ

МОДЕЛЬ РАННЬОГО ПОПЕРЕДЖЕННЯ ПРО КІБЕРЗАГРОЗИ У МЕРЕЖАХ 5G З ВИКОРИСТАННЯМ МАРКІВСЬКИХ ПРОЦЕСІВ

Вступ

Сучасні безпроводові міські телекомунікаційні мережі мають архітектуру з центральною станцією, яка керує роботою абонентських станцій. Така архітектура є основою технології 5G.

Однією з особливостей таких мереж є складність протоколу підрівня управління доступом до середовища, який відповідає за організацію доступу абонентів до загального каналу зв'язку. Крім того, у таких мережах є багато невизначених частин, у яких стандартизовані лише деякі механізми мережевого взаємодії.

Безпека телекомунікаційних мереж, у яких канал передачі може використовуватися одночасно багатьма користувачами, є особливо важливою проблемою. У безпроводових міських мережах ця проблема ускладнюється тим, що канал зв'язку є загальнодоступним.

Іншими словами, інформація, яка передається в таких мережах, може бути легко перехоплена зловмисниками. Це може призвести до крадіжки персональних даних, фінансових збитків або навіть до порушення безпеки критичної інфраструктури.

Безпека інформації є важливим фактором, який визначає надійність 5G [1 – 5]. Основною загрозою безпеці таких систем є вразливості, особливо в програмних компонентах. Пошук вразливостей у програмних компонентах є складним і трудомістким завданням, яким займаються здійснюють великі компанії та дослідницькі центри. Інформацію про вразливості можна знайти у загальнодоступних джерелах, таких як Open Source Vulnerability Database, Common Vulnerabilities and Exposures та Natioal Vulnerability Database.

Незважаючи на те, що інформація про вразливості програмних продуктів є загальнодоступною, існуючих даних недостатньо для того, щоб кількісно оцінити безпеку цих продуктів за одним загальним критерієм. Також неможливо прогнозувати, наскільки вони будуть захищені від атак у майбутньому. Одна з основних проблем вибору найбільш захищеної конфігурації 5G полягає в складності кількісної оцінки рівня інформаційної безпеки. Крім того, важко обрати адекватні показники для оцінки, які враховують всі фактори, що впливають на успішне проникнення в мережу та розмір потенційних збитків [6 – 8].

Метою цієї статті є вивчення методів оцінки та прогнозування рівня інформаційної безпеки програмних засобів 5G. Ці методи базуються на моделюванні процесів виявлення та усунення вразливостей за допомогою марківських процесів.

Основна частина

Інформаційна безпека може бути порушена відмовами, які впливають на доступність, цілісність або конфіденційність інформації. Ці відмови можуть бути викликані вразливостями – дефектами в програмному або апаратному забезпеченні, які можуть бути використані зловмисниками для отримання несанкціонованого доступу до інформації.

Результати попереднього аналізу процесів виявлення та усунення вразливостей свідчать про те, що їх можна представити як систему масового обслуговування (СМО) з необмеженою довжиною черги. Параметри цієї системи можна визначити на основі статистичних даних про виявлення та усунення вразливостей таким чином [5]:

- кількість каналів обслуговування n залежить від кількості організацій або груп розробників, які відповідають за усунення вразливостей конкретного програм-

ного продукту 5G. У найпростішому випадку може бути достатньо одного каналу обслуговування;

- інтенсивність надходження заявок λ, яка відповідає інтенсивності виявлення вразливостей в програмному продукті 5G, можна оцінити на основі кількості вразливостей, опублікованих за аналізований проміжок часу (тиждень, місяць, рік). Ця оцінка може бути отримана на основі аналізу бази даних вразливостей CVE (первинної бази);
- інтенсивність обслуговування заявок μ, яка відповідає інтенсивності усунення вразливостей (випуску оновлень, що виправляють вразливості), може бути оцінена з використанням інформації з бюлетенів безпеки, що публікуються компаніями-виробниками програмного продукту 5G, а також баз вразливостей NVD та OSVDB (вторинні бази);
- час обслуговування $T_{обсл}$ окремих вразливостей в програмному продукті 5G, який також називають «кількістю днів ризику» [2, 5], визначається як середній період між появою та усуненням цих вразливостей;
- ймовірність того, що заявка на усунення вразливості буде оброблена Q, теоретично дорівнює одиниці. Однак на практиці існують випадки, коли деякі вразливості окремих програмних компонентів не усуваються;
- ймовірність відмови $P_{відм}$ вразливості – це ймовірність того, що вразливість не буде усунена;
- середня кількість заявок в СМО $z_{ср}$ відображає середню кількість вразливостей, які існують в мережі на даний момент часу та для яких ще не випущено програмне оновлення. Цей показник є одним з найважливіших, адже він визначає число потенційних можливостей для атаки на інфокомунікаційну мережу;
- за середньою кількістю заявок в черзі $r_{ср}$ можна судити про те, скільки вразливостей потребують випуску оновлення;
- середній час очікування заявки в черзі $t_{оч.ср}$ показує, скільки в середньому потрібно часу для усунення вразливості з моменту її виявлення;
- середня кількість зайнятих каналів $k_{ср}$ свідчить про те, скільки робочих груп в середньому зайняті виправленням вразливостей. Цей показник дає уявлення про те, наскільки активно ведеться робота з виправлення вразливостей.

Розглянуту вище систему масового обслуговування можна представити у вигляді системи станів, де кожному стану буде відповідати певна кількість виявлених вразливостей, присутніх в системі, для яких ще немає рекомендації або програмного оновлення для їх усунення. Такі вразливості будемо називати активними. Подібні процеси ефективно описуються марківськими ланцюгами. Марківські ланцюги мають порівняно мало інженерних застосувань, тому що досить рідко на практиці моменти можливих переходів системи з одного стану в інший заздалегідь відомі та зафіксовані. Набагато частіше переходи з одного стану в інший можуть відбуватися не в фіксовані моменти часу, а в випадкові.

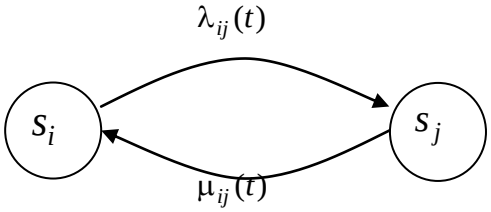


Рис. 1. Перехід із стану S_i в один із сусідніх станів S_j і потім назад в початковий стан під впливом $\lambda_{ij}(t)$ та $\mu_{ij}(t)$

Вважатимемо, що система змінює свій стан під впливом випадкових подій. Ці події відбуваються незалежно одна від одної і слідують пуассонівському закону. Пуассонівський потік не має післядії. Це означає, що ймовірність настання події в майбутньому не залежить від того, що відбувалося в минулому. Знаючи поточний стан системи s_i в момент t, можемо

прогнозувати її майбутню поведінку, не враховуючи, як вона опинилася в цьому стані. Це значно спрощує аналіз поведінки систем, що описуються пуассонівськими потоками.

Нехай на графі станів системи S існує стрілка, яка веде зі стану s_i в один із сусідніх станів s_j (рис. 1).

Вважатимемо, що перехід системи зі стану s_i в стан s_j здійснюється під впливом пуассонівського потоку подій з інтенсивністю $\lambda_{ij}(t)$. Перехід з s_i в s_j відбувається в момент настання першої події потоку.

На осі часу $0t$ виділимо малий проміжок Δt, який примикає до точки t (рис. 2). Знайдемо ймовірність того, що за цей проміжок часу Δt система перейде зі стану s_i в стан s_j, якщо в момент часу t вона знаходилась в стані s_i.

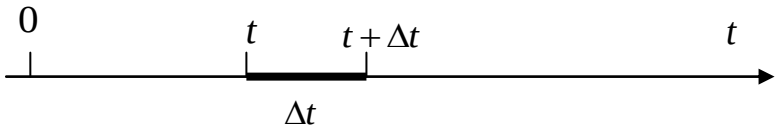


Рис. 2. Елементарний відрізок часу Δt на осі $0t$

Ця ймовірність дорівнює $p_i(t) = \lambda_{ij}(t)\Delta t$, тому що випадкова величина, що дорівнює числу подій потоку, які потрапляють на елементарний відрізок Δt, має математичне очікування $m = \lambda_{ij}(t)\Delta t$, і з точністю до нескінченно малих вищих порядків дорівнює ймовірності p_i попадання на елементарний відрізок однієї події. Знаючи інтенсивності пуассонівських потоків подій, що переводять систему з одного стану в інший, можна сформувати систему диференціальних рівнянь для ймовірностей перебування системи в цих станах.

Для будь-якої пари станів системи s_i, s_j існує інтенсивність $\lambda_{ij}(t)$ пуассонівського потоку подій, що переводять систему зі стану s_i в будь-який інший стан s_j ($i \neq j$). Якщо прямий перехід зі стану s_i в стан s_j неможливий, вважаємо цю інтенсивність нульовою.

Позначимо $p_i(t)$ – можливість, що у момент часу t система перебуває у стані s_i ($i = 1,2,...,n$). Тепер додамо t збільшення Δt і знайдемо ймовірність $p_i(t + \Delta t)$ того, що в момент $t + \Delta t$ система буде перебувати в стані s_i. Позначимо цю подію A: $A = \{S(t + \Delta t) = s_i\}$.

Ця подія може статися двома способами: або станеться подія B, що полягає у тому, що у момент t система вже була у стані s_i, і протягом часу Δt не вийшла із цього стану; або станеться подія C, що полягає у тому, що у момент t система була у одному із сусідніх станів s_j, з яких можливий перехід в s_i і за час Δt перейшла зі стану s_j в s_i.

Вочевидь, $A = B + C$. Знайдемо ймовірність подій B та C. Згідно з правилом множення ймовірностей ймовірність події B дорівнює ймовірності $p_i(t)$ того, що система в момент t була у стані s_i, помноженої на умовну ймовірність того, що за час Δt вона вийде з цього стану, тобто. у сумарному потоці подій, що виводять систему зі стану s_i, не з'явиться жодної події .

Так як сумарний потік подій, що виводить систему зі стану s_i, як і всі його складові, – пуассонівський з інтенсивністю, що дорівнює сумі інтенсивностей доданків: $\sum_{j=1}^{n} \lambda_{ij}(t), i \neq j$,

то умовна ймовірність того, що на ділянці Δt з'явиться хоча б одна подія, дорівнює

$$p_i(t) = \sum_{j=1}^{n} \lambda_{ij}(t)\Delta t, i \neq j,$$

а умовна ймовірність протилежної події

$$1 - \sum_{j=1}^{n} \lambda_{ij}(t)\Delta t .$$

Таким чином,

$$P(B) = p_i(t)\left[1 - \sum_{j=1}^{n} \lambda_{ij}(t)\Delta t\right]. \quad (1)$$

Знайдемо тепер ймовірність події C. Представимо його у вигляді суми несумісних варіантів:

$$C = \sum_j C_j , \quad (2)$$

де підсумовування поширюється на всі стани s_j, з яких можливий безпосередній перехід у s_i. Подія C, з ординарності потоків, вважатимуться несумісними. За правилом складання ймовірностей:

$$P(C) = \sum_j P(C_j). \quad (3)$$

За правилом множення ймовірностей:

$$P(C_j) = p_j(t)\mu_{ji}(t)\Delta t ,$$

звідки

$$P(C) = \sum_{j=1}^{n} p_j(t)\mu_{ji}(t)\Delta t \quad (i \neq j). \quad (4)$$

Отже,

$$P(A) = P(B) + P(C) = p_i(t)\left[1 - \sum_{j=1}^{n} \lambda_{ij}(t)\Delta t\right] + \sum_{j=1}^{n} p_j(t)\mu_{ji}(t)\Delta t$$

Таким чином,

$$p_i(t + \Delta t) = p_i(t)\left[1 - \sum_{j=1}^{n} \lambda_{ij}(t)\Delta t\right] + \sum_{j=1}^{n} p_j(t)\mu_{ji}(t)\Delta t . \quad (5)$$

Віднімаючи з (5) $p_i(t)$, отримаємо збільшення функції на ділянці $t, t + \Delta t$:

$$p_i(t + \Delta t) - p_i(t) = \sum_{j=1}^{n} p_j(t)\mu_{ji}(t)\Delta t - p_i(t)\sum_{j=1}^{n} \lambda_{ij}(t)\Delta t .$$

Поділяючи прирощення функції на приріст аргументу Δt та спрямовуючи $\Delta t \to 0$, отримаємо для ймовірностей $p_i(t)$ систему звичайних диференціальних рівнянь зі змінними коефіцієнтами:

$$\frac{dp_i(t)}{dt} = \sum_{j=1}^{n} p_j(t)\mu_{ji}(t) - p_i(t)\sum_{j=1}^{n}\lambda_{ij}(t) \ . \tag{6}$$

Ці рівняння називаються рівняннями Колмогорова. Перша сума у правій частині формули (6) поширюється на ті значення j, для яких можливий безпосередній перехід із стану s_j в s_i, а друга – на ті значення, для яких можливий безпосередній перехід із стану s_i в s_j.

Усі потоки, що переводять систему S з одного стану в інший, є найпростішими – (стаціонарними пуассонівськими). Системи, у яких відбувається такий процес, називають найпростішими системами. Для найпростішої системи ймовірності станів визначаються рівняннями Колмогорова з постійними коефіцієнтами. Застосуємо перетворення Лапласа до розв'язання системи рівнянь Колмогорова. Позначимо зображення ймовірності стану $p_i(t)$ функцією $\pi_i(x)$:

$$p_i(t) \to \pi_i(x) \, . \tag{7}$$

Тоді системі рівнянь Колмогорова для ймовірностей станів відповідатиме система рівнянь для їх зображень:

$$x\pi_i(x) = \sum_{j=1}^{n}\pi_j(x)\mu_{ji} - \pi_i(x)\sum_{j=1}^{n}\lambda_{ij} + p_i(0) \, , i = 1,2,...,n \, . \tag{8}$$

Звідки

$$\pi_i(x) = \frac{\sum_{j=1}^{n}\pi_j(x)\mu_{ji} + p(0)}{x + \lambda_i} \, , \tag{9}$$

де $\lambda_i = \sum_{j=1}^{n}\lambda_{ij}$.

Таким чином, замість системи однорідних диференціальних рівнянь з постійними коефіцієнтами для ймовірностей станів отримана система однорідних алгебраїчних рівнянь з постійними коефіцієнтами для зображень ймовірностей станів.

Цю систему потрібно вирішувати з урахуванням нормувальної умови

$$\sum_{i=1}^{n} p_i(t) = 1 \, . \tag{10}$$

Отже, одне з рівнянь можна замінити на

$$\sum_{i=1}^{n}\pi_i(t) = \frac{1}{x} \, , \tag{11}$$

яке є зображенням нормувальної умови.

Знаючи інтенсивності λ_{ij} та μ_{ij} появи подій, що породжуються потоком, можна зіміту-вати випадковий інтервал між двома подіями в цьому потоці:

$$\tau_{ij} = -\frac{1}{\lambda_{ij}}\ln(r) \, , \ \tau_{ji} = -\frac{1}{\mu_{ij}}\ln(r) \, .$$

де τ_{ij} – інтервал часу між знаходженням системи в i -му і j -му стані; r – рівномірно розподілене від 0 до 1 випадкове число, яке береться з генератора випадкових чисел (ГВЧ).

Далі, очевидно, система з будь-якого i -го стану може перейти в один із кількох станів j, j + 1, j + 2, …, пов'язаних з ним переходами. У j-й стан вона перейде через τ_{ij}; в (j + 1)-й стан вона перейде через τ_{ij+1}; в (j +2)-й стан вона перейде через τ_{ij+2} і т. д.

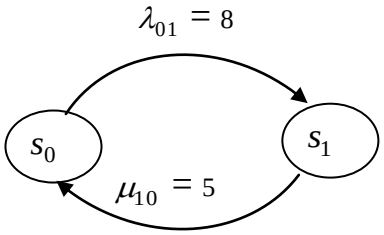


Рис. 3. Граф станів

Зрозуміло, що система може перейти з i -го стану тільки в один із цих станів, причому в той, перехід в який настане раніше.

Тому з послідовності часів: τ_{ij}, τ_{ij+1}, τ_{ij+2} і т. д. треба вибрати мінімальне і визначити індекс j, що вказує, в який стан відбудеться перехід.

Розглянемо приклад. Нехай надходять заявки на виявлення вразливостей. Позначимо стани (рис. 3): s_0 – немає заявки, s_1 – надійшла заявка. Задамо інтенсивність потоків:

$\lambda_{01} = 8$ заявок на хвилину; $\mu_{10} = 5$ оброблених заявок на хвилину.

Вважатимемо, що система в початковий момент перебувала в стані s_0 (немає заявки).

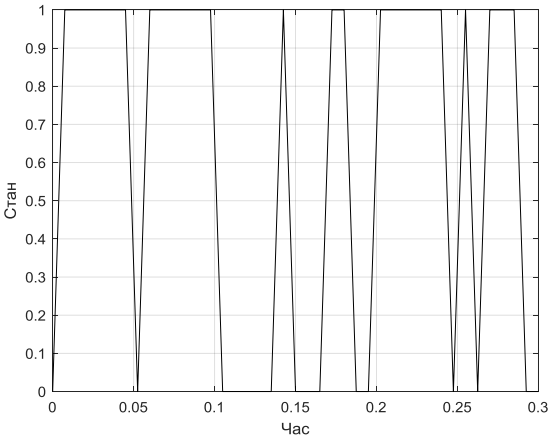


Рис. 4. Часова діаграма надходження заявок на виявлення вразливостей

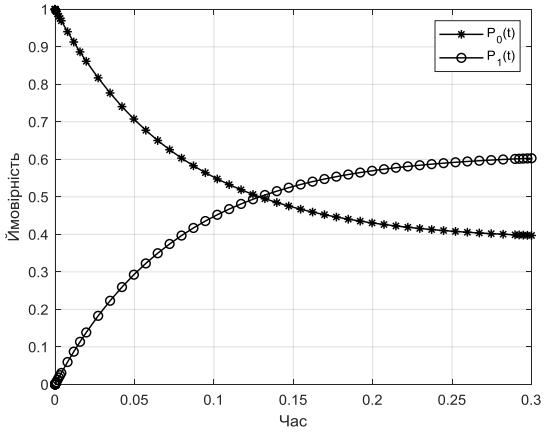


Рис. 5. Зміна ймовірностей станів: s_0 – немає заявки, s_1 – надійшла заявка

За допомогою імітаційного моделювання в середовищі Matlab отримано часову діаграму надходження заявок на виявлення вразливостей (рис. 4). Таким чином, знаючи інтенсивність потоків, можна в реальному масштабі часу моделювати процеси надходження заявок на виявлення вразливостей. На рис. 5 показано зміну ймовірностей станів: $P_0(t)$ – це ймовірність, що система знаходиться у стані s_0 (немає заявки), $P_1(t)$ – це ймовірність, що система знаходиться у стані s_1 (надійшла заявка). Як видно з наведених графіків, ймовірність стану s_0 спочатку дорівнює одиниці, потім різко зменшується та досягає 0,4 в сталому стані. Ймовірність стану s_1 навпаки спочатку дорівнює нулю, потім з плином часу збільшується та досягає значення 0,6 в сталому стані.

Висновок

Інформаційна безпека є однією із складових гарантоспроможності 5G. Основну загрозу безпеці таких систем становлять вразливості насамперед програмних компонентів. Пошук вразливостей у програмних компонентах є актуальним та ресурсомістким завданням, яким останнім часом займаються великі компанії та дослідницькі центри. Аналіз процесів виявлення та усунення вразливостей показує, що вони можуть бути описані системою масового обслуговування з необмеженою довжиною черги. Розроблено модель виявлення та усунення вразливостей у мережах зв'язку 5G на основі апарату марківських процесів. За допомогою даної моделі, знаючи інтенсивності потоків, можна в реальному масштабі часу моделювати процеси надходження заявок на виявлення вразливостей.

Список літератури:

1. Nick McKeown. Openflow: enabling innovation in campus networks/ Nick McKeown, Tom Anderson, Hari Balakrishnan, Guru Parulkar, Larry Peterson, Jennifer Rexford, Scott Shenker, Jonathan Turner // ACM SIGCOMM Computer Communication Review, 38[2]. 2008. P. 69–74.

2. OpenFlow Switch Specification Ver 1.5.1, 2016 [accessed January 11, 2016]. https://www.opennetworking.org/images/stories/downloads/sdnresources/ onf-specifications/openflow/openflow-switch-v1.5.1.pdf.

3. Партика Т.Л., Попов І.І. Інформаційна безпека : навч. посіб. для студентів закладів середньой професійної освіти. Москва : ФОРУМ: ІНФРА-М, 2002. 368с.

4. Лукацький А. Інформаційна безпека 2015 // Іт-безпека. Стандарти. Засоби захисту. Заходи. 2013. № 12. С.64–69.

5. Ложковський А.Г. Теорія масового обслуговування в телекомунікаціях : підручник. Одеса : ОНАС ім. А. С. Попова, 2012. 112 с. ISBN 978-966-7595-43-3.

6. Ложковський А.Г. Моделювання багатоканальної системи обслуговування з організацією черги / А.Г. Ложковський, Н.С. Салманов, О.В.Вербанов // Східно-європейський журнал передових технологій. 2007. №3/6(27). С.72–76.

7. Muliar B., Koliadenko Y., Moskalets M., Loshakov V. and Ageyev D. Interaction Model and Phase States at Frequency Resource Allocation in a Grouping of Radio-Electronic Equipment of 5G Mobile Communication Network // 2022 IEEE 9th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T), Kharkiv, Ukraine, 2022, pp. 495–501, doi: 10.1109/PICST57299.2022.10238581.

8. Koliadenko Y., Moskalets M., Badieiev V., Savchenko R. (2023). Method Radio Resource Allocation in Cognitive Radio Network // Dovgyi, S., Trofymchuk, O., Ustimenko, V., Globa, L. (eds) Information and Communication Technologies and Sustainable Development. ICT&SD 2022. Lecture Notes in Networks and Systems, vol 809. Springer, Cham. Pp. 102-115 https://doi.org/10.1007/978-3-031-46880-3_7

Надійшла до редколегії 03.02.2024

Відомості про авторів:

Коляденко Юлія Юріївна – д-р техн. наук, професор, Харківський національний університет радіоелектроніки, професор кафедри інфокомунікаційної інженерії ім. В.В. Поповського; Україна; e-mail: yuliia.koliadenko@nure.ua; ORCID: https://orcid.org/0000-0002-0247-2736

Бадеєв Валерій Олександрович – Харківський національний університет радіоелектроніки, аспірант кафедри інфокомунікаційної інженерії ім. В.В. Поповського; Україна; e-mail: valerii.badieiev@nure.ua; ORCID: https://orcid.org/0009-0005-4982-1840

УДК 621.38 **DOI:10.30837/rt.2024.1.216.09**

В.С. ЛАЗЕБНИЙ, канд. техн. наук, О.О. ОМЕЛЬЯНЕЦЬ

ОСОБЛИВОСТІ ПЕРЕДАВАННЯ ГОЛОСОВОГО ТРАФІКА ЗАСОБАМИ БЕЗПРОВОДОВИХ МЕРЕЖ IEEE 802.11AC

Вступ

Останнім часом значного поширення набула технологія передавання голосового трафіка через IP мережі (VoIP) [1]. Здебільшого використовують IP телефони, з'єднані з IP мережею за технологією Ethernet. Проте, все частіше використовують і безпроводове з'єднання засобами мережі Wi-Fi (стандарт IEEE 802.11) [2]. Пересторогі щодо більш широкого використання Wi-Fi виникають у користувачів через нестабільність показників якості (QoS) безпроводових мереж. Технології безпроводових мереж постійно зазнають удосконалення, з метою поліпшити їх якісні показники і розширити сферу їх застосування [3]. Найбільш розповсюдженими натепер є безпроводові мережі стандарту IEEE 802.11 специфікацій IEEE 802.11n та IEEE 802.11ac. Специфікацію IEEE 802.11n призначено для використання як у частотному діапазоні 2,4 ГГц, так і в діапазоні 5 ГГц, а специфікацію IEEE 802.11ac, яку можна вважати удосконаленою версією специфікації IEEE 802.11n, – призначеною для використання тільки в діапазоні 5 ГГц. У 2005 році прийнято специфікацію IEEE 802.11e, яку розроблено для підвищення якості надання телекомунікаційних послуг Wi-Fi мережами шляхом пріоритизації мережного трафіка [4]. В деяких специфікаціях, що стосуються безпосередньо канального і фізичного рівнів, IEEE 802.11e передбачено використовувати опційно, а в специфікації IEEE 802.11ac передбачено використовувати її обов'язково [5]. Проте, не можна сказати, що процес пошуку найкращих режимів застосування механізмів якості обслуговування IEEE 802.11e вже завершено [6], тому дослідження в цьому напрямі є актуальними.

Для організації послуги IP-телефонії треба забезпечити невелику затримку передавання голосових кадрів і невелику нерівномірність цієї затримки. В мережах IEEE 802.11 внаслідок спільного використання середовища передавання і конкурентного доступу до каналу за наявності великої кількості активних користувачів можуть виникати колізії, що призводить до зменшення пропускної здатності і погіршення інших показників якості.

Відомі компанії-виробники мережного обладнання приділяють велику увагу удосконаленню технології VoIP. Так, компанія Cisco в постійно оновлюваних рекомендаціях щодо організації мереж з послугою VoIP [7] зазначає, що під час планування таких мереж треба надавати перевагу мережним технологіям, що призначені для використання в діапазоні 5 ГГц. Для забезпечення високої якості надання послуги VoIP треба забезпечити умови, за яких наскрізна затримка передавання голосового кадру не буде перевищувати 150 мс, а нерівномірність затримки (джитер) буде в межах 100 мс. Також зазначено, що треба забезпечити відношення сигнал-шум в точці приймання не менше 25 дБ, а навантаження мережі має не перевищувати 50%.

У роботі [8] наведено рекомендації, що ґрунтуються на наявному досвіді і теоретичних дослідженнях. Серед цих рекомендацій можна відзначити таке: для кадрів VoIP треба використовувати пріоритизацію з гарантованим доступом до каналу, а також застосовувати протокол реального часу (RTP).

У роботі [9] крім згаданих вище засобів підвищення якості обслуговування рекомендовано здійснювати керування пропускною здатністю каналу і уникати надмірного навантаження.

Наведені вище рекомендації сприяють поліпшенню якості послуги IP-телефонії, але не надають кількісної оцінки впливу окремих чинників. Наприклад, говорити про ефективну пропускну здатність безпроводової мережі неможливо без прив'язки до розмірів кадрів даних. Потребує уточнення питання стосовно розподілу пропускної здатності мережі між

трафіком з різними пріоритетами, а також питання щодо кількості активних станцій, які можуть одночасно функціонувати в зоні обслуговування точки доступу.

Метою дослідження є з'ясувати особливості передавання голосового трафіка для організації послуги IP-телефонії в офісних приміщеннях засобами мережі IEEE 802.11ac, щоб забезпечити якісне надання зазначеної послуги для достатньо великої кількості користувачів, навіть за умови інтенсивного передавання змішаного трафіка.

Кодеки і особливості їх застосування

Перш ніж перейти до розгляду процесів у безпроводовій мережі IEEE 802.11ac, необхідно з'ясувати параметри й характеристики голосового трафіка, який треба передавати мережею. У цифрових системах для передавання голосового трафіка застосовують стиснення сигнального потоку з метою зменшити його інтенсивність для передавання цифровими мережами. Голосовий потік після стиснення подають кадрами однакової величини і однакової тривалості. Існує велика кількість голосових кодеків, що використовують у системах цифрового голосового зв'язку [10]. У табл. 1 за матеріалами [11] наведено параметри кількох кодеків, що мають застосування в IP-телефонії.

Кодек G.711 – один із перших голосових кодексів, що був призначений для застосування в каналах ISDN. Його часто використовують і в Інтернет-телефонії (VoIP).

Таблиця 1

Параметри кодеків голосових сигналів

Параметри	**G.711**	**G.729**	**G.722**	**iLBC**
Тип	вузькосмуговий	вузькосмуговий	широкосмуговий	вузькосмуговий
Звукові частоти, Гц	300-3400	300-3400	50-7000	300-3400
Частота дискретизації, Гц	8000	8000	16000	8000
Розрядність	8	16	14	16
Потік, кбіт/с	64	8	48, 56, 64	13,33 – 15,2
Навантаження	160 байтів/20мс 240 байтів/30мс	20 байтів/20мс	160 байтів/20мс	38 байтів/20мс 50 байтів/30мс
Метрика MOS	4,1	3,9	4,3 (64 кбіт/с)	4,1 (15,2 кбіт/с)

G.729 – це кодек із малою інтенсивністю сигнального потоку і малим обсягом блоків даних корисного навантаження. Зниження якості відтвореного голосу є незначним, у порівнянні з кодеком G.711. У кодеку використано алгоритм стиснення з втратами. Цей кодек використовують у мережах з обмеженою пропускною здатністю, таких як WAN. Як і G.711, це один із найпоширеніших кодеків у сфері VoIP.

Кодек G.722 є широкосмуговим і забезпечує більш природне звучання голосу, в порівнянні з G.711 і G.729.

iLBC (Internet Low Bitrate Codec) – Інтернет-кодек з малою інтенсивністю сигнального потоку, що забезпечує чудову якість передавання голосу. В ньому передбачено деяку компенсацію втрачених голосових кадрів, що може статися внаслідок втрати або затримки IP-пакетів. Необхідне навантаження на процесор подібне до G.729. Кодек призначено для використання в Інтернеті в рамках протоколу WebRTC (real-time communications) для організації голосового і відеозв'язку.

Розрахунок часу передавання за різних режимів модуляції і кодування

Для дослідження особливостей передавання голосового трафіка в мережах IEEE 802.11ac скористаємось параметрами кодеку G.711 як одного із поширених кодеків для IP-телефонії і такого, що формує кадри даних з великим навантаженням (табл. 1).

Визначимо час передавання одного кадру голосового трафіка, сформованого кодеком G.711. Розглянемо час передавання в каналі IEEE 802.11ac з частотною смугою 20 МГц у режимі з одним просторовим потоком, в разі застосування різних схем модуляції і кодування (MSC). Розглянемо два режими функціонування кодеку G.711: з тривалістю вибірки

20 мс і з тривалістю вибірки 30 мс. Для розрахунку часу передавання голосового кадру скористаємось розподілом часових інтервалів, наведених на рис. 1.

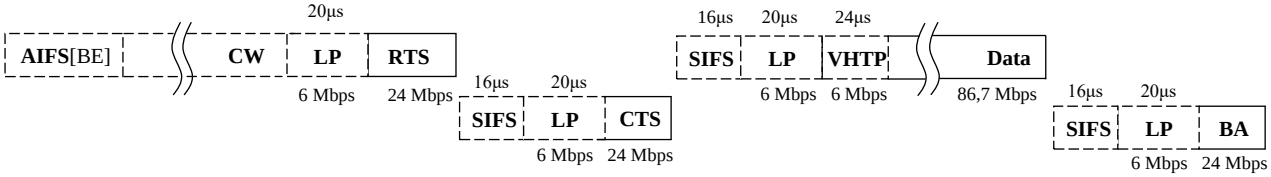


Рис. 1. Розподіл часових інтервалів під час доступу до безпроводового каналу 802.11ac [12]

Тривалість інтервалу передавання голосового кадру $E[T_{PL1}]$ визначимо за очевидним співвідношенням, що випливає безпосередньо з розподілу часових інтервалів, рис. 1:

$$E[T_{PL1}] = AIFS[BE] + CW + T_{RST} + SIFS + T_{CST} + SIFS + T_{MPDU} + SIFS + T_{ACK}, \quad (1)$$

де $AIFS[BE]$ – міжкадровий арбітражний інтервал, CW – тривалість затримки, обумовленої лічильником зворотного відліку, T_{RTS} – кадр запиту на передавання, $SIFS$ – короткий міжкадровий інтервал, T_{CTS} – кадр підтвердження готовності прийняти кадр, T_{MPDU} – тривалість кадру даних, яким передають блок голосової інформації разом зі службовою інформацією протоколів верхніх рівнів моделі OSI, рис. 2 [13], T_{ACK} – кадр підтвердження прийнятого кадру даних.

IP 20 байтів	UDP 8 байтів	RTP 12 байтів	Голосові дані *n* байтів	FCS 4 байти

Рис. 2. Структура даних в кадрі корисного навантаження (Data)

Для аналізу особливостей передавання голосового трафіка розглянемо кілька режимів доступу до середовища передавання. Розглянемо режим передавання голосового трафіка в мережі DCF без пріоритизації і режим передавання голосового трафіка з пріоритизацією в мережі EDCF. Ці режими вибрано для досліджень, оскільки різні виробники мережного обладнання пропонують по-різному реалізовувати послугу передавання голосового трафіка [14].

Для кращої надійності приймання службової інформації і кращої електромагнітної сумісності близько розташованих мереж стандарту IEEE802.11 преамбули кадрів на канальному рівні передають з малою кратністю модуляції і з найменшою швидкістю завадозахисного коду (R=1/2). В результаті швидкість передавання преамбул становить 6 МГц/с. Визначимо тривалості часових інтервалів, наведених на рис. 1. В інтерфейсі безпроводового каналу IEEE 802.11ac застосовано систему багаточастотної модуляції й кодування OFDM. Дані передають символами OFDM, які складаються з угрупування ортогональних частот. Угрупування, яке передбачено застосовувати в каналі з частотною смугою 20 МГц, містить 56 частот, 52 із яких передбачено для передавання даних, а 4 – для передавання пілот-сигналів. Тривалість символу OFDM згідно зі специфікацією 802.11ac може бути 4 мкс (захисний інтервал 0,8 мкс) або 3,6 мкс (захисний інтервал 0,4 мкс). Тривалість символу 4 мкс використовують завжди для передавання кадрів службової інформації, частини преамбули кадрів даних і для передавання кадрів даних в мережах з абонентськими станціями різних поколінь. Тривалість символу 3,6 мкс використовують для передавання частини преамбули дуже швидкісного режиму (VHT) і даних в однорідних мережах, що підтримують режим VHT [4]. Надалі будемо вважати, що для передавання голосового трафіка використовуємо символи OFDM тривалістю 4 мкс. Важливі системні параметри режимів DCF і EDCF наведено в табл. 2 [15].

Таблиця 2

Системні параметри для різних класів корисного навантаження

Параметри EDCA за початковим налаштуванням для кожного класу доступу			
Клас доступу	**CWmin**	**CWmax**	**AIFSN**
Фоновий (AC_BK)	15	1023	7
Краща спроба (AC_BE)	15	1023	3
Відео (AC_VI)	7	15	2
Голос (AC_VO)	3	7	2
Успадкований DCF	15	1023	2
**AIFSN – число (N) для визначення тривалості арбітражного інтервалу (AIFS).*			

Тривалості міжкадрових інтервалів, протягом яких станції мережі не здійснюють дій для доступу до каналу, мають такі значення: SIFS = 16 мкс (короткий міжкадровий інтервал), DIFS = 34 мкс, AIFS[AC_BE] = SIFS+3·ST = 16+3·9 = 43 мкс, AIFS[AC_VO] = =SIFS+2·ST = 16+2·9 = 34 мкс, AIFS[AC_BK] = SIFS+7·ST = 16+7·9 = 79 мкс [16].

У мережі DCF та у мережі EDCF для класів доступу BE і BK значення конкурентного вікна однакові та знаходяться в межах від $CW_{\min} = 15$ до $CW_{\max} = 1023$. Кожна станція перед початком доступу до мережі завантажує в свій лічильник зворотного відліку число із множини $\{0, 1, 2, \ldots, CW_{\min}\}$. Вибір числа відбувається випадковим чином і вибір будь-якого числа є однаково ймовірним. Якщо середовище передавання вільне станція здійснює декремент лічильника зворотного відліку через інтервали часу, що мають назву часові слоти, $ST = 9$ мкс. Коли значення лічильника зворотного відліку досягає значення «нуль», станція здійснює передавання кадру. У разі виникнення колізії, станція збільшує множину чисел, із яких буде вибране число для завантаження лічильника зворотного відліку, за формулою $CW := 2(CW + 1) - 1$ [5]. Якщо одна активна станція мережі буде тривалий час передавати голосовий трафік у мережі DCF, тоді в середньому затримка зворотного відліку становитиме $CW = CW_{\min}/2 = 7{,}5$ (часових слотів).

Тривалість кадру RTS визначимо для швидкості передавання 24 Мбіт/с (найбільша передбачена у стандарті IEEE 802.11 швидкість для кадрів RTS і CTS). Стандартом передбачено передавати кадри RTS і CTS з високою надійністю. Можливі швидкості передавання блоку даних цих кадрів становлять 6, 12 і 24 Мбіт/с. Преамбулу цих кадрів завжди передають зі швидкістю 6 Мбіт/с, і тривалість преамбули становить 20 мкс, рис. 1. Блок даних RTS становить 20 байтів. Швидкість 24 Мбіт/с є успадкованою від 802.11a. В режимі передавання з такою швидкістю застосовують модуляцію носійних частот 16-QAM і згорткове кодування зі швидкістю R=1/2. Кількість бітів блоку даних кадру RTS з урахуванням завадозахисного кодування становитиме 20·8·2 = 320. Один символ OFDM містить 52 носійні частоти, кожна з яких передає 4 біти даних. Одним символом можна передати 208 бітів. Для передавання блоку даних кадру RTS треба 320:208=1,54 → 2 символи. Таким чином, загальна тривалість кадру RTS становить 20 мкс+4 мкс·2 = 28 мкс.

Аналогічно визначимо тривалість інтервалу передавання кадру CTS. Обсяг даних цього кадру становить 14 байтів або 112 бітів. З урахуванням завадозахисного кодування, блок даних для передавання становитиме 224 біти. Кількість символів становить 224:208 = 1,077 → 2 символи. Тобто тривалість кадру CTS становить також 28 мкс.

Визначимо тепер тривалість інтервалу передавання блоку даних, сформованого кодеком G.711, рис. 2.

Інтенсивність потоку на виході кодека становить 64 кбіт/с, табл. 1. Інформаційними IP-мережами передають інформаційні пакети цього кодека двох типів: пакети з вибіркою 20 мс голосового сигналу і пакети з вибіркою 30 мс. Кодек G.711 формує сигнал за методом ІКМ (імпульсно-кодової модуляції) з частотою вибірки 8 кГц, розрядністю оцифрованої вибірки 8 біт/відлік і можливістю компандирування сигналу. Під час оброблення звукового

сигналу тривалістю 20 мс кодек сформує блок даних, що містить 160 вибірок. Окрім безпосередньо голосових даних блок даних містить 20 байтів заголовку IP, 8 байтів заголовку UDP і 12 байтів заголовку RTP, тобто разом іще 40 байтів даних, рис. 2. Сумарно блок даних має обсяг 160+40 = 200 байтів, що дорівнює 1600 бітів.

Відстань, на якій можна здійснювати передавання даних між абонентською станцією і точкою доступу залежить від потужності передавача і схеми модуляції і кодування радіочастотних сигналів. Найбільшу швидкість передавання в режимі MCS8 можна реалізувати на найменшій відстані від точки доступу. Користувачі можуть знаходитись на значній відстані від точки доступу, і тому режим передавання даних буде повільнішим ніж у разі застосування MCS8. Крім відстані на режим передавання впливають різні перешкоди, що знаходяться на шляху розповсюдження електромагнітних хвиль [17]. В офісних приміщеннях це можуть бути перегородки із різноманітних матеріалів, стелажі, інші співробітники тощо. Для оцінювання того, наскільки зміняться умови передавання голосового трафіка в разі використання меншої швидкості для передавання даних, визначимо час передавання голосового кадру в разі застосування різних схем модуляції і кодування (MCS3 – MCS8). Для прикладу наводимо розрахунок для режиму MCS8 – найбільш швидкісного режиму для каналу 20 МГц мережі 802.11 ac з одним просторовим потоком.

У режимі з MCS8 застосовують модуляцію 256-QAM і швидкість завадозахисного коду R=3/4. Після завадозахисного кодування обсяг даних зросте до 1600·4:3 = 2134 бітів. Одним OFDM символом можна передати 8 бітів·52 = 416 бітів. Для передавання всього блоку даних знадобиться 2134:416 = 5,13 → 6 символів або 24 мс. Час передавання кадру даних з урахуванням преамбули (44 мкс) становитиме 44+24 = 68 (мкс).

Згідно з (1), загальна тривалість циклу доступу до каналу для передавання блоку голосової інформації тривалістю 20 мс в мережі DCF складе:

$$E[T_{PL1}] = 34 + 7{,}5\cdot 9 + 28 + 16 + 28 + 16 + 68 + 16 + 32 = 305{,}5 \text{ мкс}.$$

Результати розрахунків тривалості циклу доступу до каналу для передавання одного голосового кадру, в разі застосування різних режимів, наведено на рис. 3.

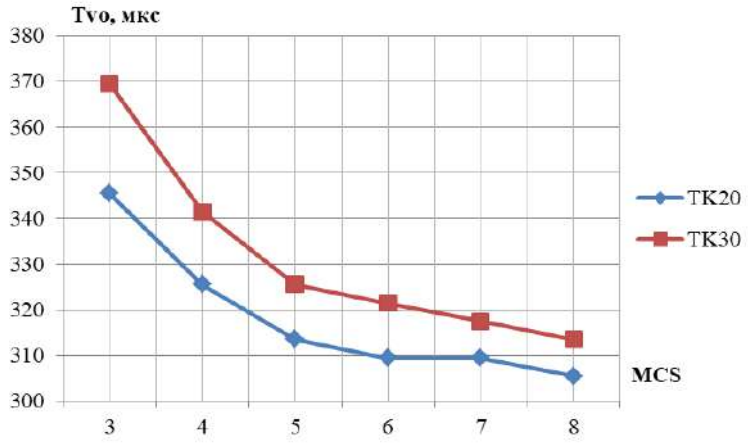


Рис. 3. Залежність тривалості T_{VO} передавання голосового кадру від режиму модуляції і кодування MCS

На рис. 3 наведено також результати розрахунків часу передавання голосових кадрів з вибіркою 30 мс.

Якщо тільки одна станція в мережі передає голосовий трафік без агрегування, то вона рівномірно передаватиме 50 кадрів за секунду, в разі опрацювання звукових фрагментів тривалістю 20 мс і 33,3(3) кадри – в разі опрацювання фрагментів тривалістю 30 мс.

Якщо порівняти час формування звукового кадру і тривалість інтервалу доступу до каналу для його передавання, то очевидно, що час передавання складає незначну частку від часу формування звукового кадру. Так, в разі передавання кадру з вибіркою 20 мс, час передавання становить 1,72 ÷ 1,53 %, а для кадру з вибіркою 30 мс – 1,23 ÷ 1,04 %.

Із отриманих результатів (рис. 3) випливає, що час передавання кадру даних, що містить голосову інформацію мало залежить від режиму модуляції й кодування. Тобто, умови передавання голосового трафіка для станцій, що знаходяться на різній відстані від точки доступу, будуть майже однаковими.

Можна визначити теоретичну межу кількості активних станцій, які могли б функціонувати в зоні обслуговування однієї точки доступу. За ідеального узгодження активних станцій в часі у мережі 802.11ac з каналом 20 МГц одночасно могли б функціонувати без взаємних завад 57 станцій, в яких кодеки працюють з вибірками 20 мс або 86 станцій, що формують звукові кадри з вибірками по 30 мс.

Передавання голосового трафіка в мережах зі змішаним навантаженням

За реальних умов голосовий трафік передають в мережах, в яких за доступ до середовища передавання конкурують різні станції, які можуть передавати як голосові кадри, так і кадри, що передають іншу інформацію.

Розглянемо особливості функціонування мережі, в якій є кілька станцій з насиченим навантаженням (буфер даних постійно заповнений), що передають дані з низьким пріоритетом, і кілька станцій, що передають голосову інформацію.

Розглянемо режим, коли в мережі є M станцій, що передають голосові дані, і N станцій з насиченим навантаженням. Режим насиченого навантаження використовуємо для визначення граничних можливостей мережі [18].

Проаналізуємо сценарій, за якого насичене навантаження віднесено до класу AC_BK (низький пріоритет), а голосові дані мають пріоритет AC_VO, табл. 1. Розподіл часових інтервалів в безпроводовому каналі буде таким, як наведено на рис. 4.

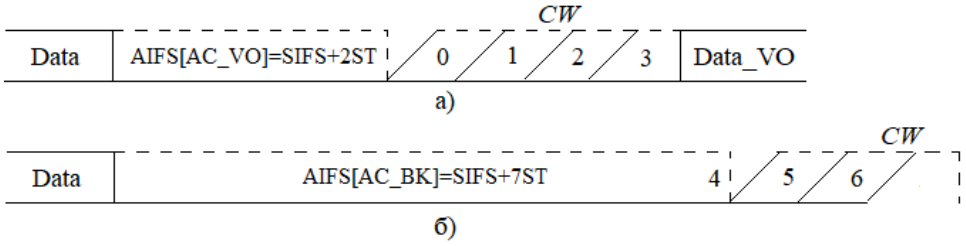


Рис. 4. Розподіл часових інтервалів у мережі з гібридним пріоритизованим навантаженням

Після звільнення радіочастотного каналу (завершення інтервалу Data) станції VO витримають паузу, обумовлену арбітражним міжкадровим інтервалом SIFS+2ST, а станції BK – SIFS+7ST. Тобто, станції VO мають інтервал тривалістю п’ять часових слотів (ST), щоб передати свої кадри без конкуренції з кадрами BK. П’ятий інтервал може бути використаний, в разі виникнення колізії між станціями VO.

Також треба взяти до уваги, що в лічильник зворотного відліку станція VO завантажить число із множини {0, 1, 2, 3}. Тобто, передавання VO кадру почнеться ще до того, як закінчиться арбітражний інтервал для BK станції.

Особливістю передавання голосового трафіка є те, що він не створює насиченого навантаження. Станція передає стислу звукову інформацію з періодичністю 20 мс, якщо не застосовано механізм агрегування кадрів, а в разі агрегування – через більші проміжки часу, кратні 20 мс.

Тепер треба оцінити, скільки буде міжкадрових інтервалів, протягом яких станції VO мають можливість передавати кадри без конкуренції BK. Зробимо розрахунок для випадку, коли кадри BK мають навантаження 1500 байтів, що характерно для великих кадрів даних, які надходять через мережу Ethernet. Саме такі кадри характерні для локальних мереж як «великі кадри» [12]. Розглядаємо великі кадри, оскільки вони потребують для передавання більше часу і створюють гірші умови для передавання голосового трафіка.

Якщо кадри даних з пріоритетом BK міститимуть по 1500 байтів корисної інформації, то за умови передавання даних у режимі MCS3 (16-QAM, R=3/4) і з урахуванням тривалості

арбітражного інтервалу (79 мкс), тривалість циклу доступу до каналу для передавання цих кадрів становитиме 606,5 мкс. У режимі MCS5 тривалість циклу становитиме 530,5 мкс, а в режимі MCS8 – 410,5 мкс.

Протягом 20 мкс у разі передавання низькопріоритетного насиченого трафіка виникне щонайменше 32 арбітражних інтервали (у разі застосування MCS3), в кожному з яких кадри з голосовими даними можуть конкурувати тільки між собою.

Розглянемо, як буде передано голосові кадри, якщо в мережі M станцій, що передають голосовий трафік.

Всі M станцій є незалежними, і кожна намагається отримати доступ до мережі під час випадково обраного арбітражного інтервалу після відліку випадкового числа лічильником.

Якщо врахувати 32 арбітражні інтервали, наявні протягом 20 мкс, і в кожному інтервалі по 4 часові слоти, які випадковим чином може обрати станція, то для початку циклу передавання M голосових кадрів є 128 можливих реалізацій. Позначимо літерою K загальну кількість можливих реалізацій, коли станції VO можуть розпочати передавання. Це моменти часу, під час яких конкурувати за доступ до каналу будуть тільки станції VO.

Оцінимо ймовірність виникнення колізій між M станціями VO, що конкурують за доступ до каналу протягом 20 мкс. Подібне завдання було вирішене в [19] і запропоновано співвідношення для визначення ймовірності виникнення колізії. З урахуванням зроблених вище позначень, це співвідношення набуде вигляду

$$P_c = \frac{\tilde{A}_K^M - A_K^M}{\tilde{A}_K^M} = 1 - \frac{K!}{(K-M)!K^M}, \qquad (2)$$

де $\tilde{A}_K^M = K^M$ – кількості розміщень із K по M з повторами, $A_K^M = \frac{K!}{(K-M)!}$ – кількості розміщень із K по M без повторів.

Результати розрахунку ймовірності виникнення колізій наведено на рис. 5. Розраховано ймовірність колізій для трьох режимів передавання низькопріоритетного трафіка: для режиму MCS3 (K=32), для режиму MCS5 (K=37), для режиму MCS8 (K=48).

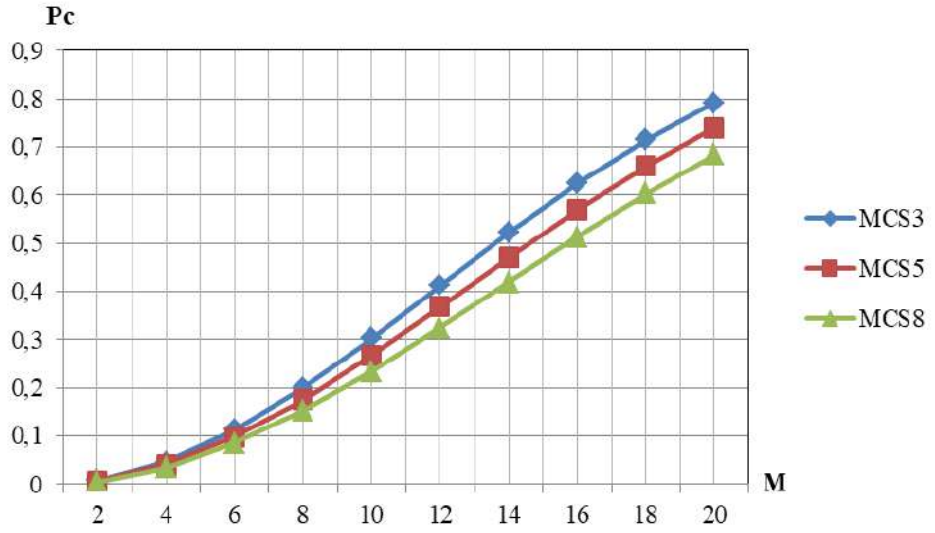


Рис. 5. Ймовірність виникнення колізій в мережі IEEE 802.11ac з M станціями AC_VO і насиченим трафіком AC_BK

Обговорення результатів

Безпосередньо із графіка, наведеного на рис. 5, випливає, що за наявності в мережі IEEE 802.11ac станцій, що передають низькопріоритетний трафік класу AC_BK, навіть за умови насиченого навантаження можливе одночасне функціонування великої кількості станцій, що

передають голосовий трафік. Так, за наявності в мережі одночасно активних 10-и станцій з голосовим трафіком, ймовірність виникнення колізій для таких станцій становить не більше 0,3. Це означає, що колізія між станціями AC_VO буде виникати в середньому один раз на три цикли по 20 мкс. У разі наявності 15-и активних станцій AC_VO, ймовірність колізії становить приблизно 0,5, і колізія буде в середньому виникати один раз на два цикли по 20 мкс. Станції, що потрапили в колізію, швидко її подолають із застосуванням стандартного механізму, оскільки всі інші станції успішно передадуть свої голосові кадри і не будуть створювати конкуренції.

У разі зменшення часу передавання кадрів низькопріоритетного трафіка, ймовірність виникнення колізій для станцій AC_VO зменшується, внаслідок збільшення кількості арбітражних інтервалів і збільшення кількості інтервалів, коли голосові кадри передають без конкуренції з низькопріоритетним трафіком. У нашому дослідженні розглянуто сценарій, за якого для низькопріоритетного трафіка використано великі кадри даних (1500 байтів), але в реальних офісних мережах трафік складається із кадрів даних різного розміру [12], що сприяє поліпшенню умов для передавання трафіка класу AC_VO. Також можна відзначити, що виникнення колізій між станціями з низькопріоритетним трафіком практично не призводить до збільшення затримки передавання і нерівномірності затримки голосових кадрів, оскільки колізії відбуваються в інтервалах передавання кадрів RTS і CTS. Тобто, станції з кадрами AC_VO отримають доступ до середовища передавання одразу після колізійного інтервалу.

Затримка передавання голосового кадру в розглянутій мережі IEEE 802.11ac становить приблизно 20 мкс, а нерівномірність не перевищує кількох мілісекунд, що обумовлено технологією доступу до каналу (зворотний відлік часових слотів) і часом подолання колізії, в разі її виникнення (можливе виникнення паузи під час передавання кадру низькопріоритетного трафіка).

Окремо треба зауважити, що для зони обслуговування однієї точки доступу мережі IEEE 802.11ac наявність одночасно активних 15-20 станцій, що передають голосовий трафік, є доволі малоймовірною, оскільки ці мережі призначено для використання в приміщеннях, і радіус зони обслуговування є відносно невеликим (до кількох десятків метрів [12]). Тому, застосування безпроводової мережі IEEE 802.11ac для організації IP-телефонії в офісних і подібних приміщеннях може бути ефективним технічним рішенням. Для обслуговування великих приміщень і забезпечення мобільності співробітників треба застосовувати безшовний роумінг між зонами обслуговування окремих точок доступу.

Висновки

У результаті дослідження особливостей передавання голосового трафіка для організації послуги IP-телефонії в офісних приміщеннях засобами мережі IEEE 802.11ac з'ясовано, що в разі застосування пріоритизації мережного трафіка можна забезпечити якісне надання зазначеної послуги для достатньо великої кількості користувачів, навіть за умови інтенсивного передавання змішаного трафіка.

Кодеки голосових сигналів забезпечують ефективне стиснення, що обумовлює малу тривалість циклу доступу до безпроводового каналу для передавання голосового кадру, навіть за умови великої частки непродуктивних витрат часу. За наявності в зоні обслуговування точки доступу 15 – 20 активних клієнтів, що передають голосовий трафік, затримка передавання трохи більша за тривалість інтервалу вибірки. Результати отримано, з урахуванням характеристик кодека G.711, що формує великий блок цифрових даних на виході, водночас їх можна розповсюдити на інші мережі, в яких застосовані інші голосові кодеки з такими ж або меншими блоками цифрових даних на виході.

Отримані результати можна розповсюдити і на безпроводові мережі, в яких голосові дані передають шляхом агрегування кількох голосових кадрів.

Наведені вище висновки стосуються мереж, в яких для надання послуг IP-телефонії здійснено пріоритизацію згідно зі специфікацією IEEE 802.11e з наданням голосовому трафіка пріоритету AC_VO, а іншим даним, які передають тією ж мережею – AC_BK. Для інших сценаріїв функціонування мереж IEEE 802.11ac доцільно зробити окремі дослідження.

Список літератури:

1. Cameron Johnson . What Is VoIP? The Newbie's Guide to Voice over IP. URL: https://www.nextiva.com/blog/what-is-voip.html
2. Josh Epstein. 5 Ways to Troubleshoot WiFi Issues with VoIP. URL: https://telzio.com/blog/5-ways-troubleshoot-wifi-voip
3. How to optimize your Wi-Fi network for VoIP. URL: https://info.teledynamics.com/blog/how-to-optimize-your-wi-fi-network-for-voip
4. 802.11 QoS Tutorial. URL: https://www.ieee802.org/1/files/public/docs2008/avb-gs-802-11-qos-tutorial-1108.pdf
5. Matthew S. Gast. 802.11ac: A Survival Guide. *O'Reilly Media*, 136 p., USA, 2015. URL: https://freecomputerbooks.com/802.11ac-A-Survival-Guide.html
6. Why and How To Implement Wi-Fi QoS? URL: https://community.fs.com/article/why-and-how-to-implement-wifi-qos.html
7. Wireless VoIP QoS Best Practices. (Last updated Aug 24, 2023). URL: https://documentation.meraki.com/Architectures_and_Best_Practices/Cisco_Meraki_Best_Practice_Design/Best_Practice_Design_-_MR_Wireless/Wireless_VoIP_QoS_Best_Practices
8. Joe Manna. What Is VoIP QoS & How Does It Improve Call Quality? November 2, 2023. URL: https://www.nextiva.com/blog/voip-qos.html
9. Howard. Why and How To Implement Wi-Fi QoS? December 21, 2023 – URL: https://community.fs.com/article/why-and-how-to-implement-wifi-qos.html
10. Voice Codecs. URL:https://www.gl.com/voice-codecs.html
11. The wonderful world of voice codecs. URL:https://info.teledynamics.com/blog/the-wonderful-world-of-voice-codecs
12. Chuck Lukaszewski, Liang Li. Very High-Density 802.11ac Networks Theory Guide // *Aruba Networks*, 62 p. URL: https://howwirelessworks.com/wp-content/uploads/Aruba_VHD_VRD_Theory_Guide.pdf.\
13. IP Protocol Header Fundamentals Explained with Diagrams. URL: https://www.thegeekstuff.com/2012/03/ip-protocol-header/
14. Daniel Andrews. VoIP vs. VoWiFi: Comparing Benefits & Highlighting Differences. URL: https://www.calilio.com/blogs/voip-vs-vowifi-comparison-differences
15. White Paper of Home Wi-Fi Networks with Optimal User Experience. URL: https://carrier.huawei.com/~/media/CNBG/Downloads/Technical%20Topics/Fixed%20Network/White%20Paper%20of%20Home%20Wi-Fi%20-en.pdf
16. Interframe Space (RIFS, SIFS, PIFS, DIFS, AIFS, EIFS). URL: https://wifisharks.com/2020/11/14/interframe-space/
17. Wi-Fi Signal Attenuation. URL: https://blog.wavlink.com/en-us/article/TechnicalNews/92442c2444eaa02541dd27fe90bed782.html
18. Lazebnyi V.S., Yin Ch., Omelyanets O.O. Doslidzhennya realnoyi propusknoyi zdatnosti bezdrotovoyi informatsiynoyi merezhi spetsyfikatsiyi 802. [Study of the real bandwidth of the wireless information network of the 802.11n specification.] // Scientific notes of the Tavria National University named after V. I. Vernadsky Series: Technical Sciences. 2018. № 5. Part 1.Vol. 29 (68). P. 155–160.
19. Lazebnyi V.S., Yin Ch. Estimation of probabilistic processes in wireless networks of 802.11 standard // *Microsystems, electronics and acoustics*. 2017. № 5. P. 47–53. URL: https://www.researchgate.net/publication/322016385_Estimation_of_probabilistic_processes_in_wireless_networks_of_80211_standard

Надійшла до редколегії 12.02.2024

Відомості про авторів:

Лазебний Володимир Семенович – канд. техн. наук, доцент, Національний технічний університет України "Київський політехнічний інститут ім. Ігоря Сікорського", канд. техн. наук, доцент кафедри акустичних та мультимедійних електронних систем; Україна; e-mail: lvs50469-ames@lll.kpi.ua; ORCID: 0000-0002-5702-2775

Омельянець Олександра Олександрівна – Національний технічний університет України "Київський політехнічний інститут ім. Ігоря Сікорського", асистент кафедри акустичних та мультимедійних електронних систем; Україна; e-mail: omelyanets2011@gmail.com; ORCID: 0009-0006-6549-201X

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

УДК 621.3.082.62 **DOI:10.30837/rt.2024.1.216.10**

О.В. МЯГКИЙ, канд. техн. наук, Р.П. ОРЕЛ, канд. техн. наук,
С.Н. МЕШКОВ, канд. техн. наук, В.О. СТОРОЖЕНКО, д-р техн. наук

ШЛЯХИ ПІДВИЩЕННЯ ЕРС НАПІВПРОВІДНИКОВИХ ЕЛЕМЕНТІВ НА ОСНОВІ ТЕРМОЕЛЕКТРИЧНИХ ЕФЕКТІВ

Вступ

Протягом наступних десятиліть очікується значне збільшення енергоспоживання, пов'язане з розвитком економіки та приростом населення. Це призведе до зростання тиску на систему енергопостачання та вимагатиме підвищеної уваги до ефективності використання енергії. Це проблеми сучасної енергетики, які треба вирішувати зараз. Доступність енергоресурсів є ключовим фактором для розвитку економіки та сприяє покращенню якості життя. Як правило, в основі прогнозів енергоспоживання лежать такі фактори, як зростання світових економік та збільшення чисельності населення, що виступають як основна рушійна сила безперервного зростання енергоспоживання.

Проблему зі зростаючим енергоспоживанням та скороченням енергетичних ресурсів передбачалося вирішувати за рахунок альтернативних джерел енергії та енергозбереження, адже виснаження родовищ нафти, вугілля та газу може призвести до глобальної енергетичної катастрофи. Адже традиційні джерела енергії обмежені. А вітер, Сонце, річки, океани і моря мають невичерпні запаси енергії. Найбільше стабільним і прогнозованим з цих джерел є Сонце, тому в енергетиці зростає зацікавленість до нових систем перетворення цього виду енергії. У якості подібних систем найбільш часто використовуються сонячні панелі. Це зумовлює дослідницьку увагу до їх вдосконалення.

Суттєвим недоліком сонячних панелей є відносно невелика ЄРС. Перспективним напрямком підвищення ЕРС таких пристроїв є напилення або конденсація на них напівпровідникових структур GeS [1, 2].

Генеруючі ЕРС-структури на основі GeSi

Принцип дії варізонного генеруючого елемента ґрунтується на явищі виникнення термоЕРС у неоднорідному напівпровіднику за умови розігріву структури.

Для нашої системи повинні виконуватися такі основні співвідношення для напруженості електричного поля $\vec{E}$ та електрорушійної сили (ЕРС) ε:

$$\vec{E} = -grad\,\varphi,$$

$$\varepsilon = IR,$$

де φ – потенціал електричного поля; I – сила струму; $R = \int \frac{dx}{\sigma}$ повний електричний опір; σ – електропровідність.

Для спрощення завдання вважаємо, що $\vec{E}$ і ε є одномірними функціями. Тоді густина результуючого струму, що викликаний нерівноважними носіями зарядів для k-го елемента можна записати [3, 4]:

$$j_k = -\sigma_k \left(\frac{d\tilde{\varphi}_k}{dx} + \alpha_k \frac{dT_k}{dx} \right), \quad (1)$$

де σ_k – електропровідність речовини k-го елемента; $\tilde{\varphi}_k$ – електрохімічний потенціал речовини k-го елемента; α_k – коефіцієнт термоЕРС; T_k – температура k-го елемента.

Електрохімічний потенціал речовини визначається за формулою

$$\tilde{\varphi}_k = \frac{F_k}{e_k} = \varphi + \frac{\mu_1}{\mu_2}$$

де F_k – квазірівень Ферми речовини k-го елемента; e_k – заряд носіїв k-го елемента; μ_1 і μ_2 – хімічні потенціали речовин першого та другого типу.

Тоді вираз (1) можна привести до вигляду:

$$\varepsilon = \oint \frac{\sigma_1}{\sigma} \frac{dy}{dx} \left(\tilde{\varphi}_2 - \tilde{\varphi}_1 \right) dx = \oint \frac{\sigma_2}{\sigma} \frac{dy}{dx} \left(\tilde{\varphi}_1 - \tilde{\varphi}_2 \right) dx . \qquad (2)$$

З урахуванням (1), (2) система, що розглядається, повинна задовольняти рівнянню

$$\varepsilon = -\oint \sum_{k=1}^{N} \frac{\sigma_k}{\sigma} \left(\frac{d}{dx} \tilde{\varphi}_k + \alpha_k \frac{d}{dx} T_k \right) dx , \qquad (3)$$

де $\sigma = \sum_{k=1}^{N} \sigma_k$ – загальна електропровідність контуру; N – кількість шарів SiGe, $N = 2$.

Видно, що температура T_k входить у рівняння (3) у двох доданках: безпосередньо у α_k (градієнт T) і опосередковано в $\tilde{\varphi}_k(T)$. У випадку $T_k = \text{const}$ складова $\alpha_k = 0$.

Розглянемо рівняння (1) з урахуванням виразу (3), яке описує термоЕРС. При $T_k = \text{const}$ та виконанні умови

$$\psi = \left(\frac{\mu_2}{e_2} - \frac{\mu_1}{e_1} \right) \neq const$$

отримується співвідношення для електропровідності:

$$\frac{\sigma_1}{\sigma_2} \neq const .$$

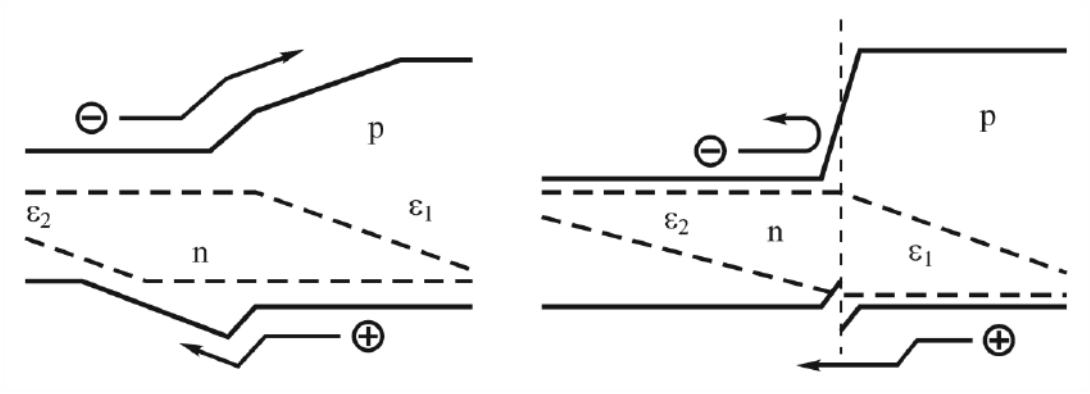
Після заміни змінних щодо $\tilde{\varphi}_k(T)$ отримаємо

$$\varepsilon = \oint \frac{\sigma_1}{\sigma} \frac{d}{dx} \left(\frac{\mu_2}{e_2} - \frac{\mu_1}{e_1} \right) dx = \oint \frac{\sigma_2}{\sigma} \frac{d}{dx} \left(\frac{\mu_1}{e_1} - \frac{\mu_2}{e_2} \right) dx . \qquad (4)$$

Очевидно, що вираз (4), що описує нерівноважність і неоднорідність напівпровідникового матеріалу, а також його біполярність ($N = 2$), є відомою умовою виникнення ЕРС у напівпровіднику і визначає збільшення перепаду концентрацій носіїв зарядів [5]. Таким чином, у розімкнутому ланцюгу виникає ЕРС, а при замиканні ланцюга тече електричний струм у повній відповідності до рівняння (1).

Описану модельну ситуацію можна побачити у варізонному напівпровіднику SiGe [6, 7].

Для отримання максимального значення термоЕРС запропоновано наступну двошарову структуру: два варізонні шари SiGe (рис. 1, *а*) при об'єднанні яких у площині контакту утворюється гетероперехід (рис. 1, *б*).



а *б*

Рис. 1. Інжекція носіїв зарядів у гетеропереході при прямому зміщенні з урахуванням рівнів Фермі в структурі: *а* – у плавному гетеропереході за наявності внутрішніх «полів, що тягнуть», *б* – одностороння інжекція дірок у різкому гетеропереході

Отриманий гетероперехід має більшу генеруючу здатність. При цьому шари SiGe виконують функцію підвищення генеруючої здатності, чим формує цілісну структуру [8].

Моделювання та розрахунок температурного поля структури

Згідно з рівнянням (3), температура T двічі входять в рівняння (2), і досліджуваний об'єкт має складну двошарову структуру з параметрами, що плавно змінюються. Таким чином, для розрахунку поширення в ній тепла та зміни температури було запропоновано наступну теплофізичну модель [9, 10], що зображена на рис. 2.

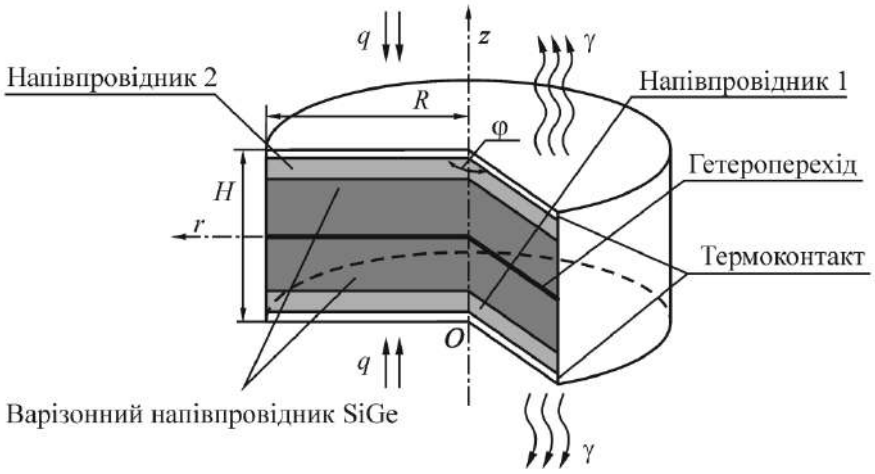


Рис. 2. Теплофізична модель варізонного напівпровідника у циліндричних координатах

Розрахунок за наведеною теплофізичною моделлю заснований на розв’язку диференціального рівняння нестаціонарної теплопровідності граничними умовами. Зважаючи на центральну симетрію моделі зручно використовувати циліндричну систему координат. Тоді рівняння нестаціонарної теплопровідності для неї матиме вигляд [11]:

$$div(\lambda(\vec{r},T)\nabla T(\vec{r},t)) + q(\vec{r},t) = c\rho\frac{\partial T(\vec{r},t)}{\partial t}, \quad (5)$$

де $\lambda(\vec{r},T)$ – коефіцієнт теплопровідності матеріалу елемента; $\vec{r}$ – радіус-вектор елемента; $T(\vec{r},t)$ – температура елемента; $q(\vec{r},t)$ – функція внутрішніх джерел тепла; c – питома теплоємність матеріалу елемента; ρ – густина елемента.

На зовнішніх поверхнях досліджуваної структури для рівняння (5) виконуються граничні умови 2-го та 3-го роду [12]:

– для $z = H$ (зовнішня межа, яка контактує з джерелом нагріву)

$$\left(\lambda(\vec{r},t)\frac{\partial T(\vec{r},t)}{\partial n}\right)\Bigg|_S = \gamma\left(T(\vec{r},t)\Big|_S - T_{cp}\right) - q(\vec{r},t),$$

де γ – коефіцієнт тепловіддачі поверхні; q – густина потоку тепла від джерела; T_{cp} – температура навколишнього середовища;

– для $z = 0$ (зовнішня межа, яка не контактує з джерелом нагріву)

$$-\lambda(\vec{r},t)\frac{\partial T(\vec{r},t)}{\partial n}\Bigg|_S = -\gamma\left(T(\vec{r},t)\Big|_S - T_{cp}\right),$$

– для $z = h$ (межа розділу між шарами)

$$-\lambda_1(\vec{r},T,t)\left(\frac{\partial T_1(\vec{r},t)}{\partial n}\right)\Bigg|_S = -\lambda_2(\vec{r},T,t)\left(\frac{\partial T_2(\vec{r},t)}{\partial n}\right)\Bigg|_S.$$

Для розв'язку рівняння (1) застосовано чисельний (сіточний) метод кінцевих різниць та метод кінцевих елементів.

В результаті розрахунків за рівняннями (4) і (5) отримуємо, що сумарна ЕРС досліджуваної структури описується виразом

$$\varepsilon = \varepsilon_1 + \varepsilon_2 + \varepsilon_3,$$

де ε_1 – термоЕРС першого варізонного напівпровідника; ε_2 – термоЕРС гетеропереходу; ε_3 – термоЕРС другого варізонного напівпровідника.

В результаті проведеного моделювання встановлено що в рамках заданої моделі рекомендованою температурою для роботи елементів на основі з'єднань SiGe є $T_{рек}$ = 353 – 358 К, а додаткова ЕРС склала 1,12 *В*, при цьому неоднорідність матеріалів, що враховується, у виготовлених варізонних шарах напівпровідників не перевищувала 5 %.

Висновки

1. Представлено двошарову варізонну структуру, що має три генеруючі шари.
2. Побудовано теплофізичну модель зазначеної структури, що дозволяє зробити розрахунок зовнішнього та внутрішнього температурних полів.
3. Визначено температурні межі найефективнішої роботи системи, що становлять 353 – 358 *К*.
4. Відповідно до розрахунків рівень додаткової ЕРС становить не менше 18 %.

Список літератури:

1. Saidov A., Leyderman A.Yu., Karshiev A.B. Photothermovoltaic Effect in a SixGe1–x Variband Solid Solution // Applied Solar Energy, 2019. №1(55). P. 12–17.

2. Хворостяний А.Д., Гензель В. Термоелектричний генератор. Пат. 119222 Україна МПК H01L35/00, заявл. 03.07.17; опубл. 11.09.17, Бюл. № 17, 8 с.

3. Гуревич Ю.Г., Юрченко В.Б. Проблемы формирования ЭДС в полупроводниках и вывода ее во внешнюю цеп // Физика и техника полупроводников. 1991. Вып. 12, т. 25. С. 2109–2114.

4. Fakhri M.A., Alwahib A.A., Salim E.T. Preparation and Characterization of UV-Enhanced GaN/Porous Si Photodetector using PLA in Liquid // Silicon. 2023. Vol. 15. P. 7523–7540.

5. Усмонов Ш., Мягкий А., Саидов А., Усмонова С. Термовольтаический эффект в варизонных полупроводниках // International Conference “Fundamental and Applied Problems of Physics”, September 22-23, 2020. P. 188–190.

6. M.A. Loganathan Ravi, K-L Rather, C-T Lin, T-Y Wu, K-Y Yu, Lai, J-I Chyi. Epitaxial Growth of GaN/AlN on h-BN/Si (111) by Metal-Organic Chemical Vapor Deposition: An Interface Analysis // ACS Applied Electronic Materials. 2023. Vol. 5(1). P. 146–154.

7. J-H Lee, K-S Im. Growth of High Quality GaN on Si (111) Substrate by Using Two-Step Growth Method for Vertical Power Devices Application. Crystals. 2021. Vol. 11(3), 234.

8. Saidov A.S., Usmonov S.N., Saparov D.V. Structural Studies of the Epitaxial Layer of a Substitutional Solid Solution (GaAs)1-x(ZnSe)x with Nanocrystals // Advances in Materials Science and Engineering. 2019. Vol. 2019, Article ID 3932195, 9 p.

9. Стороженко В.А., Малик С.Б. , Мягкий А.В. Оптимизация режимов тепловой дефектоскопии на основе теплофизического моделирования // Вісник НТУ “ХПІ”. 2008. №48. С. 50–54.

10. Малик С.Б., Мягкий А.В. , Стороженко А.В. Повышение чувствительности тепловой дефектоскопии в условиях наличия излучательной помехи // Вісник НТУ “ХПІ”. 2009. №14. С. 49–52.

11. Лазоренко О.В., Стороженко В.А., Мягкий А.В. Обработка результатов тепловой дефектоскопии сотовых конструкций с целью понижения уровня // Вісник НТУ “ХПІ”. 2013. № 34. С. 108–112.

12. Storozhenko V. , Myagkiy A., Orel R. Optimization of the Procedure of Thermal Flaw Detection of the Honeycomb Construction by Improving of Accuracy of Interference Function // Eastern-European Journal of Enterprise Technologies. 2016. №5/5 (83). P. 12–18

Надійшла до редколегії 23.02.2024

Відомості про авторів:

Мягкий Олександр Валерійович – кандидат технічних наук, Харківський національний університет радіоелектроніки, доцент кафедри фізики; Україна; e-mail: aleksandr.mjagky@nure.ua; ORCID: https://orcid.org/0000-0002-0442-5570

Орел Роман Петрович – кандидат технічних наук, доцент, Харківський національний університет радіоелектроніки, доцент кафедри фізики; Україна; e-mail: roman.orel@nure.ua; ORCID: https://orcid.org/0000-0002-3592-2393

Мешков Сергій Миколайович – кандидат технічних наук, доцент, Харківський національний університет радіоелектроніки, доцент кафедри фізики; Україна; e-mail: sergiy.meshkov@nure.ua; ORCID: https://orcid.org/0000-0003-3464-8318

Стороженко Володимир Олександрович – доктор технічних наук, професор, Харківський національний університет радіоелектроніки, професор кафедри фізики; Україна; e-mail: volodymyr.storozhenko@nure.ua; ORCID: https://orcid.org/0000-0002-7609-2955

RELATED PROBLEMS OF RADIO ENGINEERING
СУМІЖНІ ПРОБЛЕМИ РАДІОТЕХНІКИ

UDC 528.811 (1-021) **DOI:10.30837/rt.2024.1.216.11**

O.I. KOVALENKO, PhD, S.V. KALINICHENKO, D.M., N.I. SKIYAR, D.M.,
S.M. KULISH, PhD, prof., V.M. LEVCHENKO, PhD, T.I. ANTUSHEVA, PhD

THE ROLE OF OXYGEN IN THE MODIFICATION PROCESS OF STATE FUNCTIONALS OF WHEAT SEEDS AND LACTOBACTERIA BY AN ELECTROMAGNETIC FIELD

Introduction

Currently, one of the important tasks is the development and implementation of environmentally friendly technologies in various sectors of economic activity. In particular, attention is paid to the intensification of the cultivation of agricultural crops, including the improvement of methods of presowing seed treatment in order to increase their germination and productivity. In medicine, the issues of increasing the effectiveness of existing drugs, as well as the creation of alternative means to antibiotics for the treatment and prevention of infectious processes based on improved probiotic strains, remain relevant.

One of the universal factors that can influence the functional performance of biological objects of different classes is low-intensity EMF. There are experimental and clinical evidence of the effectiveness of the effect of specially organized EMFs on different classes of living organisms, including humans [1–4].

Existing models of the EMF interaction with the matter take into account the lines of resonant absorption of gases, the excitation of which triggers a chain of physicochemical processes that ultimately lead to functional changes in the organism.

In this regard, the question arises about the role of some gases on the life processes of biological objects and the possibility of their activation through the effect of low-intensity EMFs on the corresponding absorption lines.

Oxygen is the main biogenic element that is part of the molecules of all the most important substances that provide the structure and function of cells: proteins, nucleic acids, carbohydrates, lipids, as well as many low-molecular compounds. In percentage terms, the oxygen content in each plant or animal is much higher than the content of other elements (on average from 25 to 65 %). It enters living organisms in free and bound form (with water) during the process of respiration or biological oxidation, which is a more accurate formulation, since it characterizes the main reaction, and not the «devices» for its implementation. The process of biological oxidation, like all intracellular reactions that occur using nutrients as energy sources, is exergonic, i.e. with the release of energy [5, 6].

Biological oxidation, regardless of whether it occurs in the human body, plant tissues or in a bacterial cell, is a modification of chemical reactions of one of two types: 1) direct oxidation – obtaining energy as a result of the direct oxidation of various substrates by free atmospheric oxygen: molecular hydrogen, oxide carbon and sulfur, using oxidase enzymes, 2) indirect oxidation by dehydrogenation – the process of enzymatic removal of hydrogen from nutrient molecules (or substrates). The enzymes involved in these reactions are called dehydrogenases. When hydrogen is removed, an electron (energy) is released and becomes available for the cell. One of the dehydrogenases, the coenzyme diphosphopyridine nucleotide, contains the vitamin nicotine amide, or niacin, as its main component. Another dehydrogenase, the coenzyme flavin adenine dinucleotide, contains the vitamin riboflavin (vitamin B_2). Hence there is the need for these vitamins in food (or nutrient media) for those organisms that are not able to synthesize these compounds for their needs (humans and some bacteria).

The result of both processes is the same one, since in both cases, due to the transfer of electrons, the energy necessary for the cells is released. Consequently, the basis of all biological processes is electron transfer. The loss of an electron leads to oxidation, the addition of an electron to reduction. Since electrons cannot remain in a free state, every oxidation is accompanied by a reduction.

The presence of oxygen in the atmosphere significantly determined the nature of biological evolution, as a result of which aerobic, i.e., proceeding with the participation of free O_2, and anaerobic – without the participation of O_2, types of metabolism were formed. The use of oxygen, which has a high redox potential, as the final electron acceptor in the chain of respiratory enzymes has led to the emergence of a biochemical respiration mechanism that provides energy to aerobic organisms and is energetically more efficient than the anaerobic type [7].

In the aerobic type of respiration, molecular oxygen acts as a hydrogen acceptor, in the anaerobic one the hydrogen acceptor is not oxygen, but inorganic compounds – nitrate or sulfate.

In a living cell, the hydrogen of the substrate is transferred from the molecule of one hydrogen acceptor to the molecule of another acceptor, as if along a conveyor belt. As a result, hydrogen is transferred to a final acceptor located outside the cell, for example, oxygen (forming H_2O or H_2O_2), sulfur (forming H_2S) or CO_2 (forming CH_4). The nature of the final hydrogen acceptor is determined by the set of enzymes existing in the cell and is a constant and distinctive feature of cells of various types (aerobic or anaerobic) [6].

Aerobic respiration is typical for seeds. Anaerobic (intramolecular) respiration is concomitant at certain stages. Under unfavorable conditions, anaerobic respiration can become the main one. The difference between these two types of respiration is the final product that comes out. Aerobic respiration releases CO_2 and H_2O, and anaerobic respiration releases CO_2 and C_2H_5OH. Since in both cases the reactions occur with the release of carbon dioxide, the intensity of respiration is judged by the ratio of the volume of carbon dioxide released to the absorbed oxygen: CO_2/O_2 – respiratory coefficient. In seeds of cereal crops and seeds of other plants that have a lot of starch, it is close to 1. Under conditions of oxygen starvation, ethyl alcohol accumulates in plant seeds, which can lead to their poisoning with loss of germination [8].

The presence of oxygen is one of the main factors determining seed germination. Thanks to cell respiration, energy is provided too many interconnected processes – the breakdown of nutrients, their transformation, transport and the formation of new substances from them that go towards building cells and organs [9].

The highest intensity of oxygen absorption by seeds occurs in the first stages of germination after they are soaked. The intensity of the hexose monophosphate pathway, and then glycolysis, increases especially strongly. Increasing respiration intensity is accompanied by an increasing the accumulation of adenosine triphosphate (ATP), which is, in turn, a necessary condition for metabolic processes. After 10–12 hours from the beginning of swelling, mitochondria are rapidly growing and differentiating. Some of the mitochondria that were degraded during seed maturation are reactivated. Subsequently, after 24 hours, mitochondria fission occurs and their number increases sharply. The process of oxidative phosphorylation intensifies and becomes the main source of ATP accumulation. The compounds, formed as a result of decomposition, flow into the axial part of the embryo, where they are partially consumed during respiration, and partially for the construction of substances necessary for the growth of new cells and organs (proteins and nucleic acids, components of cell membranes: cellulose, pectin substances, as well as various lipids, which are part of the membranes). At this germination phase, DNA (deoxyribonucleic acid), RNA (ribonucleic acid) are synthesized, and phytohormones are also formed that regulate the growth of the embryo (embryogenesis). Thus, the germination phase is characterized by the sprout being fed with ready-made organic substances found in the endosperm or cotyledons. When the first green leaves appear and photosynthesis begins, germination ends and the plant enters the next – juvenile phase [10].

The quantity of oxygen required varies greatly among different plants. For example, rice seeds germinate underwater with very little dissolved oxygen. Most agricultural seeds need plenty of air and do not germinate under water [11].

As for microorganisms, they are characterized by aerobic, anaerobic and mixed types of respiration. Thus, many bacteria can exist in aerobic and anaerobic conditions. Such microorganisms are called facultative (optional) anaerobes. For example, staphylococci, Escherichia coli and other facultative anaerobes have a full set of respiratory enzymes that ensure their existence in oxygen and oxygen-free environments. Facultative anaerobes have nitrate respiration, when the oxidation of organic compounds produces nitrate (a hydrogen acceptor), which is reduced to molecular nitrogen and ammonia.

There are also obligate (obligatory) anaerobes, which can only exist in strictly anaerobic conditions. Among the pathogenic ones are the causative agents of tetanus, gas gangrene, and botulism. Obligate anaerobes, when oxidizing organic compounds, form sulfate, which is reduced to hydrogen sulfide, therefore obligate respiration is also called sulfate one [6].

To neutralize toxic forms of oxygen, microorganisms that can exist in its atmosphere have protective mechanisms. In obligate aerobes and facultative anaerobes, the accumulation of the oxygen radical O_2 is prevented by the enzyme superoxide dismutase, which breaks down the oxygen radical into hydrogen peroxide and molecular oxygen. Hydrogen peroxide in these bacteria is decomposed by catalase into water and molecular oxygen. The growth of obligate anaerobes stops in the presence of oxygen. This is due to the fact that life in aerobic conditions leads to the fact that the final product of the oxidation of organic compounds is hydrogen peroxide, and since anaerobes do not produce the enzyme catalase, which breaks down hydrogen peroxide, it accumulates and has a toxic effect on anaerobic bacteria [12].

The universal carrier of chemical energy in processes with releasing energy is ATP. The formation of ATP energy is observed among other things during fermentation. The peculiarity of fermentation is that organic compounds simultaneously serve as electron donors (during their oxidation) and acceptors (during their reduction). Fermentation occurs in the absence of oxygen, under strictly anaerobic conditions. The main compounds of fermentation are carbohydrates. The alcoholic, lactic acid (homofermentative and heterofermentative), acetic acid, butyric acid and other types of fermentation are distinguished depending on the participation of a particular microbe and the final products of carbohydrate breakdown. The release of energy during anaerobic processes is much less; for example, during the fermentation of glucose by yeast, alcohol is formed and only 31,2 kcal. Alcoholic fermentation occurs mainly in yeast. The final products are ethanol and CO_2. Glucose fermentation occurs under anaerobic conditions. With the access of oxygen, the fermentation process weakens and respiration takes its place.

Lactic acid bacteria are aerotolerant, i.e. they do not use oxygen to obtain energy, but can exist in its atmosphere. Basically, lactobacilli obtain energy through heterofermentative lactic acid fermentation [12].

It is necessary in laboratory studies of this group of bacteria to take into account the gas composition of the incubation atmosphere as one of the important parameters for the development of microorganisms. It is known that in the biological niches of the human body *in vivo*, the conditions for cultivating bacteria differ significantly when they are extracted *in vitro*. The priority for them is microaerophilic conditions – with a reduced oxygen content. The atmosphere of reduced partial pressure of oxygen and increased carbon dioxide content, to a certain extent, reproduces the living conditions of lactobacilli *in vivo*. To create it, special devices are used – anaerostats, from which air oxygen is removed or replaced with another inert gas. Oxygen-free conditions can also be created by boiling the medium or using chemicals that actively absorb oxygen from the space where the dishes and test tubes with cultures are placed.

Thus, when developing methods for the influence of low-intensity, specially organized EMFs on plant seeds and microorganisms, for the purposeful modification of their functional properties, it is relevant to study the role of individual gases, in particular oxygen, as a separate factor determin-

ing the viability of biological objects, as well as a link in the model of perception and transmission of electromagnetic energy.

Purpose of the work: to study the role of oxygen in the process of modifying the functional indicators of the state of wheat seeds of soft varieties and strains of lactobacilli by irradiating them with low-intensity EMF on the resonant absorption lines of oxygen, hydrogen and ozone, with additional enrichment of water with oxygen during its irradiation and subsequent soaking of seeds in it, as well as by creating conditions for cultivating bacteria in an environment with normal and reduced oxygen content.

Materials and methods

The studied objects were soft wheat seeds, as well as standard probiotic strains of lactobacilli: *L. rhamnosus*, *L. acidophilus* and a strain of *L. plantarum* extracted from the intestines of bees.

A measuring stand was prepared to carry out the experimental work.

Generators G4-141 (f = 37,5–53,57 GHz) and G4-142 (f = 53,57–78,33 GHz) were used as EMF sources in narrow frequency bands of the EHF range, the radiation power of which did not exceed 5 mW. The waveguide outputs of the generators were loaded with horn antennas with apertures in 6,0×5,0 cm^2 and 8,5×6,5 cm^2. Irradiation was carried out in the near zone of the antenna, at a distance of 5–7 cm from the opened horn. The power flux density was 0,1 mW/cm^2 with uneven irradiation at the location of the objects no more than 3dB.

The electromagnetic effect on wheat seeds was carried out indirectly, by soaking dry seeds in water pre-irradiated with EMF and aerating it with oxygen. To carry out the electromagnetic effect, frequencies in the EHF range were selected corresponding to the resonant absorption lines of atmospheric gases: 61,0 GHz for oxygen, 58,0 GHz for hydrogen, 42,2 GHz for ozone. The effect time was 5, 10, 30 and 60 minutes.

To enrich water with oxygen, a device was made, consisting of a container for carrying out chemical reactions and a system of tubes that ensure the delivery and uniform distribution of gas in water. Oxygen was produced in a laboratory manner as a result of the reaction of a solution of hydrogen peroxide with potassium permanganate. Aeration of water with oxygen was carried out during its irradiation with EMF for 15 minutes.

Seed germination was carried out in Petri dishes of 50 pieces each, which were placed in a specially made thermostat and kept at a temperature of 23 ± 1 ºC.

The main indicators of the biological activity of plant seeds were assessed – germination energy (E_g), average length of roots (L_{rmid}) and sprouts (L_{smid}) for 72 hours of observations carried out in accordance with state standards [13, 14].

Irradiation of lactobacilli strains was carried out in the frequency ranges of 42,2 and 61,0 GHz for 3 hours. Cultivation of bacteria was carried out in aerobic (at normal oxygen content *in vitro* conditions 20 %) and microaerophilic conditions (at low oxygen content, simulating *in vivo* conditions).

Microaerophilic conditions for the cultivation of bacteria were created in microanaerostats using gas-generating packages Generator GENboxmicroaer (bioMerieux, France) or a gas mixture manufactured in a factory and consisting of O_2 – 5 %, CO_2 – 10 % and N_2 – 85 %.

The following features were assessed:

1) The quantity of glucose consumed by strains of *L. rhamnosus*, *L. acidophilus* and *L. plantarum* from the nutrient medium using the glucose oxidase method. This indicator determines the potential ability of cells to actively develop. It is used to judge the metabolic activity of microorganisms, as well as the activation or inhibition of catabolic processes [15].

2) Fractional composition of *L. plantarum* exometabolites, which was determined by gel filtration chromatography (exclusive, gel permeation or sieve chromatography) [16]. This method is based on the separation of substance molecules by size due to their different penetrating abilities into the pores of the carrier.

Exometabolites are metabolic products released by microorganisms into the environment. They play an important role in inter- and intrapopulation communications. Exometabolites include high and low molecular weight peptides, the molecules of which are built from two or more amino acid residues. Antimicrobial peptides that can kill microbial cells are distinguished from the total number – these are bacteriocins or plantaricins (due to *L. plantarum*). Plantaricins are cationic thermostable peptides with a molecular weight of less than 10 kDa (most often in the range of 2–6 kDa) [17, 18].

The results obtained were processed in accordance with the rules of variation statistics [19] using standard programs.

Research results

In the first experiment the changes in the functional parameters of soft wheat seeds, which were soaked in water pre-irradiated with EMF and additionally saturated with oxygen, were studied. The measurement results are presented in table. 1.

Table1

The influence of low-intensity EMFs on the functional parameters of soft wheat seeds, carried out indirectly through irradiated water enriched with oxygen (* – $p < 0,05$; ** – $p < 0,001$)

Exposure mode			Functional indices		
O_2	EMF				
T, min	f, GHz	T, min	E_g, %	$L_{r\,mid}$, mm	$L_{s\,mid}$, mm
Control			90,0	19,9	15,6
15	oxygen control		92,1	24,0*	16,3
	61,0	5	90,4	28,4*	18,2*
		10	94,0	31,9**	19,3**
		30	93,3	21,7	15,8
		60	92,8	24,9	18,0
	58,0	5	91,3	26,5	16,8
		10	91,7	25,1	16,0
		30	91,7	24,0	16,6
		60	91,0	20,7*	15,0
Control			91,4	18,4	14,0
15	oxygen control		92,1	24,0*	16,3
	42,2	5	90,7	13,7**	13,3*
		10	92,0	14,6**	14,3
		30	90,7	17,8**	15,7
		60	92,0	15,6**	14,5

As a result of soaking wheat seeds in water pre-enriched with oxygen without EMF irradiation, stimulation of all considered functional indicators was observed. At the same time, a significant increasing 1,2 times ($p < 0,05$) was found only when measuring the average root length. These data

are taken as control ones for assessing the indirect water effect of EMF on seeds when it is additionally enriched with oxygen («oxygen control») (Fig. 1, 2).

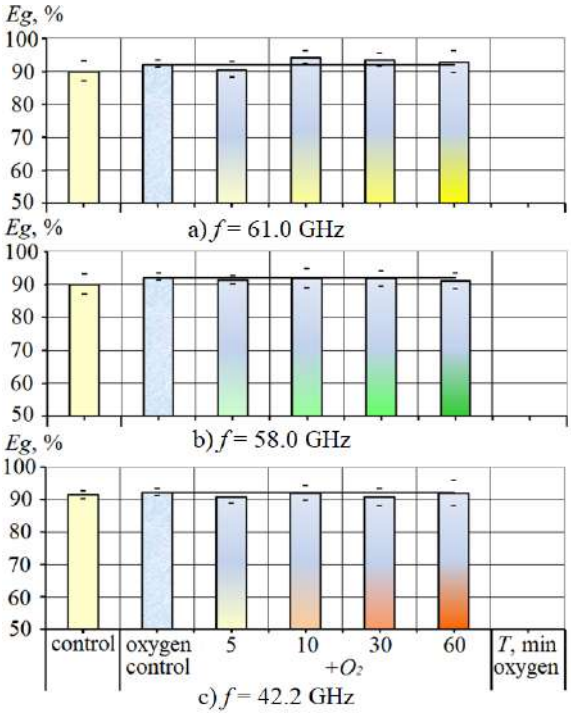


Fig. 1. Changes in germination energy during indirect EMF irradiation of soft wheat seeds through oxygen-enriched water

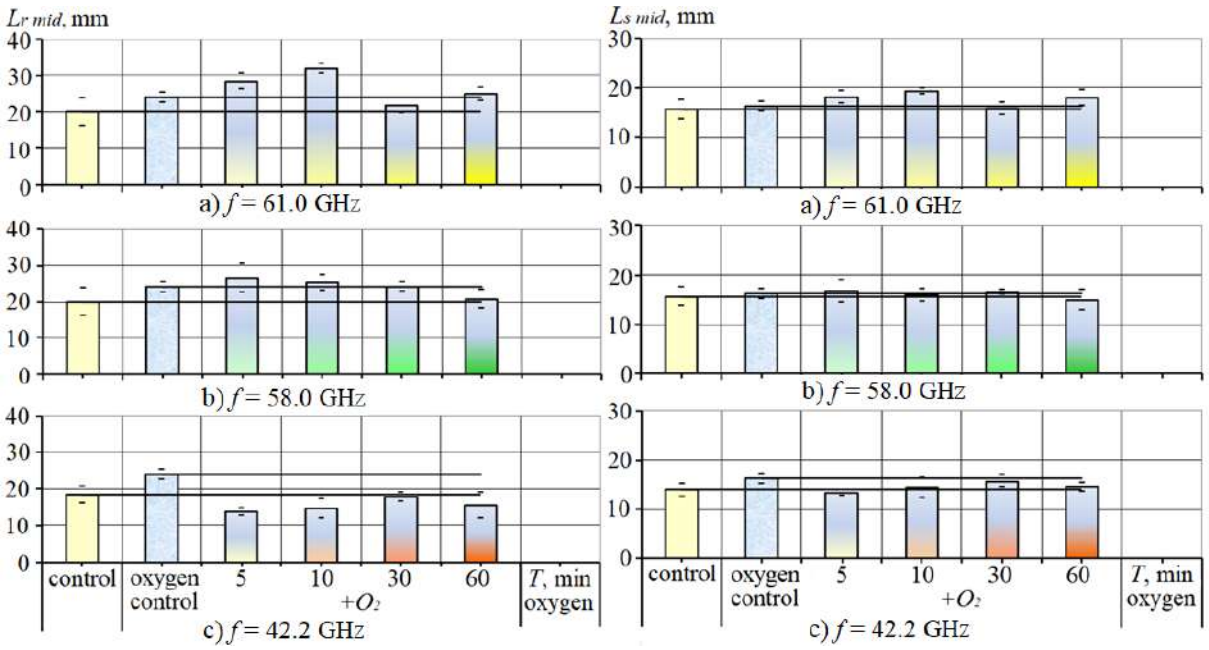


Fig. 2. Changing the average length of roots and sprouts during indirect EMF irradiation of soft wheat seeds through oxygen-enriched water

Irradiation of wheat seeds in the range of 61,0 GHz through water enriched with oxygen, led to additional stimulation relative to the «oxygen control» of the L_{rmid} and L_{smid} indicators by an average of 1,2 times with short-term effect of 5 and 10 minutes. At the same time, a 10-minute effect turned out to be more effective ($p < 0{,}001$). Increasing the effect time of EMF to 30 and 60 minutes did not

give significant changes. At 30 minutes of signal exposure a tendency was observed towards inhibition of the average length of roots and sprouts (see Fig. 2).

When wheat seeds were soaked in water irradiated in the frequency range of 58,0 GHz, there was a tendency for E_g decreasing relatively to the «oxygen control» under all effect modes. A reliable result was obtained with signal exposure for 1 hour – inhibition of the average root length by 1,2 times ($p < 0,05$).

Irradiation of water in the 42,2 GHz frequency band while enriching it with oxygen and subsequent soaking of seeds in it led to inhibition of all the studied functional parameters of the seeds, regardless of the time of signal effect. Thus, the average length of sprouts decreased on average by 1,6 times ($p < 0,001$). Irradiation for 5 minutes turned out to be the most effective with the average length of roots decreasing by 1,2 ($p < 0,05$), and sprouts by 1,8 times ($p < 0,001$) (see Fig. 1, 2).

Previously, indirect EMF irradiation of soft wheat seeds through water was carried out under similar effect modes, but without additional enrichment of water with oxygen [20].

Comparing the published data [20] with the results presented in Table 1, we can note the general positive role of oxygen on seed germination. When oxygen is activated in the frequency range of 61,0 GHz, additional stimulation of the state functionals of wheat seeds is observed with short-term irradiation for 5 and 10 minutes. Increasing the effect time is less effective.

When water enriched with oxygen is irradiated in the hydrogen absorption band of 58,0 GHz, a decreasing the efficiency of electromagnetic influence is observed. Tendencies of inhibition of the functional state of wheat seeds intensify with increasing signal exposure.

Irradiation of water enriched with oxygen at the ozone absorption line of 42,2 GHz leads to additional inhibition of the functional state of wheat seeds. The value of inhibition varies depending on the time of electromagnetic effect.

In the next experiment, we studied the influence of EMF in the frequency ranges of 42,2 and 61,0 GHz on the functional parameters of microorganisms, the cultivation of which was carried out under different conditions: at high (aerobic) and low (microaerophilic) oxygen content.

The studied microorganisms were strains of lactobacilli: *L. plantarum*, *L. rhamnosus*, *L. acidophilus*. The condition of the bacteria was assessed by changes in their enzymatic activity, namely, by the quantity of glucose consumed from the nutrient medium.

For most organisms glucose is a universal source of energy and also serves as an indicator of the potential rate of development of subpopulations. Therefore, determining the quantity and rate of its utilization is very important in the selective search for strains producing biologically active substances and assessing their stability with subsequent use in biotechnology.

As a result of preliminary studies of the influence of the cultivation atmosphere on the quantity of glucose consumed by lactobacilli, it was defined that microaerophilic conditions contributed to its increase (Table 2).

Table 2

The quantity of glucose consumed by lactobacilli strains under different cultivation conditions (* – $p < 0,05$)

Strains *Lactobacillus spp.*	Cultivation conditions	
	aerobic	microaerophilic
L. plantarum	13,2±0,16*	14,7±0,06*
L. rhamnosus	11,4±0,07*	12,6±0,07*
L. acidophilus	12,5±0,07*	14,5±0,06*

In all studied strains of *Lactobacillus spp.* the quantity of glucose consumed increased on average by 12,6 % ($p < 0,05$), it may be associated with a changing the rate of metabolic processes under conditions of oxygen deficiency.

In the next part of the experiment lactobacilli *L. plantarum*, *L. rhamnosus* and *L. acidophilus* were subjected to electromagnetic irradiation in the frequency ranges of 42,2 and 61,0 GHz for 3 hours. The results of measuring the quantity of glucose consumed by lactobacilli cultivated under aerobic conditions are presented in table. 3.

Table 3

The influence of low-intensity EMFs on the quantity of glucose consumed by lactobacilli strains when they are cultivated under aerobic conditions (* – $p < 0,05$)

Strains *Lactobacillus spp.*	EMF exposure mode		
	Control	42,2 GHz	61,0 GHz
L. plantarum	13,9±0,16	13,0±0,05	14,2±0,06
L. rhamnosus	12,0±0,07	15,6±0,1*	16,2±0,09*
L. acidophilus	12,5±0,07	14,0±0,07*	14,5±0,08*

The data obtained indicate increasing the quantity of glucose consumed in most strains after irradiation. Significant changes are observed in strains of *L. rhamnosus* and *L. acidophilus*. When effected to the 42,2 GHz range, the quantity of glucose consumed increased by 30 and 12 % ($p < 0,05$), respectively. When irradiated in the range of 61,0 GHz, increasing was 35 and 20 % ($p < 0,05$) (Fig. 3).

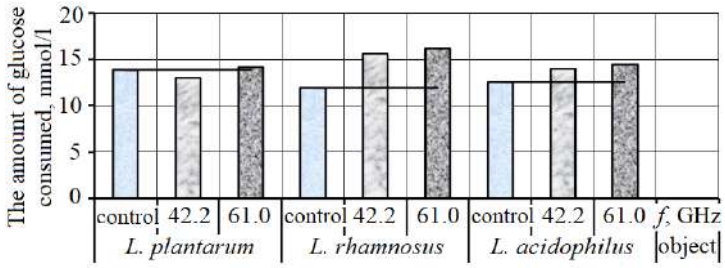


Fig. 3. Changes in the average quantity of glucose consumed by lactobacilli: *L. plantarum*, *L. rhamnosus*, *L. acidophilus*, cultivated under aerobic conditions, after EMF effect

Thus, one can see a frequency dependence of the effectiveness of electromagnetic influence on the functional state of lactobacilli strains cultivated under aerobic conditions. The greatest stimulation of consumed glucose was observed for irradiation in the 61,0 GHz frequency band in the *L. rhamnosus* strain.

The positive effect of lactobacilli on the human organism is due not only to their ability to colonize, but also to their high antagonistic abilities in the biocenosis with pathogens, and they, in turn, depend on the production of antimicrobial compounds of protein origin (plantaricins). The activity and level of their production is determined by the conditions in which lactobacilli are found.

A study of the fractional composition of *L. plantarum* exometabolites under different conditions of the gas composition of the cultivation atmosphere was carried out (Table 4).

In the studied exometabolites of the *L. plantarum* strain the low molecular weight peptides were extracted – protein components of the nutrient medium (fractions I – E), as well as peptides with a relatively high molecular weight: 1195–7670 Da – presumably plantaricins (molecular weight 2–6 kDa, fractions D–A). Peptides with molecular weight ≥ 12 kDa were not selected.

Under aerobic cultivation conditions 9 fractions of microbial peptides with a molecular weight from 546 to 5667 Da were extracted from exometabolites of the *L. plantarum* strain. Share of peptide fractions with molecular weight up to 2 kDa was 23,8 %, from 2 to 6 kDa – 71 %, ≥ 12 kDa – 5,2 % of the total quantity.

When cultivated under microaerophilic conditions, 10 fractions of microbial peptides were extracted. Fraction D appeared, which was absent under aerobic cultivation conditions. At the same time, the share of low molecular weight peptides with molecular weight up to 2 kDa significantly decreased by 1,3 times ($p < 0,05$) and amounted to 18,5 %, and the share of peptides with molecular weight 2–6 kDa increased to 76,8 %.

Table 4

Influence of cultivation conditions and low-intensity EMF on the share of peptide fractions (%) *L. plantarum*

Fractions	Molecular weight, Da ($M \pm m$)	Aerobic conditions			Microaerophilic conditions		
		control	*f*, GHz		control	*f*, GHz	
			42,2	61,0		42,2	61,0
0	≥12000	5,2	7,7	2,9	4,7	7,5	5,2
Aa	7300±370	–	–	27,3	–	–	–
A	5580±87	51,3	51,5	12,6	58,8	59,4	59,5
B	3710±125	8,8	8,4	6,6	7,3	6,2	3,7
C	3020±29	10,9	9,2	–	7,9	8,4	12,3
D	2330±63	–	1,8	5,0	2,8	–	–
E	1780±36	3,4	2,7	2,9	2,7	2,6	3,4
F	1460±16	5,5	5,1	4,8	4,7	5,0	5,4
G	1220±25	4,2	3,2	14,2	3,2	3,1	3,2
H	870±20	6,5	4,9	14,3	4,4	4,3	4,0
I	550±4	4,2	5,5	9,4	3,5	3,5	3,3

Thus, it was experimentally shown that microaerophilic cultivation conditions at a reduced partial pressure of oxygen contribute to the stimulation of the production of peptides with molecular weight 2–6 kDa by the *L. plantarum* strain (presumably plantaricins – antimicrobial compounds of protein origin) and a decreasing the share of low molecular weight proteins in the nutrient medium, which indirectly indicates increasing the antagonistic activity of the strain and, accordingly, an improvement in its absorption of nutrients from the medium. These data were taken as reference ones for further assessment of the effectiveness of electromagnetic influence.

The results of studying the fractional composition of exometabolites of the *L. plantarum* strain after its irradiation with EMF under different cultivation conditions are presented in Table. 4.

After irradiation of the *L. plantarum* strain in the frequency band 42,2 GHz, 10 fractions of microbial peptides with a molecular weight from 546 to 5667 Da were extracted from exometabolites obtained under aerobic cultivation conditions. In this case, fraction D with share of 1,8 % missing in the control was extracted. When comparing the obtained data with the reference ones, the share of low-molecular and high-molecular fractions on average decreased slightly.

When irradiated in the range of 61,0 GHz under aerobic cultivation conditions, 10 fractions of microbial peptides with a molecular weight from 546 to 7670 Da were also extracted. The share of fractions with a molecular weight up to 2 kDa was 45,6 %, from 2 to 6 kDa – 24,2 %, ≥ 12 kDa – 2,9 %. At the same time, fraction Aa was extracted from exometabolites of *L. plantarum* – 27,3 % of the total quantity of microbial peptides, which was absent in other studied samples. Fraction C

was not extracted, whereas in the control the share of these peptides was 10,9 %. When comparing these data with the reference ones, it is clear that the share of low molecular weight peptides with a molecular weight of up to 2 kDa significantly increased by 1,9 times ($p < 0,001$), and the share of putative plantaricins (2–6 kDa), on the contrary, decreased by 2,9 times ($p < 0,001$), and even taking into account the Aa fraction, the decreasing was 1,4 times (Fig. 4, *a*).

Under microaerophilic cultivation conditions, 9 fractions of microbial peptides with a molecular weight from 546 to 5667 Da were extracted from exometabolites of *L. plantarum* obtained after its irradiation with EMF in the frequency ranges of 42,2 and 61,0 GHz. In this case, fraction D was absent, which in the reference was 2,8 % (Table 4). Effect in the range of 42,2 GHz did not significantly affect the changing the fractional composition of exometabolites of the *L. plantarum* strain.

Irradiation of *L. plantarum* in the range of 61,0 GHz when cultivated in microaerophilic conditions contributed to the stimulation of the formation of peptides with a molecular weight from 1 to 2 kDa by 1,1–1,2 times ($p < 0,05$), with a molecular weight of 2991–3049 Da – by 1,55 times ($p < 0,05$) and inhibition with a molecular weight of 3585–3835 Da by 1,97 times ($p < 0,05$) (Fig. 4, *b*).

Thus, it has been obtained that the activation of oxygen by EMF in the EHF range has a diverse effect on the functional indicators of aerotolerant lactobacilli, for which microaerophilic conditions are a priority. In this case, stimulation of some functions is observed, for example, glucose uptake, and, consequently, increasing the colonization ability of the population, and inhibition of others, for example, antimicrobial abilities, occurs, which is further aggravated under aerobic cultivation conditions.

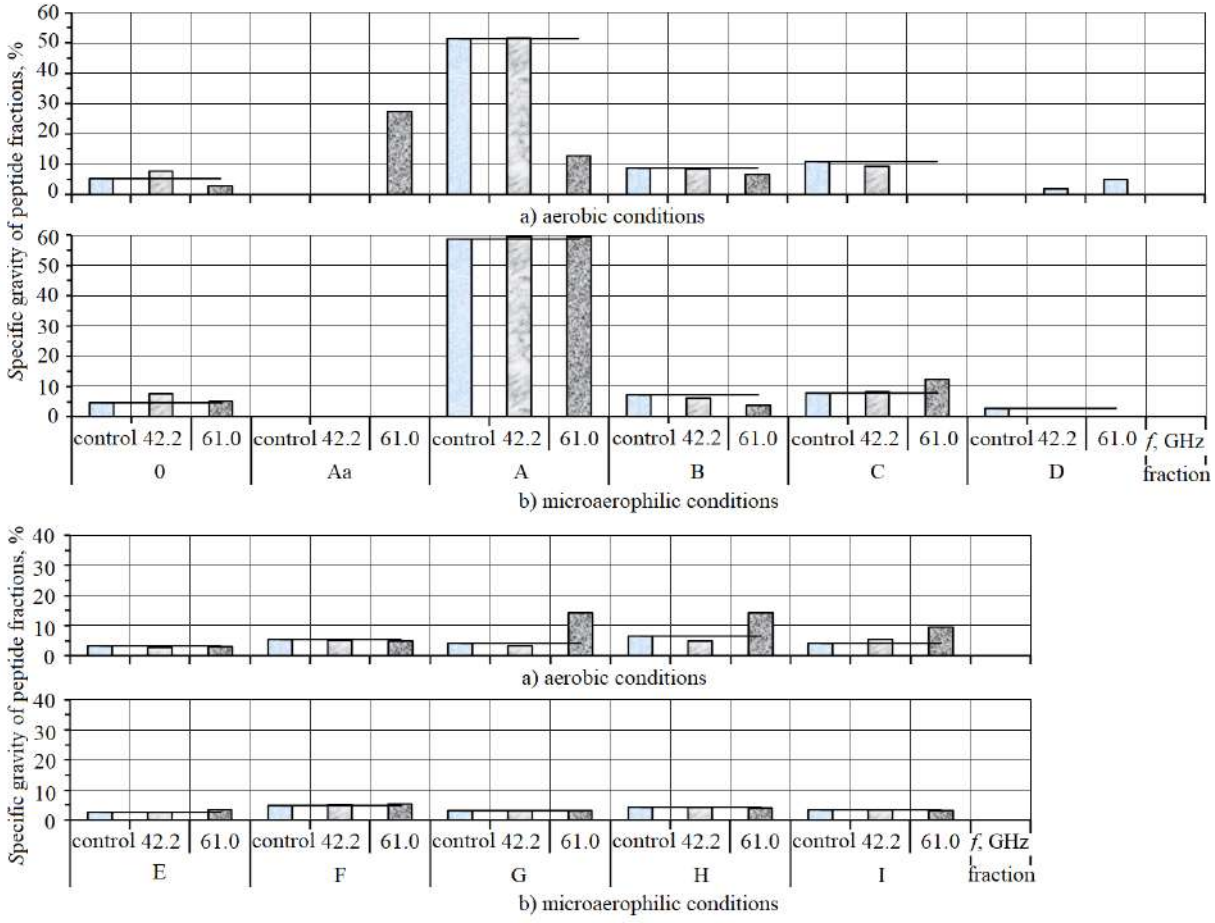


Fig. 4. Changes in the share of peptide fractions of *L. plantarum* cultivated under aerobic conditions after EMF effect

Conclusions

1. The possibility of targeted modification of the functional parameters of soft wheat seeds and lactobacilli through their irradiation with low-intensity EMF in the EHF range on the resonant absorption lines of oxygen, hydrogen and ozone has been defined.

2. The role of oxygen in the life activity of biological objects of different classes is shown: wheat seeds and lactobacilli. The possibility of stimulating the germination process of soft wheat seeds by soaking them in water previously enriched with oxygen has been found. For lactobacilli, the priority of microaerophilic cultivation conditions is shown with a reduced partial pressure of oxygen and an increased content of carbon dioxide, which imitates the conditions for the presence of bacteria *in vivo* (inside the body). Thus, in strains of lactobacilli under microaerophilic conditions the following are observed:

– stimulation of enzymatic activity, namely increasing the quantity of glucose consumed, which indicates increasing growth rate of subpopulations;

– stimulation of the production of peptides, presumably plantaricins (with a molecular weight of 2–6 kDa) and a decreasing the share of low molecular weight proteins in the nutrient medium, which, accordingly, indicates increasing the antagonistic activity of probiotic strains in the biocenosis with pathogenic bacteria and an improving the absorption of nutrients from the environment.

3. The dependence of the effectiveness of low-intensity irradiation in the EHF range on frequency has been defined. The possibility of stimulating seed germination, when irradiated indirectly through oxygen-enriched water at the oxygen resonance absorption line of 61,0 GHz with a short signal exposure of 5 and 10 minutes, has been shown. Increasing the effect time does not contribute to stimulation, it may be caused by the formation of active and reactive oxygen forms under the influence of EMF at a resonant frequency. Irradiation in frequency ranges not associated with oxygen resonance is less effective. Thus, when effected to hydrogen absorption lines at 58,0 GHz, tendencies toward suppression are observed. Irradiation at the ozone resonance frequency of 42,2 GHz leads to a significant suppression of the studied parameters. Thus, the relevance of water-dissipative and gas models of interaction of EMF with matter has been confirmed.

4. A non-monotonic dependence of the biological response on the time of signal effect, which is individual for each frequency range, is shown. The most significant modes of effect have been identified.

5. It has been obtained that when irradiated with low-intensity EMFs in the EHF range on the cultures of *L. plantarum, L. rhamnosus, L. acidophilus*, a dispersion dependence on frequency is observed. The magnitude of the influence depends on the cultivation conditions. Thus, effect in the frequency range of 42,2 and 61,0 GHz contributed to increasing the quantity of glucose consumption by lactobacilli when cultivated under aerobic conditions. At the same time, the 61,0 GHz frequency range turned out to be more efficient.

6. When assessing the share of peptide fractions of exometabolites of the *L. plantarum* strain after irradiation in the frequency range of 61,0 GHz under aerobic cultivation conditions, inhibition of the production of high molecular weight peptide fractions (presumably plantarcins – antimicrobial compounds of protein origin) and increasing low molecular weight proteins of the nutrient medium were observed. Under microaerophilic cultivation conditions, changes after irradiation turned out to be insignificant. This confirms the unfavorable effect of oxygen on lactobacilli when they are *in vitro*. Effect of EMF in the frequency range of 42,2 GHz under aerobic and microaerophilic cultivation conditions also had a depressing result, which manifested itself to a lesser extent.

The results obtained open up the prospect of using electromagnetic technologies in agriculture when preparing seeds for sowing and in medicine, in particular in the development of new generation drugs based on lactobacilli with increased colonization and antagonistic properties towards pathogens.

References:

1. Avdeenko V.S., Kalyuzhny I.I., Krenitsky A.P. [etc.]. Influence of electromagnetic EHF oscillations at the frequencies of the molecular absorption spectrum of atmospheric oxygen on the functional state of red blood cells in animals // Biomedical technologies and radio electronics. 2003. 2: 29–8. [in Russian].
2. Belous O.I., Malakhov V.A., Doroshenko G.I., Sirenko S.P., Fisun A.I. Comparative Study into Effeciency of Treating the Initial Stage of Cerebral Ischemia with Low-Intensity Millimeter and Centimeter Electromagnetic Waves // Telecommunications and Radio Engineering. 2003. 59 (3&4): 151–3.
3. Bingi V.N., Savin A.V. Physical problems of the action of weak magnetic fields on biological systems // Physical problems of the action of weak magnetic fields on biological systems. 2003. 173 (3): 265–6. [in Russian].
4. Kovalenko O.I., Kivva F.V., Movchan L.N., Korotkikh E.O. The influence of pulsed EMFs of the microwave range on human health // Current problems of the humanities and natural sciences. 2014. 01(60). Part 2: 184–4. ISSN 2073–0071. [in Russian].
5. Oxygen is the basis of life: monograph. In: Syrovoy A.O., editor. Kharkov; 2013. 232 p. [in Russian].
6. Frobisher M. Fundamentals of microbiology [transl. from English V. A. Shorina]. M. : Mir, 1965. 678 p. [in Russian].
7. Vorobyov A.V., Bykov A.S., Pashkov E.P., Rybakova A.M. Microbiology : Textbook. 2nd ed., revised and expanded. M. : Medicine, 2003. 336 p. [in Russian].
8. Kuznetsov V.V., Dmitrieva G.A. Plant Physiology in 2 Vol. Volume 2, 4th ed. revised and expanded. Text-book for academic bachelor's degree. M. : Publishing house Yurayt, 2019. 459 p. ISBN: 978–5–534–01713–7 [in Russian].
9. Volodko I.K., Rupasova Zh.A., Titok V.V. // Parfenova VI, editor. Ecological and biological bases of the introduction of rhododendrons (Rhododendron L.) in the conditions of Belarus. Minsk : Belaruskaya navuka;, 2015. 269 p. ISBN 978–985–08–1812–6. [in Russian].
10. Isain V.N. Fundamentals of botany. M. : Selkhozgiz, 1954. 167 p. [in Russian].
11. Rogozhin V.V., Verkhoturov V.V., Kurilyuk T.T., Okhlopkova E.P. The influence of temperature, ultraviolet radiation and functionally active substances on the germination of wheat seeds // News TSHA. 1999; 3: 105–20. [in Russian].
12. Methods of determination of germination energy and germination capacity: GOST 10968–88. [Effective from 1988–01–07]. M. : Publishing house of standards, 1988. 5 p. [in Russian].
13. Seeds of agricultural crops. Methods of the quality determination: DSTU 4138–2002. [Effective from 2002–12–28]. K. : Derzhspozhyvstandart of Ukraine, 2003. 173 p. (National Standard of Ukraine). [in Ukrainian].
14. Medical microbiology, virology and immunology // acad. RAMS Vorobyova A.A., editor. M. : MIA; 2004. 691 p. 5000 copies. ISBN 5–89481–209–7. [in Russian].
15. Bidlingmeyer B., Fried B., Hegnauer G. and others. Preparative liquid chromatography: Trans. from English // Bidlingmeyer B, editor. M. : Mir, 1990. 360 p. [in Russian].
16. Rybalchenko O.V., Orlova O.G., Bondarenko V.M. Antimicrobial peptides of lactobacilli // Journal of Microbiology, Epidemiology and Immunobiology. 2013. 4: 12. [in Russian].
17. Sobolev A.V., Kolobov A.A., Grishina T.V. Chromato-mass spectrometric analysis of antimicrobial peptides from the culture of Lactobacillus plantarum 8PA-3 [Internet] // Modern problems of science and education. 2014; 3. Avaslable from: http://www.science-education.ru/pdf/2014/3/576.pdf.
18. Bendat J. and Pirsol A. Applied random data analysis [tr. English Privalsky V.E., Kogubinsky A.I.]. M.: World, 1989. 540 p. [in Russian].
19. Kovalenko O.I., Roenko A.N., Kivva F.V. Wheat seeds in direct exposure to micro wave radiation through water // Telecommunication and Radio Engineering. 2019. 78 (18): 10. ISSN Print: 0040–2508, ISSN Online: 1943–6009.

Received 09.02.2024

Information about the authors:

Kovalenko Olga Ivanivna – Ph.D. of Physico-mathematical Sciences, O.Ya.Usikov IRE NAS of Ukraine, Ukraine; e-mail: kovalenko-ire@ukr.net; ORCID: https://orcid.org/0000-0003-1002-7904

Kalinichenko Svitlana Viktorivna – Head of the laboratory, D.M., D.Hab., GA "Institute of Microbiology and Immunology named after I.I. Mechnikov of the National Academy of Medical Sciences"; Ukraine; e-mail: kalinichenko_sv@ukr.net; ORCID: https://orcid.org/0000-0002-3482-9605

Sklyar Nadia Ivanivna – D.M., D.Hab., GA «IMI NAMS»; Ukraine; e-mail:sklyarimi@ukr.net; ORCID: https://orcid.org/0000-0002-8534-1431

Kulish Sergey Mykolayovych – Ph.D. of Engineering Sciences, Professor, National Aerospace University "Kharkiv Aviation Institute"; Ukraine; e-mail: s.kulish@khai.edu; ORCID: https://orcid.org/0000-0002-5506-2714

Levchenko Volodymyr Mykolayovych – Ph.D. of Engineering Sciences, O.Ya.Usikov IRE NAS of Ukraine, Ukraine; e-mail: goldangel271@gmail.com; ORCID: https://orcid.org/0000-0002-2411-4198

Antusheva Tetyana Ivanivna – Ph.D. of Biology Sciences, GA «IMI NAMS», Ukraine; ORCID: https://orcid.org/0009-0006-0953-2830

УДК 004.89: 621.396 **DOI:10.30837/rt.2024.1.216.12**

В.В. ЖИРНОВ, канд. техн. наук, С.В. СОЛОНСЬКА, канд. техн. наук

МЕТОДИ ЛОГІЧНОЇ ОБРОБКИ ЗОБРАЖЕНЬ ВІДМІТОК РАДІОЛОКАЦІЙНИХ ОБ'ЄКТІВ НА ОСНОВІ СЕМАНТИЧНИХ ОЗНАК

Вступ

Наводяться результати обґрунтування та розробки методів логічної обробки зображень відміток радіолокаційних об'єктів на основі семантичних ознак, дослідження можливостей створення алгоритмів та програм автоматичного виявлення радіолокаційних позначок повітряних об'єктів та їх розпізнавання в оглядових РЛС з обробкою реальних записів сигналів. Актуальність цих робіт – створення універсальних алгоритмів автоматичної обробки інформації для забезпечення ефективного виявлення та розпізнавання корисних сигналів на основі семантичних ознак. Складність класичних радіолокаційних систем [1, 2] полягає в недостатній автоматизації процесів обробки даних, у тому числі в системах виявлення та радіолокаційного розпізнавання відміток повітряних об'єктів щодо аналізу їх зображень. У нашому випадку необхідно наблизити процедуру обробки зображень об'єктів радіолокації до логіки експерта, для якої характерно послідовне залучення до аналізу ситуації розрізнювальних ознак між відображеннями від різних об'єктів. Завдання виявлення та розпізнавання сигнальних образів об'єктів радіолокації в даному випадку трансформується в завдання ознакової класифікації (розпізнавання).

В сучасній техніці обробки сигналів та інформації недостатньо ефективно використовуються можливості експерта – оператора РЛС, який на основі даних про радіолокаційну обстановку: координати, форма, яскравість корисних і завадових відміток та багатооглядова передісторія, може ефективно отримувати та передавати радіолокаційну інформацію (РЛІ) споживачеві. Основною перевагою інтелектуальних моделей є аналіз просторово-часової картини, що відображається на екрані індикатора, виявлення відміток, фільтрування геометричних образів трас літальних апаратів і завадового фону [3 – 4]. Це дозволяє регулювати неявні пороги візуального виявлення, відкладати та змінювати недостовірні рішення та оцінки, приймати рішення щодо накопиченого траєкторного сигналу ЛА, надавати ознаки. Основою є розробка алгоритмів формування образів радіолокаційних сигналів для інтелектуальної системи виявлення відміток рухомих об'єктів та автоматизації операцій обробки інформації, що підвищують ефективність виявлення слабких сигналів завдяки накопиченню сигнальної (енергетичної) та логічної інформації. При цьому логічна інформація накопичується з аналізу динамічної карти інтенсивностей радіолокаційних сигналів з відстеженням змін, що відбуваються в ній, протягом багатьох зондувань РЛС.

Методи обробки та розпізнавання радіолокаційних сигнальних образів [5] застосовуються в багатьох областях – у військовій справі, в авіації, у наземному та надводному транспорті. Базовим поняттям цих методів є подоба об'єктів і, навіть, кількісна міра подоби.

Розпізнавання зображень є окремим випадком розпізнавання образів. Це перетворення інформації, що міститься у зображеннях, з метою виділення найважливіших з погляду того чи іншого конкретного завдання даних. Існують методи логічного розпізнавання [5], у яких обробка інформації виконується згідно з чітко визначеним алгоритмом з метою виділення цінної інформації, та методи інтуїтивного розпізнавання, коли відбувається генерація цінної інформації.

Основна складність в існуючих системах полягає у недостатній автоматизації процесів обробки даних, в тому числі в системах виявлення та розпізнавання сигналів об'єктів та процесів за розрізняючими ознаками сигналів та сигнальних образів (просторового та спектрального зображень). Вирішення цієї проблеми стає важливим у випадках, коли об'єкти та відносини предметної області пов'язані складними логічними залежностями, що, у свою чергу, вимагає побудови математичних моделей, завдяки яким можливий ефективний логічний висновок, що відповідає вимогам користувача.

Семантична складова зображення радіолокаційного об'єкта – це семантичний елемент, що містить смислову складову, і може виступати як одна з його характеристик. В інформаційних радіолокаційних системах, що оперують семантичними кодами, семантична складова може виражатися окремим символом – семантичним множником або ознакою.

Постановка завдань дослідження. Існує суперечність у практиці: низька автоматизація процесів обробки даних, зокрема, у системах виявлення та розпізнавання сигналів об'єктів та процесів за розрізняючими ознаками сигналів та сигнальних образів. У той самий час немає ефективних технологій для вирішення завдань, коли об'єкт та його відображення (відносини, зображення) в сигнальній області пов'язані складними логічними залежностями. Застосування алгебри предикатів під час формування та опису сигнального образу дає можливість визначати семантичні складові його поведінки та на їх основі розробляти системи автоматичного виявлення та розпізнавання радіолокаційних об'єктів в реальному часі.

Метод логічної обробки зображень відміток радіолокаційних об’єктів

Аналіз методів виявлення та розпізнавання показав, що для систем автоматичної обробки радіолокаційної інформації доцільно використовувати методи логічного виявлення та розпізнавання [1, 2, 5], в яких обробка інформації виконується за визначеним алгоритмом з метою виділення цінної інформації, та методи інтуїтивного розпізнавання, коли відбувається генерація цінної інформації. Основна складність у методах логічного розпізнавання образів полягає у низькій автоматизації процесів обробки даних, у тому числі в системах виявлення та розпізнавання сигналів об'єктів та процесів за розрізняючими ознаками сигналів та сигнальних образів (просторового та спектрального зображень).

Результати аналізу процесу формування та аналізу сигнальних образів для інтелектуальних систем виявлення та розпізнавання об'єктів показали доцільність класифікації всієї сукупності зображень відміток [6 – 8]. Такий підхід дозволяє створювати алгоритми автоматичної обробки інформації та підвищувати ефективність виявлення та розпізнавання корисних сигналів за рахунок накопичення сигнальної (енергетичної) та логічної інформації в аналізованому елементі дозволу та в його осередку. Для цього пропонується метод представлення інтелектуального образу радіолокаційних відміток, який дозволяє формалізувати та спостерігати динаміку формування семантичної ознаки протягом кількох зондувань РЛС. Далі було згенеровано узагальнену семантичну ознаку, яка характеризує поведінку сигнальної відмітки протягом декількох зондувань РЛС, як певний образ, подібний до образу, яким користується оператор при ототожненні сигнальних відміток.

Розроблено метод прийняття рішення про виявлення та розпізнавання радіолокаційних об'єктів на основі аналізу матриці простору ознак (рис. 2). Перевага даного методу пов'язана з використанням додаткової інформації, отриманої під час створення та аналізу інтелектуального зображення радіолокаційної відмітки (рис. 3). Запропонований підхід включає багаторівневі процедури для формалізації та автоматичної генерації символьних зображень точкового об'єкту, такого як літак, вертоліт, БПЛА. Модель включає систему предикатних рівнянь, в результаті розв'язання цих рівнянь визначається вид і значення предикатних ознак, а також перелік процедурних і семантичних операцій обробки.

Суть метода логічної обробки радіолокаційних образів при автоматичному виявленні й розпізнаванні об’єктів на основі семантичних ознак – це формування вектору прийняття рішення про виявлення та розпізнавання зображень радіолокаційних відміток шляхом логічної обробки простору векторів семантичних ознак $W\left(I_g, I_s, I_f \right)$, який задано на множині

семантичних ознак зображень $\{I_1, I_2,...,I_k\}$ з урахуванням геометричної $\{I_{g1}, I_{g2},...,I_{gk}\}$, смислової $\{I_{s1}, I_{s2},...,I_{sk}\}$ складових зображень та семантичної ознаки їх флуктуацій $\{I_{f1}, I_{f2},...,I_{fk}\}$.

На рис. 1 наведено алгоритмічну схему автоматичного прийняття рішення про виявлення та розпізнавання радіолокаційних зображень літальних апаратів. Ухвалення рішень у вигляді вектор $O_k = W(I_s, I_g, I_f, I_e)$ про виявлення та ідентифікацію *k* літальних апаратів здійснюється шляхом обробки предикатної операції $W\{I_s, I_g, I_f, I_e\}$, яка задана на множині предикатних ознак відміток $\{I_s, I_g, I_f, I_e\}$ на основі смислової $\{I_{s1}, I_{s2},...,I_{sk}\}$, геометричної $\{I_{g1}, I_{g2},...,I_{gk}\}$, енергетичної $\{I_{e1}, I_{e2},...,I_{ek}\}$ складових символьних зображень та ознаки їх флуктуацій $\{I_{f1}, I_{f2},...,I_{fk}\}$.

З аналізу семантичних ознак смислової I_s, геометричної I_g, енергетичної I_e та ознаки флуктуації I_f інтелектуальної моделі сигнальних відміток, здійснюється процедура виявлення та розпізнавання радіолокаційних об'єктів, у тому числі точкових рухомих і малорухомих літальних апаратів: літак, вертоліт, БПЛА.

Метод логічної обробки зображень радіолокаційних об'єктів на основі семантичних ознак

Проведемо обґрунтування запропонованого методу обробки. Позначимо через *X* множину об'єктів радіолокації. Семантична ознака – це деяка характеристика об'єкта, відображення $I: X - D_I$, де D_I – множина допустимих значень ознаки. Якщо задано ознаки $I_1, I_2,...,I_n$, тоді вектор $x = (I_1(x), I_2(x),..., I_n(x))$ назвемо ознаковим описом об'єкту.

Рис. 1. Схема прийняття рішення

На основі системи первинних семантичних ознак [6]: предикат Z_{pij} наявності сигналу в a_{ij} інформаційному осередку (i, j – номери елементів зони огляду РЛС); предикати сусіднього осередку Z_{dij} та Z_{aij} переходу сигналу з поточного осередку a_{ij} до суміжного осередку за дальністю або азимутом, сформовано складники інтелектуальної моделі зображень сигналів для точкових рухомих та малорухомих літальних апаратів:

- первинні семантичні ознаки Z_{pij}, Z_{dij}, Z_{aij}, що дозволяють створити опис об'єкту радіолокації на підставі семантичних зв'язків і відносин

$$x_1=\left\{I_1\left(Z_{pij},Z_{dij},Z_{aij}\right),I_2\left(Z_{pij},Z_{dij},Z_{aij}\right),\ldots,In\left(Z_{pij},Z_{dij},Z_{aij}\right)\right\}$$

між подіями в інформаційних осередках під час формування віртуального просторово – семантичного зображення радіолокаційних відміток;

- семантичні ознаки радіолокаційних зображень $X=(I_1(x_1),\ldots,I_n(x_1)),\ldots,(I_1(x_k),\ldots,I_n(x_k))$ для k об'єктів на основі аналізу первинних семантичних ознак;

- матриця семантичних ознак об'єктів радіолокації, розміру $k\times n$, $\left\{I_S(X),I_g(X),I_e(X),I_f(X)\right\}$, що створена з урахуванням смислової $\left\{I_{s1}(x_1),I_{s2}(x_2),\ldots,I_{sk}(x_k)\right\}$, геометричної $\left\{I_{g1}(x_1),I_{g2}(x_2),\ldots,I_{gk}(x_k)\right\}$, енергетичної $\left\{I_{e1}(x_1),I_{e2}(x_2),\ldots,I_{ek}(x_k)\right\}$ складових інтелектуальних зображень і ознаки флуктуації $\left\{I_{f1}(x_1),I_{f2}(x_2),\ldots,I_{fk}(x_k)\right\}$. Стовпці цієї матриці відповідають ознакам, а кожен рядок є ознаковим описанням одного об'єкту радіолокації. На рис. 2 наведено зразок матриці.

$I_{s1}(x_1)$	$I_{g1}(x_1)$	$I_{e1}(x_1)$	$I_{f1}(x_1)$
$I_{s2}(x_2)$	$I_{g2}(x_2)$	$I_{e2}(x_2)$	$I_{f2}(x_2)$
…	…	…	…
$I_{sk}(x_k)$	$I_{gk}(x_k)$	$I_{ek}(x_k)$	$I_{fk}(x_k)$

Рис. 2. Матриця семантичних ознак об'єктів радіолокації

Метод логічної обробки зображень для автоматичного виявлення й розпізнавання радіолокаційних об’єктів

Проведено дослідження для розроблення методу логічної обробки зображень відміток для оглядових РЛС. У ході дослідження:

1. Сформовано символьні зображення огинаючої пачки імпульсів РЛ відміток літальних апаратів. Це – n мірний вектор загальної матриці зони огляду РЛС. При цьому у кожній пачці сигналу може змінюватися частота Допплера і величина сигналу для заданої дальності. За допомогою таких операцій змодельовано різні радіолокаційні ситуації: політ одного літального апарату по всіх елементах дальності на тлі завади, політ літаків із різними швидкостями, що знаходяться на різній дальності. Відповідно до моделей реальних сигналів обрано три типи характерних радіолокаційних зображень сигналів та їх символьні зображення, які наведено на рис. 3, 4. З цих типів реальних зображень обрано еталонні типи пачок радіолокаційних сигналів цілей і завад та їх символьні зображення S_j. Кожному типу зображення відповідає певна комбінація геометричних та семантичних (предикатних) ознак, що визначаються із систем предикатних рівнянь.

2. Розроблено метод логічної обробки зображень радіолокаційних об’єктів на основі семантичних ознак. Для ідентифікації радіолокаційних зображень сформовано простір ознак

для множини радіолокаційних об’єктів з урахуванням допустимих значень признака D_I у вигляді матриці ознакових описів зображень об'єктів радіолокації. Матрицю створено на множині ознак $\left\{ D_s(X), D_g(X), D_e(X), D_f(X) \right\}$ на основі смислової $\left\{ D_{s1}(x_1), D_{s2}(x_2), ..., D_{sk}(x_k) \right\}$, геометричної $\left\{ D_{g1}(x_1), D_{g2}(x_2), ..., D_{gk}(x_k) \right\}$, енергетичної $\left\{ D_{e1}(x_1), D_{e2}(x_2), ..., D_{ek}(x_k) \right\}$ складових інтелектуальної моделі зображень і семантичної ознаки флуктуації $\left\{ D_{f1}(x_1), D_{f2}(x_2), ..., D_{fk}(x_k) \right\}$

Розроблено алгоритм ідентифікації типів S_j інтелектуальних зображень, що описується системою предикатних рівнянь, складеної виходячи з того, що кожному символьному типу S_j зображень (рис. 4) відповідає певна комбінація геометричних та семантичних (предикатних) ознак, що визначаються системами предикатних рівнянь. Наприклад, для типів зображень S_1 точкових рухомих і малорухомих літальних апаратів: літак, вертоліт, БПЛА використовується система предикатних рівнянь, у результаті яких визначаються семантичні ознаки зображення відмітки. На рис. 3, 4 показано типи характерних зображень радіолокаційних сигналів та їх інтелектуальна модель.

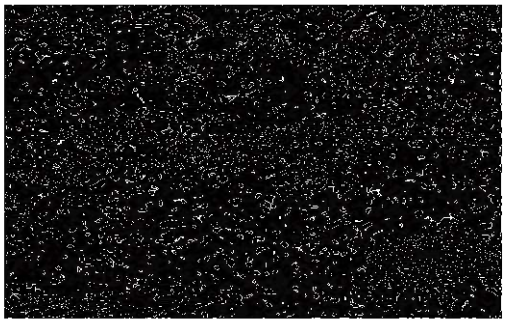


Рис. 3. Реальні РЛ зображення

Рис. 4. Інтелектуальна модель РЛ зображення

На підставі зазначених вище закономірностей було сформовано простір ознак для обраних типів об'єктів радіолокації з урахуванням допустимих значень ознаки, що дозволяють відрізняти зображення відміток об'єктів радіолокації.

Кожна складова інтелектуальної моделі зображень може мати свій підпростір ознак залежно від типу або класу об'єкта радіолокації. Наприклад, якщо об'єкт точковий і рухається, то формується модель у вигляді протяжної по азимуту відмітки з розривами за рахунок допплерівських флуктуацій амплітуди. Якщо ж об'єкт протяжний, наприклад хмари, дощові хмари, зграї птахів, локальні повітряні неоднорідності ангел-луна, то з прийнятих сигналів формується модель цього об'єкту як сукупність зображень окремих блискучих точок. Тоді отримаємо матрицю розміру $k \times n$ (k рядків, n стовпців). Стовпці цієї матриці відповідають ознакам зображень відміток, а кожен рядок є ознаковим описанням зображення відмітки об'єкта радіолокації. Тут l – розмір підпростір ознак залежно від типу або класу об'єкта радіолокації і може мати значення 1…l. На рис. 5 наведено зразок матриці.

$D^l_{s1}(x_1)$	$D^l_{g1}(x_1)$	$D^l_{e1}(x_1)$	$D^l_{f1}(x_1)$
$D^l_{s2}(x_2)$	$D^l_{g2}(x_2)$	$D^l_{e2}(x_2)$	$D^l_{f2}(x_2)$
…	…	…	…
$D^l_{sk}(x_k)$	$D^l_{gk}(x_k)$	$D^l_{ek}(x_k)$	$D^l_{fk}(x_k)$

Рис. 5. Матриця ознак інтелектуальної моделі зображень об'єктів радіолокації

Висновки

Результати аналізу процесу формування та аналізу сигнальних образів радіолокаційної інформації для інтелектуальних систем виявлення та розпізнавання об'єктів показали доцільність класифікації всієї сукупності зображень. Для цього пропонується інтелектуальна модель радіолокаційних відміток, яка дозволяє формалізувати та спостерігати динаміку формування семантичної ознаки протягом кількох зондувань РЛС. Надалі, аналізуючи цю картину, було сформовано узагальнену семантичну ознаку, яка характеризує поведінку сигнальної відмітки протягом ряду зондувань РЛС, як певний образ, подібний до образу, яким користується оператор при ототожненні сигнальних відміток. Цей образ, як правило, враховує розмір, форму, характер зміни розміру та форми сигнальної відмітки. Розроблено метод прийняття рішення про виявлення та розпізнавання радіолокаційних об'єктів на основі аналізу матриці простору ознак. Пропонована інтелектуальна модель включає багаторівневі процедури для формалізації та автоматичного конструювання символьних зображень точкового об'єкта, що рухається, такого як літак, вертоліт, БПЛА. Модель включає систему предикатних рівнянь, в результаті розв'язання цих рівнянь визначається вид і значення предикатних ознак інтелектуальної моделі, а також перелік процедурних і семантичних операцій обробки.

Список литературы:

1. Li Jian Radar Signal Processing and Its Applications / Jian Li, R. Hummel, P. Stoica, E. G. Zelnio. Springer, 2013. 279 p.
2. Skolnik M. I. (eds) (2021) Radar Handbook, McGraw-Hill, New York.
3. Russel S. Artificial intelligence. A modern approach, Second Edition / S. Russel, P. Norvig. Williams, 2006. 1410 p.
4. Бондаренко М. Ф. Теория интеллекта : учебник / М. Ф. Бондаренко, Ю. П. Шабанов-Кушнаренко. Харьков : СМИТ, 2007. 576 с.
5. Журавлев Ю. И. Об алгебраическом подходе к решению задач распознавания или классификации // Проблемы кибернетики. 2005. Вып. 33. С. 5–68.
6. Volodymyr Zhyrnov, Svitlana Solonska “Symbolic model of radar images when detecting aircraft”// Telecommunications and Radio Engineering. 2022. Vol. 81, Is. 2. P. 25–35.
7. Жирнов В.В., Солонская С.В. Предикатная модель процессных знаний при обнаружении и распознавании пачечной структуры сигналов от летательных аппаратов в обзорных РЛС // Радиотехника. 2020. Вып. 201. С 137–144.
8. Jianping Ou, Jun Zhang, and Ronghui Zhan. Processing Technology Based on Radar Signal Design and Classification // International Journal of Aerospace Engineering. Vol. 2020, pp. 1–19. Article ID 4673763. https://doi.org/10.1155/2020/4673763.
9. Солонская С.В., Жирнов В.В. Предикатная модель процессных знаний при обнаружении и распознавании протяженных объектов типа облака, тучи, «ангел-эхо» в обзорных РЛС // Радиотехника. 2020. Вып. 202. С 164–172.
10. Zhirnov V.V., Solonskaya S.V. Intelligent system for detection of low-visible air objects in surveillance radars // Telecommunications and Radio Engineering. 2020. Vol. 79, Is. 17. P. 1513–1519. DOI: 10.1615/TelecomRadEng.v79.i17.20.
11. Advanced Methods and Deep Learning in Computer Vision.1st Edition / Editors: E. R. Davies, Matthew Turk. Academic Press. 2021. Page Count: 586. ISBN: 9780128221099.

Надійшла до редколегії 21.01.2024

Відомості про авторів:

Жирнов Володимир Віталійович – канд. техн. наук, Харківський національний університет радіоелектроніки, п.н.с. НДЦ інтегрованих радіоелектронних систем і технологій, Україна; e-mail: nauka123@ukr.net; ORCID: http://orcid.org/0000-0002-2397-3126

Солонська Світлана Володимирівна – канд. техн. наук, НТУ "Харківський політехнічний інститут", Україна; e-mail: solonskaya@ukr.net, ORCID: https://orcid.org/0000-0002-8841-7825

УДК 621.396.4 **DOI:10.30837/rt.2024.1.216.13**

В.А. БУЛАГА

ДОСЛІДЖЕННЯ КУТОВОГО РОЗПОДІЛУ ПОМИЛОК ПРИ РІЗНИХ ШВИДКОСТЯХ ПЕРЕДАЧІ В ДЕКАМЕТРОВОМУ ДІАПАЗОНІ

Вступ

Відомо, що основними факторами, що спричиняють зменшення пропускної спроможності й надійності каналів зв'язку в декаметровому діапазоні є багатопроменевість і рівень завад від передавачів, що працюють за близькими частотами [1 – 4]. Один із способів боротьби з такими негативними явищами – це застосування в системах зв'язку фазованих антенних решіток (ФАР), які забезпечують поділ променів при прийомі. Водночас реалізація таких складних антенних систем як ФАР супроводжується значними економічними витратами, так як вони є високовартісними. В результаті виникає завдання в оцінці ефективності такої антенної системи за інформаційним критерієм "коефіцієнти помилок – кут місця". Представлені у літературі дослідження повною мірою не розкривають задачу, що розглядається. В [5] розглянуто проблеми формування та обробки радіолокаційної інформації в системах радіобачення авіаційно-наземного базування зі змінною відносною просторовою конфігурацією при дистанційному зондуванні радіопомітних об'єктів та об'єктів спостереження з радіопоглинаючою поверхнею. В [6, 7] проводиться аналіз методів визначення напрямку приходу сигналів в задачах просторово-часового доступу на основі методів радіопеленгації в системах мобільного зв'язку, наведено процедуру оцінки вектора розподілу поля, значення якого може бути обчислено спільно з оцінкою вектора вагових коефіцієнтів адаптивної антенної решітки. В [8] зроблено аналіз розвитку технології міліметрових і субміліметрових хвиль. В роботі [9] розглянуто метод оцінювання завадозахищеності радіообміну в мережах зв'язку в умовах реальних завад, який використовує імітаційне моделювання із визначенням коефіцієнтів подавлення радіозасобів залежно від просторового розташування постановників завад і орієнтації спрямованих антен засобів захисту своїх радіозасобів. В роботі [10] аналізуються методи визначення напрямку приходу сигналів в задачах просторово-часового доступу на основі методів радіопеленгації.

Мета роботи – дослідження кутового розподілу помилок при різних швидкостях передачі в короткохвильовому діапазоні при використанні фазованих антенних решіток за інформаційним критерієм "коефіцієнти помилок – кут місця".

Аналіз кутового розподілу рівнів випадкових радіозавад

Для дослідження використовувалися експериментальні дані кутомісних розподілів числа помилок, які були отримані на радіотрасі ідеального напрямку протяжністю 600 км. Структурна схема вимірювання кутового розподілу рівнів випадкових радіозавад (рис. 1) містить: 1 – атенюатор; 2 – приймач Р-250-2М; 3 – детектор огинаючої ; 4 – пристрій запису інформації; 5 – комутатор; 6 – АЦП (аналоговий цифровий перетворювач); 7 – ПК (персональний комп'ютер).

У передавальному пункті використовувався передавач "В'яз-М2", який працює на антену ВГДШ (вібратор горизонтальний діапазонний шунтовий). Короткохвильовий передавач В'яз-М2 призначений для роботи на радіотелефонних лініях зв'язку. Управління передавачем здійснювалося частотно-маніпульованими сигналами, які передавалися на вхід підсилювача низької частоти з швидкостями 50, 200, 600 і 1200 Бод від приладу ВО-2.

Для правильної оцінки коефіцієнта помилок під певними кутами фазування прийом відбувався одночасно на дві антени А1 і А2 з різними діаграмами направленості. В якості антени А1 використовувалося шість секцій ФАР (плече північ-південь) радіотелескопа УТР-2, А2 – одна секція.

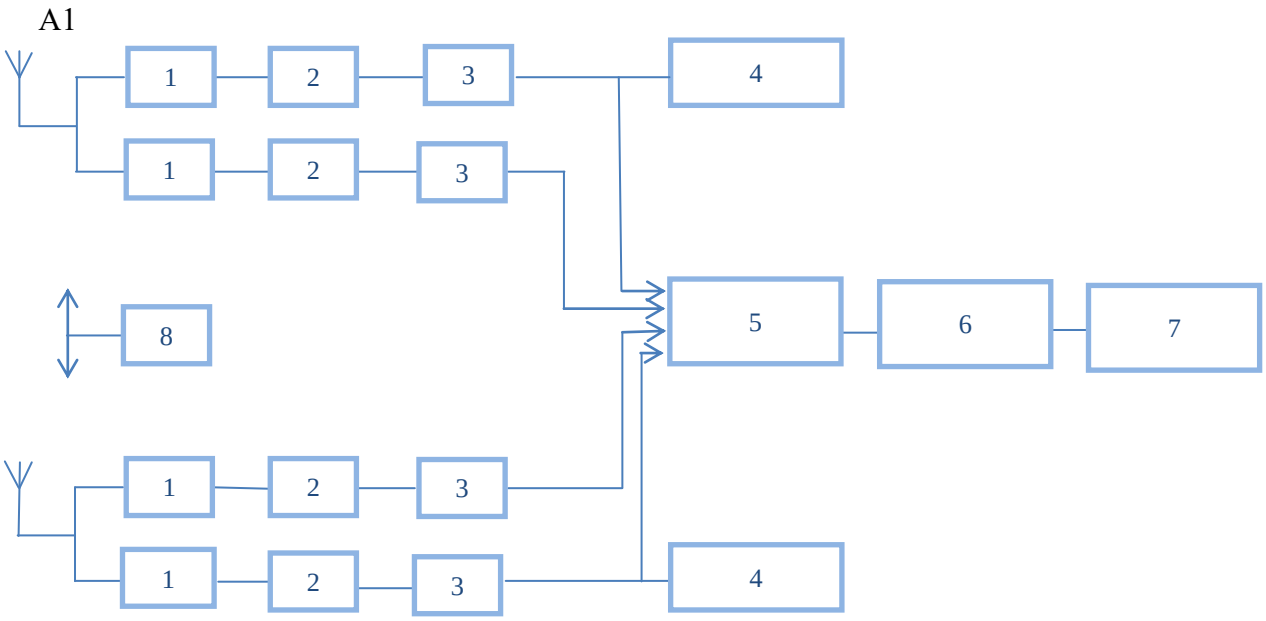
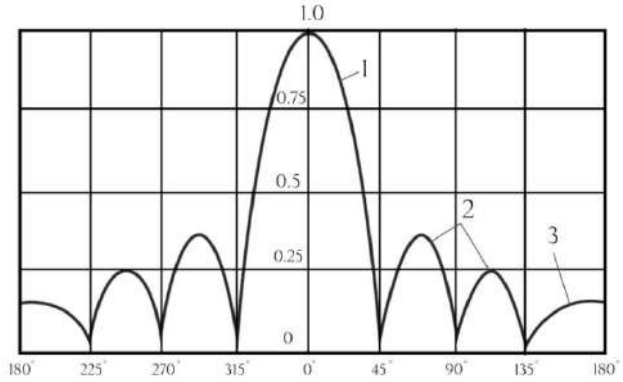


Рис. 1. Структурна схема вимірювання кутового розподілу рівнів випадкових радіозавад

Вибір антен такого виду був зумовлений наступними міркуваннями. Відомо, що порівняно невелика зміна висоти відображення, що діє, на трасі може призводити до помітних флуктацій кутів виходу і приходу. В результаті у пункті прийому буде спостерігатися сектор кутів, в межах якого щільність потоку енергії прийнятого поля співмірна в напрямку середнього кута. Як показують дослідження, ширина сектору кутів приходу може становити одиниці або десятки градусів. У першому випадку спостерігається відбиття близьке до дзеркального, у другому – дзеркально розсіяне. Співвідношення між дзеркальним і розсіяним компонентами визначає статистичну структуру сигналу, від якої залежить завадозахищеність каналу. Тому для об'єктивної оцінки завадозахищеності каналу зв'язку і пояснення механізму розподілу радіохвиль необхідно проводити синхронні виміри на дві антени, одна з яких мала ширину діаграми одиниці градусів, а інша – десятки градусів. Залежність ширини діаграми для антени А1 та А2 на рівні 0,707 (рис. 2).



1 – основна пелюстка, 2 – бічна пелюстка, 3 – задня пелюстка.

Рис. 2. Залежність ширини діаграми для антени А1 та А2 на рівні 0,707

Крок по кутку місця було обрано п'ять градусів. Такий крок забезпечує взаємне перекриття діаграми направленості під різними кутами фазування. При цьому можлива величина зміни рівня сигналу через рівноймовірне коливання кутів приходу щодо максимуму діаграми під певними кутами спостереження не перевищує 3 – 6 дБ, що відповідає допустимим змінам рівня приладу ВО-2, при якому помилки ще не фіксуються. Перед початком кожного сеансу

спостереження необхідно проводити калібрування вимірювального комплексу сигналами з виходу генератора Г4-18А на частоті випромінювання передавального пункту. Модуляція генератора Г4-18А здійснюється частотно-маніпульованими посилками від приладу ВО-2. Метою калібрування є вирівнювання підсилення трактів антен А1, А2 і виставлення такого підсилення за проміжною частотою приймача Р-250-2М, коли рівень сигналу на виході приладу ВО-2 відповідає номінальному.

При проведенні сеансу спостереження, окрім вимірювання коефіцієнта помилок, паралельно проводився запис огинаючої сигналу, що приймається. З цією метою сигнал з виходу підсилювача проміжної частоти приймача Р-250-2М подавався на детектор огинаючої. При цьому постійна часу детектора обирається рівною одній секунді. Така постійна часу дозволяє не враховувати вплив виду модуляцій та, в той же час, реєструвати зміну огинаючого сигналу під впливом як швидких, так і повільних замирань. За реалізаціями тривалістю близько двох хвилин (інтервал стаціонарності огинаючої) для двох антен та певних кутів фазування обчислювалися математичне очікування, дисперсія, середнє квадратичне відхилення, коефіцієнт кореляції. В якості приклада на рис. 3 представлено зміни середнього значення сигналу по відношенню до рівня сигналу при калібруванні коефіцієнта помилки в залежності від кута фазування для одного з сеансів спостереження (кружечки – значення $\overline{x}_{\partial Б}\left(\Theta^{\circ}\right)$ і $K_{пом}\left(\Theta^{\circ}\right)$ відповідають одній секції ФАР; трикутники – шести секціям).

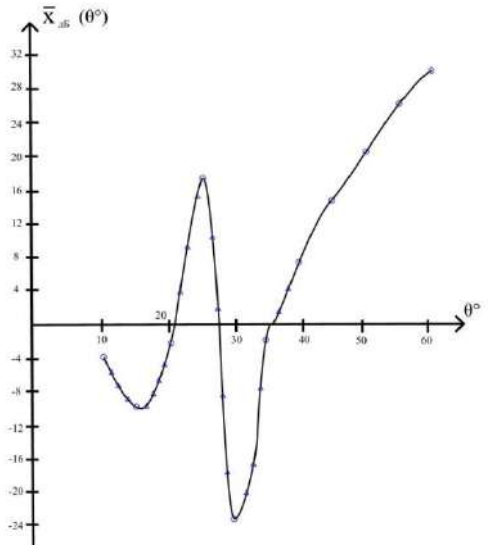


Рис. 3 Мінливість відносного середнього рівня сигналу та коефіцієнта помилок від кута місця

Рис. 3 ілюструє ступінь мінливості відносного середнього рівня сигналу та коефіцієнта помилок від кута місця. При цьому хоч і спостерігається взаємозв'язок між зміною $\overline{x}_{\partial Б}\left(\Theta^{\circ}\right)$ і $K_{пом}\left(\Theta^{\circ}\right)$, в той же час є невідповідність. Так, більш вищому середньому рівню сигналу, прийнятого антеною А2, відповідає високе значення коефіцієнта помилок. Цей факт пояснюється тим, що хоч через слабку спрямованість антени А2 рівень сигналу великий, але через багатопроменеве поширення якість зв'язку падає. Отже, представлені графіки підтверджують відомий висновок про те, що рівень радіосигналу не може бути критерієм якості зв'язку. З цих же графіків випливає, що за рахунок просторової селекції строго спрямована антена А2, навіть в умовах прийому розсіяних компонент поля, дозволяє значно підвищити надійність зв'язку.

Так, під кутом фазування 25 і 30 градусів коефіцієнт помилки дорівнює нулю для антени А1, а для антени А2 – відповідно 10^{-2} і 10^{-3} при приблизно однакових середніх рівнях. Очевидно такі кути приходу для дальності 600 км відповідають відбиттю від області Е.

В результаті відношення робочої частоти до максимально застосованої частоти в області E (МЗЧЕ) виявилося близьким до одиниці ($f_р/f_{МЗЧЕ}$=0,97), а при такому значенні відношення, як відомо, поле в пункті прийому має в основному розсіяну структуру. Кут приходу 50 градусів, при якому коефіцієнт помилки як для антени А1 так і А2 виявляється рівним нулю, відповідає відбиттю від області F. У цьому випадку відношення робочої частоти до МЗЧF склало $f_р/f_{МЗЧF}$=0,85, і в пункті прийому переважає дзеркально відбита складова одного променя.

На рис. 4 наведено кореляційні функції огинаючої сигналів двох типів антен (трикутника ФАР із шести секцій, коло – одної секції) різних кутів фазування і того ж вибіркового сеансу спостереження. Шаг Δt=12 с. Як видно з рис. 4, для більшості кутів фазування кореляційна функція спадаюча і є осцилюючою. При цьому ступінь осциляції виявляється різним, а при кутах фазування 30 і 50 градусів вони мінімальні або практично відсутні. Найбільш яскраво коливальний характер кореляційної функції проявляється (незалежно від типу антен) під кутами приходу, що не є оптимальними для даної дифузної багатопроменевості.

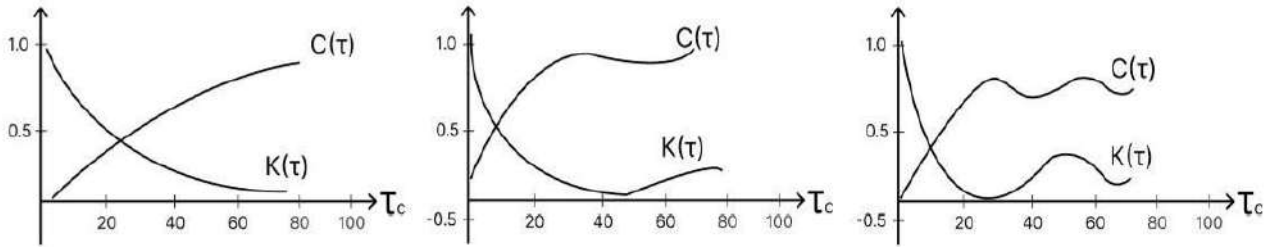


Рис. 4. Усереднені структурні та кореляційні функції

При кутах фазування 30 і 50 градусів коефіцієнт кореляції максимальний і досягає значень 0,65 і 0,85 відповідно; під іншими кутами фазування коефіцієнт кореляції має значення від 0,1 і 0,3. На підставі цього в першому випадку можна стверджувати, що сигнали мають однакову структуру і є залежними, у другому – різну і будуть незалежними. Цей результат є незалежним аргументом на користь оцінки ефективності ФАР за критерієм «коефіцієнт помилки – кут місця», а не за амплітудними значеннями прийнятого сигналу.

Оскільки значення коефіцієнта помилок від кута місця, виміряні в окремі дні, через нерегулярні зміни параметрів іоносфери виявляються нехарактерними. В результаті всього вище сказаного можна стверджувати наступне:

- коефіцієнт помилок має явну залежність від кута фазування. Для ненаправленої антени (поодинокий вібратор) коефіцієнт помилок залишається практично постійним і рівень помилок досить значний;

- фазована антенна решітка з шести секцій за інших рівних умов має коефіцієнт помилок менше, ніж одна секція. Виняток становлять лише ті кути фазування, які є оптимальними для даної траси за умовами поширення. Цей результат пояснюється в першу чергу вищими вибірковими здібностями ФАР з шести секцій або числом променів, що потрапляють у діаграму спрямованості, так як характер багатопроменевості в першу чергу впливає на величину коефіцієнта помилок;

- слабку відмінність у величині коефіцієнта помилок під різними кутами фазування та різних швидкостях передачі можна пояснити наявністю у складі вимірювального комплексу модемів і видом модуляції (АМ з двома бічними смугами);

- кути приходу 30 і 50 градусів є оптимальними за мінімальним коефіцієнтом помилок, залишаючись постійними для даного дня спостереження з 15.00 до 20.00. Такий результат здається дещо несподіваним, тому що добре відомо, що на такому інтервалі, а тим більше в перехідні години доби, коли іоносферні умови змінюються суттєво, і як наслідок, разом з діючими висотами відображення змінюються кути випромінювання та кути приходу. Очевидно, така стійкість кутів приходу 30 і 50 градусів пояснюється високою просторовою

вибірковістю ФАР із шести секцій, яка навіть у важких умовах (розсіяне поле, великий рівень загасання) дозволяє вести прийом з високою надійністю.

Висновки

Отримані результати дозволяють зробити наступні висновки:

- проведені дослідження повною мірою підтверджують можливість використання приладів виявлення похибок при випробуванні надійності каналів зв'язку декаметрового діапазону;

- застосування керованих фазованих антенних решіток на приймальній стороні дозволяє вирішувати комплекс траєкторних завдань, а також дати оцінку ефективності систем зв'язку, що використовують на прийомі розподіл променів.

Список літератури:

1. Лінії радіозв’язку та антенні пристрої : навч. посіб. / М.Д. Ільїнов, Т.Г. Гурський, І.В. Борисов, К.М. Гриценок. Київ : ВІТІ, 2018. 250 с.
2. Бондаренко І.М. Системи радіозв’язку. Кн.2, ч.1. Радіолінії зв’язку : навч. посіб. Харків : ХІ ВПС, 2003. 162 с.
3. Васильєв В. М. Радіонавігаційні системи : підручник. Київ : Політехніка, 2023. 338 с.
4. Огороднійчук М. Д., Чайка Ю. Д., Оксіюк О. Г. Комплекси і засоби військових телекомунікаційних мереж : навч. посіб. ; за ред. проф. М. Д. Огороднійчука. Київ : НУОУ, 2010. 384 с.
5. 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. Київ : Логос, 2014. 230 с.
6. Alsaleem N., Moskalets M. and Teplytska S. The analysis of methods for determining direction of arrival of signals in problems of space-time access // Eastern-European Journal of Enterprise Technologies, 2016. Vol. 4, no. 982, p. 36. doi:10.15587/1729-4061.2016.75716.
7. Lima A. G. M. and Menezes L. R. A. X. Smart Antennas as an Approach to Instantaneous Air Interface with Software-Defined Radios // IEEE Antennas and Propagation Magazine. 2007. Vol. 49, no. 3, pp. 198–208. doi: 10.1109/MAP.2007.4293975.
8. Wiltse J. C. History of Millimeter and Submillimeter Waves // IEEE Transactions on Microwave Theory and Techniques. 1984. Vol. 32, no. 9, pp. 1118–1127. doi: 10.1109/TMTT.1984.1132823.
9. Іохов О. Ю. Метод оцінювання завадозахищеності радіообміну в мережах зв'язку угрупувань військ (сил) // Системи озброєння і військова техніка. 2017. № 4. С. 11–16.
10. Alsaleem N. Y., Moskalets M., and Teplytska S. The analysis of methods for determining direction of arrival of signals in problems of space-time access // Eastern-European Journal of Enterprise Technologies. 2016. Vol. 4, no. 9(82), p. 36. doi:10.15587/1729-4061.2016.75716.

Надійшла до редколегії 20.02.2024

Відомості про автора:

Булага Вікторія Анатоліївна – Харківський національний університет радіоелектроніки, асистент кафедри комп’ютерної радіоінженерії та систем технічного захисту інформації,; Україна; e-mail: viktoriia.bulaga@nure.ua; ORCID: https://orcid.org/0000-0001-9655-6684

УДК 621.396.96 **DOI:10.30837/rt.2024.1.216.14**

І.В. СВИД, канд. техн. наук, І.В. ІГНАТЮК, О.Д. ШУНІБОРОВ,
Г.В. МАЙСТРЕНКО, М.В. ТУЛЕНКО

ОЦІНКА ЯКОСТІ РАДІОЛОКАЦІЙНОЇ ІНФОРМАЦІЇ СИСТЕМ ЗАЛЕЖНОГО КООПЕРАТИВНОГО СПОСТЕРЕЖЕННЯ

Вступ

В даний час спостереження та визначення місця розташування повітряного судна в повітряному просторі здійснюються за допомогою первинних [1 – 4] однопозиційних [5 – 7], багатопозиційних [8 – 10] та вторинних [11 – 15] оглядових радіолокаторів, систем ADS тощо. Первинний оглядовий радіолокатор визначає місце розташування повітряного судна на основі прийому відбитих радіолокаційних сигналів. Вторинний радіолокатор використовується для передачі та прийому одержуваних на борту повітряного судна даних, таких як висота, розпізнавальний індекс тощо. Однак є проблеми надскладної установки сучасних первинних та вторинних радіолокаторів в океанічних районах або важкодоступній місцевості, такій як гірські райони, які залежать від можливості установки механічного обладнання, що вимагає виконання великого обсягу робіт з монтажу і технічного обслуговування. Основою служби спостереження повітряного простору може бути сукупність трьох основних видів спостереження [16 – 18]:

– незалежне некооперативне спостереження, в якому місце розташування повітряного судна визначається на основі даних вимірювань без допомоги повітряних суден, що знаходяться на віддаленні;

– незалежне кооперативне спостереження, в якому місце розташування повітряного судна визначається на основі даних вимірювань, що виконуються підсистемою локального спостереження з використанням повідомлень з борту повітряного судна. Ці повідомлення можуть містити інформацію, отриману на борту повітряного судна (наприклад, дані про барометричну висоту, розпізнавальний індекс повітряного судна тощо);

– залежне кооперативне спостереження, у якому місце розташування повітряного судна визначається на борту повітряного судна, і ця інформація передається підсистемі локального спостереження поряд з можливими додатковими даними.

Залежні кооперативні системи спостереження [19 – 21] займають значне місце у інформаційному забезпеченні системи контролю повітряного простору та управління повітряним рухом. Можливо стверджувати, що залежні системи спостереження, що розглядаються, в даний час є перспективними системами спостереження для управління повітряним рухом. У зв'язку з тим, що координати кожного повітряного судна визначаються на борту і, в подальшому, передаються споживачам, тому питання забезпечення цілісності інформації в залежних системах спостереження є актуальним.

Оцінка імовірності цілісності інформації систем залежного кооперативного спостереження

Визначені на борту повітряного судна координати, на основі вимірів глобальної навігаційної супутникової системи, характеризуються високою точністю. Однак відмови, що виникають в системі глобальної навігаційної супутникової системи, можуть призводити до значного збільшення помилок визначення координат повітряного судна, переданих за каналами залежних систем спостереження [22 – 25]. Для користувача системи залежних систем спостереження важливо, щоб була можливість виявляти ситуації, коли помилки визначення координат повітряного судна, переданих в повідомленнях залежних систем спостереження, перевищують заздалегідь встановлений радіус утримання R_s. Будемо вважати, що в цьому випадку подається сигнал тривоги.

Під цілісністю будемо розуміти імовірність події, при якій помилка визначення місцеположення повітряного судна не перевищує деякий поріг R_s або помилка виявлена протягом інтервалу часу, що не перевищує T_a.

Будемо враховувати, що $(\bar{x}, \bar{y})$ – горизонтальні координати фактичного положення повітряного судна, (x_N, y_N) – координати, виміряні залежною системою спостереження повітряного простору. Помилки вимірювання є випадкові величини, що дорівнюють $\xi_N = x_N - \bar{x}$ і $\eta_N = y_N - \bar{y}$.

Якщо функція $f_N(\xi_N, \eta_N)$ є спільною щільністю імовірності помилок (ξ_N, η_N), то імовірність того, що помилки не перевищують R_s, можливо визначити з виразу

$$P = \iint\limits_{\xi_N^2 + \eta_N^2 \le R_S} f_N(\xi_N, \eta_N). \quad (1)$$

Слід зазначити, що вираз (1) не може бути основою забезпечення цілісності вимірювань залежних радіолокаційних систем спостереження, так як для кожного конкретного виміряного положення повітряного судна (x_N, y_N) вона не дозволяє зробити висновок про те, що помилки залежних систем спостереження повітряного простору перевершили величину R_s. Таким чином, на підставі наведеного виразу (1) неможливо реалізувати функцію подачі тривоги.

Для вирішення зазначеної задачі передбачається, що необхідно здійснювати забезпечення цілісності радіолокаційної інформації залежних систем спостереження шляхом порівняння кожного вимірювання координат повітряного судна (x_N, y_N) з координатами (x_R, y_R), які отримані від незалежних систем спостереження повітряного простору.

У подальшому будемо вважати, що незалежний від залежної системи спостереження вимір має помилки $\xi_R = x_R - \bar{x}$ і $\eta_R = y_R - \bar{y}$, а також відома їх спільна щільність розподілу $f_R(\xi_R, \eta_R)$.

Також будемо вважати, що за час спостереження $(0, T_a)$ щільність імовірності помилок координатної інформації незалежної системи спостереження (x_R, y_R) не змінює ні вид розподілу, так і ні параметри розподілу.

З урахуванням справедливості зазначеної вище гіпотези, для забезпечення цілісності координатної інформації залежних систем спостереження повітряного простору пропонується наступний спосіб.

Якщо різниця координат двох незалежних вимірювань одного і того ж положення повітряного судна більше деякої наперед заданої величини D_t, то передбачається, що якість координатної інформації залежної систем спостереження незадовільна, і подається сигнал тривоги (за час, що не перевершує T_a). Це обумовлює, що мітка (x_n, y_n) не повинна використовуватися для цілей управління повітряним рухом. В іншому ж випадку передбачається, що координатна інформація залежної системи спостереження, що розглядається, має достатню якість і може використовуватися для управління повітряним рухом.

Наведене вище підкреслює, що забезпечення цілісності з використанням зазначеного вище алгоритму об'єктивно пов'язане з наступними випадковими подіями [1, 6 – 18]:

- «правильне виявлення» – подія, при якій подається сигнал тривоги для диспетчера, оскільки відстань між незалежними випадковими мітками більше величини D_t і помилки визначення фактичного стану повітряного судна залежною системою спостереження, що розглядається більше $R_s\left(\xi_N^2 + \mu_N^2 < R_s\right)$;

- «правильне невиявлення» – подія, при якій відстань між незалежними випадковими мітками не перевищує величини D_t, сигнал тривоги у цьому разі не подається, а помилки

визначення фактичного стану повітряного судна залежною системою спостереження, що розглядається, не перевищують $R_s\left(\xi_N^2+\mu_N^2<R_s\right)$;

- «хибна тривога» – подія, при якій відстань між незалежними випадковими мітками більше D_t і подається сигнал тривоги для диспетчера, але помилки визначення фактичного стану повітряного судна залежною систем спостереження, що розглядається, не перевищують величину $R_s\left(\xi_N^2+\mu_N^2<R_s\right)$. При цьому слід зазначити, що імовірність появи події хибної тривоги $P_{F.A.}$ не повинна перевищувати прийнятну величину $\overline{P}_{F.A.}$;

- «пропуск виявлення» – подія, при якій сигнал тривоги для диспетчера не подається, оскільки відстань між незалежними випадковими мітками не перевищує величини D_t, а помилки визначення фактичного стану повітряного судна залежною системою спостереження, що розглядається, більше величини $R_s\left(\xi_N^2+\mu_N^2\geq R_s\right)$. Слід зазначити, що імовірність появи події пропуску виявлення (ризик цілісності) $P_{I.R.}$ не повинна перевищувати прийнятну величину $\overline{P}_{I.R.}$.

Оскільки поява подій хибної тривоги та пропуску виявлення вкрай негативно впливає на безпеку польотів при використанні інформації залежних систем спостереження в цілях управління повітряним рухом, завданням даної роботи є формалізація моделей оцінки імовірності помилкової тривоги $P_{F.A.}$, а також ризику цілісності $P_{I.R.}$ Після того, як труднощі формалізації будуть подолані, введемо міру цілісності радіолокаційної інформації залежної систем спостереження, що розглядається.

Відомо, що процедура забезпечення цілісності заснована на аналізі різниці координат незалежних міток горизонтального положення повітряного судна $\left(x_N,y_N\right)$ та $\left(x_R,y_R\right)$.

Введемо наступні двовимірні випадкові величини: $\vec{N}=\|X_NY_N\|$ – вектор оцінки координат повітряного судна залежної систем спостереження; $\vec{R}=\|X_RY_R\|$ – вектор оцінки координат повітряного судна незалежної систем спостереження; $\vec{S}=\|S_x,S_y\|$ – відстань між векторами $\vec{N}$ та $\vec{R}$.

Слід зазначити, що вектори $\vec{N}$ та $\vec{R}$ являються незалежними з відомими щільностями, а компоненти векторів $\vec{N}$ та $\vec{R}$ також незалежні як всередині $\vec{N}$ та $\vec{R}$, так і між векторами.

Будемо вважати, що математичні очікування компонент вектору $\vec{R}$ збігаються з координатами фактичного положення повітряного судна, а математичні очікування компонент вектору $\vec{N}$ можуть мати зміщення за координатами Δx та Δy по відношенню до фактичних координат повітряного судна, що спостерігається. При цьому слід зазначити, що зміщення за координатами такі, що виконується рівність $\Delta x^2+\Delta y^2=R_s^2$.

Будемо вважати, що $\vec{N}$ і $\vec{R}$ – незалежні випадкові величини з щільностями $\omega_N(x)$ та $\omega_R(x)$. У загальному вигляді $\vec{N}$ і $\vec{R}$ – це двовимірні випадкові величини, але всі співвідношення будуть справедливі й для одновимірних випадкових незалежних величин.

Позначимо щільність випадкової величини $S=R-N$ як $q(s)$ та розглянемо дві пари випадкових величин: (N,R) – вихідна пара; (N,S)- пара, яка бере участь у процедурі забезпечення цілісності інформації залежної систем спостереження, що розглядається.

В цьому разі завжди апріорна (до застосування процедури забезпечення цілісності) спільна щільність імовірності пари випадкових векторів (N,S), яка буде дорівнювати $w_N(x)\cdot w_R(x+s)$.

При цьому слід зазначити, що знаючи апріорну спільну щільність імовірності пари випадкових векторів (N,S), можна обчислити умовну щільність імовірності $w_{w/s}(x;s)$ випадкової величини N за умови, що виконується наступна рівність $S=s$;

$$w_{w/s}(x;s)=\frac{w_N(x)w_R(x+s)}{g(s)}. \tag{2}$$

За умови, що відомі щільності імовірності $w_N(x)$ та $w_R(x+s)$, різницю випадкових незалежних вимірювань можливо обчислити як

$$g(s)=\int_{-\infty}^{\infty} w_N(x)\cdot w_R(x+s)dx. \tag{3}$$

Слід зазначити, що процедура забезпечення цілісності заснована на досвіді, при якому випадкова величина S приймає конкретне значення $s: S=s$. У цьому разі значення s порівнюють з порогом виявлення D_t та приймають рішення про подачу сигналу тривоги. При міркуванні про те, чи вийшли помилки залежної систем спостереження за межі радіусу утримання R_s або не вийшли за умови, що $S=s$, апріорна щільність помилок вимірювання залежної систем спостереження повинна бути замінена на умовну $u_{N/s}(x;s)$. Виходячи з викладеного, моделі оцінок імовірностей $P_{F.A.}$, $P_{I.R.}$ і $P_{I.}$ повинні будуватися не на щільності $q(s)$ і $w_N(x)$, а на щільності $q(s)$ та $u_{N/s}(x;s)$.

У цьому разі, виходячи із загальних міркувань формалізації імовірності помилкової тривоги і ризику цілісності, можемо записати:

$$P_{F.A.}=P\{|s|>D_t,|x|\le R_s\};\quad P_{I.R.}=P\{|s|\le D_t,|x|\le R_s\}.$$

З урахуванням того, що випадкові величини s і x мають щільності імовірності, рівні $q(s)$ та $u_{N/s}(x;s)$, отримаємо наступні значення шуканих імовірностей:

$$P_{F.A.}=\int_{|s|>D_t} q(s)\left[\int u_{N/s}(x;s)dx\right]ds; \tag{4}$$

$$P_{I.R.}=\int_{|s|>D_t} q(s)\left[\int_{|x|>R_s} u_{N/s}(x;s)dx\right]ds. \tag{5}$$

Помилки у визначенні координат повітряного судна за допомогою залежної систем спостереження в загальному вигляді можуть мати ненульовий зсув $\Delta=\sqrt{\Delta_x^2+\Delta_x^2}=R_s$. Стан, в якому залежна система спостереження вимірює координати повітряного судна із зсувами, будемо називати відмовою. Така імовірність стану дорівнює P_f. Апріорна щільність імовірності помилок вимірювання координат повітряного судна за допомогою залежної системи спостереження при відмові позначимо як $w_N^f(x;\Delta)$. Тоді й щільність різниці випадкових величин $R-N$ також матиме параметр зсуву Δ. Отже, умовну щільність помилок вимірювання координат повітряного судна залежної систем спостереження при відмові слід записувати зі зміщенням $w_{N/s}^f(x;s,\Delta)$.

Облік стану відмови залежної системи спостереження доповнює моделі хибної тривоги та ризику цілісності:

$$R_{F.A.}=(1-P_f)P_{F.A.}^{n.f.}+P_f P_{F.A.}^{f}; \tag{6}$$

$$R_{I.R.}=(1-P_f)P_{I.R.}^{n.f.}+P_f P_{I.R.}^{f}; \tag{7}$$

в яких $P_{F.A.}^{n.f.}$ та $P_{I.R.}^{n.f.}$ визначаються із співвідношень (4) та (5):

$$P_{F.A.}^{f} = \int_{|s|>D_t} q^{f}\left(s;\Delta = R_s\right)\left[\int_{|x|\le R_S} U_{N/s}^{F}\left(x;s,\Delta = R_s\right)dx\right]ds,$$

$$P_{I.R.}^{f} = \int_{|s|>D_t} q^{f}\left(s;\Delta = R_s\right)\left[\int_{|x|>R_S} U_{N/s}^{F}\left(x;s,\Delta = R_s\right)dx\right]ds.$$

Слід зауважити, що імовірність події, при якої помилка визначення місцеположення повітряного судна не перевищує заданий поріг R_s або помилку виявлення, тобто цілісність P_I об'єднує в собі три з чотирьох можливих подій: «правильне невиявлення», «правильне виявлення» та «хибну тривогу», внаслідок чого $P_I = 1 - R_{I.R.}$, де $R_{I.R.}$ визначається із виразу (7). Таким чином, цілісність координатної інформації залежних систем спостереження визначає імовірність того, що інформація про координати повітряного судна, що передається в повідомленнях залежних систем спостереження та використовується диспетчером в цілях управління повітряним рухом, не містить невиявлених помилок, які перевищують поріг R_s.

Висновки

Отримані результати дозволяють зробити висновки:

- показано, якщо різниця координат двох незалежних вимірювань одного і того ж положення повітряного судна більше деякої наперед заданої величини, то передбачається, що якість координатної інформації залежної системи спостереження, що розглядається, незадовільна і подається сигнал тривоги;

- цілісність координатної інформації зазначених залежних систем спостереження визначає імовірність того, що радіолокаційна інформація про координати повітряного судна, які передаються в повідомленнях залежних систем спостереження та використовуються диспетчером в цілях управління повітряним рухом, не містить невиявлених помилок, які перевищують поріг встановленого радіуса утримання.

Список літератури:

1. Neindre F. L., Ferre G., Dallet D., Letellier F., and Pitois K., A successive interference cancellation-based receiver for Secondary Surveillance Radar // IEEE Transactions on Aerospace and Electronic Systems, pp. 1–12, 2022. doi:10.1109/taes.2022.3193649
2. Свид І.В., Обод І.І. Завадостійкість радіолокаційних систем ідентифікації за ознакою «свій-чужий» : монографія. Харків : Друкарня Мадрид, 2021. 254 с.
3. Gao J., Zou J., and Guo N. A secondary surveillance radar data analysis technique based on geometrical method // Lecture Notes in Electrical Engineering, pp. 707–715, Jun. 2019.
4. Обод І.І., Стрельницький О.О., Андрусевич В.А. Структура та показники якості обробки інформації систем спостереження повітряного простору // Системи обробки інформації. 2013. № 8(115). С. 80–83.
5. Kim W.-H., Jung S.-Y., Lee Y.-S., and Chang S.-M. Mark XIIA(Mode 5) IFF system integration and certification test for surface to air missile system // Journal of the Korea Institute of Military Science and Technology, vol. 25, no. 2, pp. 160–168, Apr. 2022.
6. Обод І.І., Свид І.В. Порівняльний аналіз якості виявлення повітряних об'єктів запитальними системами спостереження // Системи обробки інформації. 2010. Вип. 9 (90). С. 74–76.
7. Svyd I. V. Comparative analysis of the quality of detection of air objects by secondary radar systems // Radiotekhnika. 2023. № 213. P. 78–87. doi:10.30837/rt.2023.2.213.09.
8. Василишин В.І., Лєбєдєв В.О., Висоцький О.В., Коцюба В.П. Вторинна радіолокація як основа сучасних систем спостереження за повітряною обстановкою // Наука і техніка Повітряних Сил Збройних Сил України. 2021. № 2(43). С. 94–103. https://doi.org/10.30748/nitps.2021.43.13.
9. 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.
10. Svyd I. et al. Optimal measurement of signal data parameters of requesting radar systems, 2021 // IEEE 3rd Ukraine Conference on Electrical and Computer Engineering (UKRCON), 2021. doi:10.1109/ukrcon53503.2021.9575235
11. Obod I. I. Integrated coordinate-and-time support for the Address Inquiry in the secondary radar systems // Telecommunications and Radio Engineering. 1999. Vol. 53, No 3. P. 54–56, doi:10.1615/telecomradeng.v53.i3.100

12. Свид І.В. Показники якості інформаційного забезпечення користувачів сполученими системами спостереження повітряного простору // Радіотехніка. 2011. Вип. 165. С. 157–160.
13. Beel J. J. Anti-UAV Defense For Ground Forces and Hypervelocity Rocket Lethality Models, Monterey, California : Naval Postgr aduate School, 1992. P. 36–46.
14. Moses A., Rutherford M. J., and Valavanis K. P. Radar-based detection and identification for Miniature Air Vehicles // 2011 IEEE International Conference on Control Applications (CCA), 2011. doi:10.1109/cca.2011.6044363
15. Sadasivan S., Gurubasavaraj M., Sekar S.R. Acoustis siqnature of an unmanned air vehicle – exploitation for aircraft localisation and parameter estimation // Eronautical DEF SCI J. 2001. Vol. 51, № 3. P. 279–283.
16. Svyd I. et al., Optimizing the request signals detection of aircraft secondary radar system transponders // 2022 IEEE 41st International Conference on Electronics and Nanotechnology (ELNANO), 2022. doi:10.1109/elnano54667.2022.9926991
17. Обод І.І., Стрельницький О.О. Інформаційна безпека інформаційної мережі систем спостереження повітряного простору // Системи обробки інформації. 2015. № 9(134). С. 96–98.
18. Dhipu T. M., Rishabh V., and Rajesh R. Identification friend or foe mode code detection using Deep Pulse Detector Network // Journal of Aerospace Information Systems. 2023. Vol. 20. No. 1, P. 17–24.
19. Semenets V. et al. Method of increasing the relative throughput of requesting radar systems // Przegląd Elektrotechniczny. 2022. Vol. 1, No. 11. P. 99–103, doi: 10.15199/48.2022.11.17.
20. Обод І.І., Шевцова В.В. Пропускна спроможність відповідачів запитальних систем передачі польотної інформації // Системи обробки інформації. 2013. № 1(108). С. 105–108.
21. Andrusevich V., Obod I. Assessment of the quality of information support by air radar surveillance systems // Advanced Information Systems. 2021. Vol. 5, No. 2. P.78–82. DOI: https://doi.org/10.20998/2522-9052.2021.2.10.
22. Pavlova D. B. et al. Comparative analysis of data consolidation in Surveillance Networks // 2019 10th International Conference on Dependable Systems, Services and Technologies (DESSERT), 2019. doi:10.1109/dessert.2019.8770008.
23. 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.
24. Комплексне інформаційне забезпечення систем управління польотами авіації та протиповітряної оборони / В.В. Ткачев, Ю.Г.Даник, С.А. Жуков, І.І. Обод, І.О. Романенко. Київ : МОУ, 2004. 342 с.
25. Федоров А.В., Дергоусов М.Ю., Шевченко О.О., Пилипович О.М., Сердюк О.В. Визначення координат повітряних об'єктів системою приймачів ADS-B з застосуванням технології MLAT в умовах багатоцільової обстановки // Системи обробки інформації. 2022. № 1 (168). С. 43–51. https://doi.org/10.30748/soi.2022.168.05.

Надійшла до редколегії 17.02.2024

Відомості про авторів:

Свид Ірина Вікторівна – кандидат технічних наук, доцент, завідувач кафедри мікропроцесорних технологій і систем, Харківський національний університет радіоелектроніки, доцент кафедри авіаційних радіотехнічних систем навігації та посадки, Харківський національний університет Повітряних Сил імені Івана Кожедуба, Україна; email: iryna.svyd@nure.ua; ORCID: http://orcid.org/0000-0002-4635-6542

Ігнатюк Іван Валентинович – магістрант кафедри мікропроцесорних технологій і систем, Харківський національний університет радіоелектроніки, Україна; email: ivan.ihnatiuk@nure.ua; ORCID: https://orcid.org/0009-0005-1988-543X

Шуніборов Олег Дмитрович – магістрант кафедри мікропроцесорних технологій і систем, Харківський національний університет радіоелектроніки, Україна; email: oleh.shuniborov@nure.ua; ORCID: https://orcid.org/0009-0007-0352-0027

Майстренко Галина Валеріївна – старший викладач кафедри електронних обчислювальних машин, Харківський національний університет радіоелектроніки, Україна; email: halyna.maistrenko@nure.ua; ORCID: https://orcid.org/0000-0002-8126-9997

Туленко Михайло Володимирович – старший викладач кафедри авіаційних радіотехнічних систем навігації та посадки, Харківський національний університет Повітряних Сил імені Івана Кожедуба, Україна; email: super-tulenko@ukr.net; ORCID: https://orcid.org/0000-0003-4484-2069

COLLECTION OF SCIENTIFIC PAPERS
RADIOTEKHNIKA
Issue 216
In English and Ukrainian

ЗБІРНИК НАУКОВИХ ПРАЦЬ
РАДІОТЕХНІКА
Випуск 216
Англійською та українською мовами

Коректор Л.І. Сащенко

Підп. до друку 30.03.2024. Формат 60x90/8. Папір офсет. Гарнітура Таймс. Друк. ризограф.
Ум. друк. арк**.** 11,2. Обл.-вид. арк. 10,9. Тираж 300 прим. Зам. № 17. Ціна договір.

Харківський національний університет радіоелектроніки (ХНУРЕ)
Просп. Науки, 14, Харків, 61166.

Оригінал-макет підготовлено і збірник надруковано у ПФ „Колегіум”,
Свідоцтво про внесення суб’єкта видавничої діяльності до Державного реєстру видавців.
Сер. ДК №1722 від 23.03.2004.

ABSTRACTS РЕФЕРАТИ

SYSTEMS AND METHODS OF INFORMATION PROTECTION
СИСТЕМИ І МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ

UDC 004.056.5

Research into methods and algorithms for generating (pseudo) random sequences over an arbitrary alphabet / *I.D. Gorbenko, A.N. Alekseychuk, Ye.G. Kachko, Ya.A. Derevianko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2024. № 216. P. 7 – 29.

Randomness is an integral component of most special software and hardware CIP tools. Work and development towards improving the process of randomness generation is actively underway and requires special attention.

This paper is devoted to the research into algorithms for generating (pseudo)random sequences over an arbitrary alphabet, estimating their complexity (time and capacity), as well as statistical characteristics. This study is important because modern post-quantum algorithms use such sequences to generate keys and random components of digital signatures and key encapsulation.

Obtained results can serve as a motivation for choosing an algorithm for generating sequences of an arbitrary alphabet for use in certain cryptographic transformations or algorithms.

Key words: random sequences; sequence generation; arbitrary alphabet; generation methods; crypto providers; random number generators.

29 tabl. 8 fig. Ref: 25 items.

УДК 004.056.5

Дослідження методів та алгоритмів для генерації (псевдо) випадкових послідовностей над довільним алфавітом / *І.Д. Горбенко, А.М. Олексійчук, О.Г. Качко, Я.А. Дерев'янко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2024. Вип. 216. С. 7 – 29.

Невід'ємною складовою більшості спеціальних програмних та апаратних засобів КЗІ є випадковість. Робота та розвиток в напрямку покращення процесу генерації випадковості активно ведеться та потребує особливої уваги.

Дана робота присвячена дослідженню алгоритмів для генерації (псевдо)випадкових послідовностей над довільним алфавітом, оцінці їх складності (часової та ємнісної), а також статистичних характеристик. Це дослідження важливе в зв'язку з тим, що для сучасних постквантових алгоритмів застосовують саме такі послідовності для генерації ключів та випадкових компонентів електронного підпису та інкапсуляції ключів.

Отримані результати можуть виступати у якості мотивації вибору алгоритму для генерації послідовностей довільного алфавіту для використання у певних криптоперетвореннях чи алгоритмах.

Ключові слова: випадкові послідовності; генерація послідовностей; довільний алфавіт; методи генерації; криптопровайдери; генератори випадкових чисел.

Табл. 29. Іл. 8. Бібліогр.: 25 назв.

UDC 004.056.5

Methods and means for analysing, evaluating and comparing properties of random sequences and random numbers / *D.Yu. Holubnychiy, S.O. Kandiy, M.V. Yesina, D.Yu. Gorbenko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2024. № 216. P. 30 – 45.

Methods and means for analysing, assessing and comparing properties of random sequences and random numbers are considered in the work. The article also discusses such aspects as mathematical modeling of random processes, statistical methods for estimating distribution parameters, comparative analysis of the properties of random variables. To date, random sequences (RS) and random numbers (RN), produced by physically real (PT RNG) and non-physically real (NPT RNG) generators, are widely used in practice, they essentially legislate key generation mechanisms in cryptographic systems. Depending on the cryptographic transformations, they are used to generate long-term keys and session keys of symmetric cryptographic transformations, long-term asymmetric key pairs and session key pairs, general parameters of cryptographic transformations and cryptographic protocols, specific one-time values (nonces), challenges (challenges), blinding and masking values, etc. Among the set of requirements for such generators is the provision of the maximum possible value of the initial entropy in a number of, and possibly most, cryptographic applications. The analysis of international and national legal documents regarding the requirements for PT RNG and NPT RNG sources and, accordingly, generators, carried out in the work showed that they, taking into account the significant challenges associated with expanding the possibilities of cryptanalysis based on application, in addition to classical, quantum and side channel attacks should be significantly improved and evaluated using complex methods using a system of unconditional criteria. The purpose of this article is to substantiate, develop and confirm experimentally the correct application of RS and RN generation algorithms based on PTRNG and NPTRNG, including in the application of classical and quantum microelectronics, as well as the development of recommendations for their use for generating keys and parameters for quantum stable methods and standards of cryptographic transformations.

Key words: analysis; random sequences; random numbers; generators; noise source; entropy; evaluation methods; comparison methods; testing.

1 tabl. 5 fig. Ref: 39 items.

УДК 004.056.5

Методи та засоби аналізу, оцінки та порівняння властивостей випадкових послідовностей та випадкових чисел / *Д.Ю. Голубничий, С.О. Кандій, М.В. Єсіна, Д.Ю. Горбенко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2024. Вип. 216. С. 30 – 45.

Розглядаються методи та засоби аналізу, оцінки та порівняння властивостей випадкових послідовностей та випадкових чисел. Обговорюються також такі аспекти, як математичне моделювання випадкових процесів, статистичні методи оцінювання параметрів розподілу, порівняльний аналіз властивостей випадкових величин. На сьогодн випадкові послідовності (ВП) та випадкові числа (ВЧ), що виробляються фізично справжніми (PT RNG) та нефізично справжніми (NPT RNG) генераторами, широко застосовуються на практиці – вони по суті законодавчо визначають механізми генерування ключів у криптографічних системах. У залежності від криптографічних перетворень, вони застосовуються для генерації довгострокових ключів та ключів сеансу симетричних криптоперетворень, довгострокових асиметричних пар ключів та пар сеансових ключів, загальних параметрів криптоперетворень та криптографічних протоколів, специфічних одноразових значень (nonces), викликів (challenges), засліплення та маскування значень тощо. Серед множини вимог до таких генераторів є забезпечення у ряді, а можливо і більшості, криптографічних застосунків максимально можливого значення початкової ентропії. Аналіз міжнародних та національних нормативно-правових документів щодо вимог до PT RNG та NPT RNG джерел та відповідно до генераторів показав, що вони, з урахуванням суттєвих викликів, які пов’язані з розширенням можливостей криптоаналізу на основі застосування, крім класичних, квантових та атак бічними каналами, суттєвою мірою повинні бути удосконаленими та оцінені з використанням комплексних методик із використанням системи безумовних критеріїв. Метою даної статті є обґрунтування, розробка та експериментальне підтвердження коректного застосування алгоритмів генерування ВП та ВЧ на основі PTRNG та NPTRNG, в тому числі при застосуванні класичної та квантової мікроелектроніки, а також розробка рекомендацій щодо їх застосування для генерування ключів та параметрів для квантово стійких методів та стандартів криптографічних перетворень.

Ключові слова: аналіз; випадкові послідовності; випадкові числа; генератори; джерело шуму; ентропія; методи оцінки; методи порівняння; тестування.

Табл. 1. Іл. 5. Бібліогр.: 39 назв.

UDC 004.05

Modern threats to information and communication systems and methods of protection against them / *O.I. Peliukh, M.V. Yesina, D.Yu. Holubnychyi* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2024. № 216. P. 46 – 56.

In the modern world, information and communication systems (ICS) have become an integral part of our lives, processing, storing and transmitting information. However, this dependence makes them extremely vulnerable to various threats. The article examines the current threats that call into question the normal functioning of ICS. The authors emphasise the constant evolution of these threats, which makes them more complex and dangerous. This necessitates constant research and development of new methods and means of information protection, as well as raising awareness of ICS users about cyber threats. The purpose of the article is to study modern ICS threats and develop recommendations for improving the level of information security (IS). The article provides a classification of ICS IS threats by various criteria: by the basic principles of the cybersecurity triad (confidentiality, integrity and availability), by sources of threats (internal and external), by the amount of damage caused (from general to private), by the degree of impact (passive and active) and by the nature of occurrence (natural and artificial). The article reveals the sources of threats to ICS security: unintentional (related to user errors, software failures or hardware failures) and intentional (cyber-attacks aimed at causing damage to ICS). Particular attention is paid to cyberattacks that are becoming more widespread. The authors describe different types of cyberattacks, as well as methods and means of their implementation. An important aspect of the article is the development of recommendations for improving the level of security. Along with the technical aspects of protection, the article considers the importance of implementing organisational measures such as security policy, access control and privilege management. The article also draws attention to the importance of complying with international and national standards for the protection of information in ICS. These measures help to avoid leakage or prevent unauthorised access to valuable information.

Key words: information; information security; information and communication systems; information protection; protection methods; threats.

7 fig. Ref: 11 items.

УДК 004.05

Сучасні загрози інформаційно-комунікаційним системам та методи захисту від них / *О.І. Пелюх, М.В. Єсіна, Д.Ю. Голубничий* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2024. Вип. 216. С. 46 – 56.

Інформаційно-комунікаційні системи (ІКС) стали невід'ємною складовою нашого життя, обробляючи, зберігаючи та передаючи інформацію. Проте ця залежність робить їх надзвичайно вразливими перед різноманітними загрозами. У статті досліджуються сучасні загрози, що ставлять під питання нормальне функціонування ІКС. Автори підкреслюють постійну еволюцію цих загроз, що робить їх усе складнішими й небезпечнішими. Це викликає потребу в постійному дослідженні та розробці нових методів та засобів захисту інформації, а також у підвищенні обізнаності користувачів ІКС щодо кіберзагроз. Метою статті є дослідження сучасних загроз ІКС та розробка рекомендацій щодо підвищення рівня інформаційної безпеки (ІБ). Стаття надає класифікацію

загроз ІБ ІКС за різними ознаками: за основними принципами тріади з кібербезпеки (конфіденційність, цілісність й доступність), за джерелами загроз (внутрішніми й зовнішніми), за розмірами нанесеної шкоди (від загальних до приватних), за ступенем впливу (пасивні й активні) та за природою виникнення (природні й штучні). Матеріали статті розкривають джерела загроз ІБ ІКС: ненавмисні (пов'язані з помилками користувачів, збоями в програмному забезпеченні або апаратними відмовами) й умисні (кібератаки, спрямовані на завдавання шкоди ІКС). Особлива увага приділяється кібератакам, які стають все поширенішими. Автори описують різні типи кібератак, а також методи й засоби їхнього здійснення. Важливим аспектом статті є розробка рекомендацій щодо підвищення рівня ІБ. Поряд з технічними аспектами захисту, стаття розглядає важливість впровадження організаційних заходів, таких як політика ІБ, контроль доступу та управління привілеями. Також в статті звертається увага на важливість дотримання міжнародних та національних стандартів щодо захисту інформації в ІКС. Ці заходи допомагають уникнути витоку чи недопущенню несанкціонованого доступу до цінної інформації.

Ключові слова: інформація; інформаційна безпека; інформаційно-комунікаційні системи; загрози; захист інформації; методи захисту.

Іл. 7. Бібліогр.: 11 назв.

UDC 004.065.5

Comparative analysis of Ukrainian and foreign banking applications / *Y.O. Lohachova, M.V. Yesina* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2024. № 216. P. 57 – 61.

Mobile banking applications have been actively used in the financial sector for several years. Such applications significantly facilitate the use of banking services for their users. At the time of active digitalisation, the financial sector also needed reforms and active changes, that is why developers have been actively working on creating first home banking and then mobile banking applications since the end of the last century. Mobile banking applications have come a long way in evolution, so that users can now perform not only simple banking operations, but also many new additional functions making life easier. The development of the technologies used has also led to the emergence of new vulnerabilities, which required the improvement of security systems in such applications. The development path and experience of Ukrainian applications is somewhat different from that of foreign ones, but no less valuable. The development of foreign applications is more standardised and controlled by the government. Such solutions allow for better verification of compliance with security requirements. However, it should not be forgotten that mobile banking was created to facilitate financial transactions remotely, and therefore it should be easy to use by the average user. The article provides a comparative analysis of Ukrainian and foreign banking **applications**, including: Stanford FCU, Fideuram, N26, Banque populaire du nord, Sparkasse, Monobank, Privat24, Ukrsib-online, Oschadbank, and PUMB. The applications were compared by two groups of criteria, namely security and convenience criteria. The article focuses not only on the aspects in which Ukrainian applications should develop, but also on those in which they have an advantage over foreign apps.

Key words: bank; banking mobile applications; banking; cybersecurity; finance; security.

4 tabl. Ref: 15 items.

УДК 004.065.5

Порівняльний аналіз українських та закордонних банківських застосунків / *Є.О. Логачова, М.В. Єсіна* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2024. Вип. 216. С. 57 – 61.

Вже не перший рік мобільні банківські додатки активно використовуються у фінансовому секторі. Такі застосунки істотно полегшують користування банківськими послугами для своїх користувачів. У час активної діджиталізації фінансова сфера також потребувала реформацій та активних змін, саме тому розробники почали активно працювати над створенням спершу домашніх банкінгів, а потім мобільних банківських додатків, ще з кінця минулого століття. Банківські мобільні додатки пройшли довгий шлях еволюції, щоб зараз користувачі могли виконувати не тільки прості банківські операції, а і багато нових додаткових функцій, що полегшують життя. Розвиток використаних технологій призводив і до виникнення нових вразливостей, вирішення яких потребувало покращення систем безпеки у таких додатках. Шлях розвитку та досвід українських застосунків дещо відрізняється від закордонних, проте є не менш цінним. Розробка закордонних додатків – більш стандартизована та контрольована урядом. Такі рішення дозволяють якісніше перевіряти відповідність вимогам безпеки. Проте варто і не забувати про те, що мобільні банкінги були створені для полегшення здійснення фінансових операцій дистанційно, а отже вони мають бути зручними при використанні пересічним користувачем. У статті наведено порівняльний аналіз українських та закордонних банківських застосунків, до таких увійшли: Stanford FCU, Fideuram, N26, Banque populaire du nord, Sparkasse, Monobank, Приват24, Укрсиб-онлайн, Ощадбанк, ПУМБ. Порівняння застосунків проводилось за двома групами критеріїв, а саме критеріями безпеки та критеріями зручності. У статті увага націлена не тільки на ті аспекти, у яких українські застосунки мають розвиватись, а і ті, у яких вони мають перевагу над закордонними додатками.

Ключові слова: банк; банківські мобільні додатки; банкінг; кібербезпека; фінанси; безпека.

Табл. 4. Бібліогр.: 15 назв.

UDC 621.391:519.2

Research horizons in group cryptography in the context of post-quantum cryptosystems development / *Y. Kotukh, G. Khalimov, M. Korobchynskyi, M. Rudenko, V. Liubchak, S. Matsyuk, M. Chashchyn* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2024. № 216. P. 62 –72.

Asymmetric cryptography relies on the principle of ease of calculation and complexity of one-sided functions' inversion. These functions can be easily implemented, but inverting them is computationally difficult. In this context, NP-complete problems are ideal candidates for the role of such functions in asymmetric cryptography, since generating their cases is easy, but finding solutions is difficult. However, the practical application of NP-complete problems has certain limitations, in particular due to difficulties in creating problems that would be complex on average. Although an NP-complete problem may be hard in general, a particular case of it may be solvable, making it unsuitable for cryptography. The article considers classes of NP problems. Basic definitions and concepts are given. The properties of the class of NP-complete problems, the conditions for determining belonging to the set of NP-complete problems, and the current state of difficult to solve problems are analyzed. It turns out that the class of NP-complete problems is hard for quantum computing. The criteria for belonging of the word problem in groups to NP-complete problems are analyzed. Finite non-Abelian groups are defined for which the word problem is NP-complete. The advantages of using non-Abelian groups for cryptographic applications are considered. The rules of change of form, which determine the transformation of equivalent words, are given. The word problem in finite groups is one of the NP-complete problems. The latest research and prospects for the development of cryptographic primitives of asymmetric cryptography using difficult-to-solve problems in finite groups are analyzed.

Key words: word problem; NP-complete problems; asymmetric cryptosystem; logarithmic signature.

1 fig. Ref: 34 items.

УДК 621.391:519.2

Горизонти досліджень в груповій криптографії в контексті розробки постквантових криптосистем / *Є.В. Котух, Г.З. Халімов, М.В. Коробчинський, М.М. Руденко, В.О. Любчак, С.М. Мацюк, М.В. Чащин* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2024. Вип. 216. С. 62 – 72.

Асиметрична криптографія покладається на принцип легкості обчислення та складності обернення односторонніх функцій. Ці функції можна легко виконати, але інвертувати їх обчислювально складно. У цьому контексті NP-повні задачі є ідеальними кандидатами для виконання ролі таких функцій у асиметричній криптографії, оскільки генерувати їх випадки легко, але знаходити рішення – складно. Проте, практичне застосування NP-повних задач має певні обмеження, зокрема через складності зі створенням задач, які були б складними у середньому. Хоча NP-повна задача може бути загалом складною, окремий її випадок може бути вирішений, що робить її непридатною для криптографії. В статті розглядаються класи NP проблем. Дано основні визначення та поняття. Проаналізовано властивості класу NP-повних задач, умови визначення належності до множини NP-повних задач та поточний стан складних для розв'язання проблем. Визначається, що клас NP-повних проблем є складним для квантових обчислень. Проаналізовано критерії належності проблеми слова в групах до NP-повних проблем. Визначено кінцеві неабелеві групи, для яких проблема слова є NP-повною. Розглянуто переваги використання неабелевих груп для криптографічного застосування. Наведено правила зміни форми, що визначають перетворення еквівалентних слів. Проблема слова в кінцевих групах є однією з NP-повних проблем. Проаналізовано останні дослідження та перспективи розробки криптографічних примітивів асиметричної криптографії з використанням складних для розв'язання проблем у кінцевих групах.

Ключові слова: проблема слова; NP-повні задачі; асиметрична криптосистема; логарифмічний підпис.

Іл. 1. Бібліогр.: 34 назв.

RADIO TECHNICAL DEVICES
РАДІОТЕХНІЧНІ ПРИСТРОЇ

UDC 621. 396:004.056.5

Assessment of the localization error of radio-acoustic bug devices by means of acoustic distance measurement / *A.N. Oleynikov, Yu.V. Lykov, B.I. Zabolotnyi* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2024. № 216. P. 73 – 80.

Localization of a radio-acoustic bug device (RABD) is the determination of its location in space. Localization of the RABD can be carried out both by the electromagnetic field and by using acoustic probing signals.

Localization using acoustic probing signals is carried out using an acoustic rangefinder (AR) as part of a hardware-software complex (HSC) for detecting RABD (for example, the «ORT», «VOSTOK» hardware systems developed at KNURE). The operating principle of AR is given in the article.

The error in measuring the coordinates of the RABD with an acoustic rangefinder consists of instrumental and random errors in measuring the range, as well as the methodological error in determining the location of the RABD, which is due to the peculiarities of the rangefinder method of determining coordinates.

The article addresses the issue of minimizing the error in measuring the range of a bug device with an uncertainty of location by analyzing various methods for fixing the temporary position of an acoustic signal in real conditions for detecting radio-acoustic embedded devices in designated premises.

The advantages and disadvantages of various methods for fixing the time position of an acoustic signal along one of the pulse fronts are analyzed simultaneously on the leading and falling edges of the pulse, at the position of the maximum signal values and using the correlation method of fixing the time position of the signal in relation to the localization of radio-acoustic bug devices in real conditions. The results of mathematical modeling and experimental research using the HSC "VOSTOK" of the error in determining the range to a radio-acoustic bug device are presented.

It has been established that when localizing bug devices using an acoustic range finder, it is advisable to use the correlation method of fixing the time position of pulses. At the same time, there is a decrease in the standard deviation of the localization error compared to the threshold method by 15% in the range of s/n values from 2 to 20, high stability of the results and low sensitivity to changes in the amplitude of the received signal.

Key words: radio-acoustic bugs; localization; hardware and software complex; range measurement error; fixation of time position; correlation method

6 fig. Ref.: 5 items.

УДК 621. 396:004.056.5

Оцінка похибки локалізації радіоакустичних закладних пристроїв засобами акустичної далекометрії / *А.М. Олейніков, Ю.В. Ликов, В.І. Заболотний* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2024. Вип. 216. С. 73 – 80.

Локалізація радіоакустичного закладного пристрою **(**РАЗП) – це визначення його місця розташування у просторі. Локалізація РАЗП може здійснюватися як по електромагнітному полю, так і із застосуванням акустичних зондувальних сигналів.

Локалізація із застосування акустичних зондувальних сигналів здійснюється за допомогою акустичного далекоміра (АД) у складі апаратно-програмного комплексу (АПК) для виявлення РАЗП (наприклад АПК «ОРТ»,«VOSTOK» розроблених у ХНУРЕ). Принцип роботи АД наведено у статті.

Похибка вимірювання координат РАЗП акустичним далекоміром складається з апаратурної та випадкової похибок вимірювання дальності, а також методичної похибки визначення місця розташування РАЗП, яка обумовлена особливостями далекомірного методу визначення координат.

Розглядається питання мінімізації помилки вимірювання дальності до закладного пристрою шляхом аналізу різних методів фіксації часового положення акустичного сигналу в реальних умовах виявлення радіоакустичних закладних пристроїв у виділених приміщеннях.

Проводиться аналіз переваг та недоліків різних методів фіксації часового положення акустичного сигналу по одному із фронтів імпульсу, одночасно по передньому та задньому фронтам імпульсу, по положенню максимальних значень сигналу та з використанням кореляційного методу фіксації часового положення сигналу стосовно локалізації радіоакустичних закладних пристроїв у реальних умовах. Наводяться результати математичного моделювання та експериментального дослідження з використанням АПК «VOSTOK» помилки визначення дальності до радіоакустичного закладного пристрою.

Встановлено, що при локалізації закладних пристроїв за допомогою акустичного далекоміра доцільно використовувати кореляційний метод фіксації часового положення імпульсів. При цьому відмічається: зменшення середньоквадратичного відхилення похибки локалізації порівняно з пороговим методом на 15 % у діапазоні значень с/ш від 2 до 20, висока стабільність результатів та мала чутливість до змін амплітуди сигналу, що приймається.

Ключові слова: радіоакустичний закладний пристрій; локалізація; апаратно-програмний комплекс; похибка вимірювання відстанні; фіксації часового положення; кореляційний метод.

Іл. 6. Бібліогр.: 5 назв.

UDC 551.501.7

Software and hardware complex based on the STM32F407VG microcontroller for studying vibrations with the LIS3DSH accelerometer / *V.V. Semenets, A.B. Grigoriev* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2024. № 216. P. 81 – 86.

The statement of the problem of building a software-hardware complex based on the STM32F407VG microcontroller for studying vibrations with the LIS3DSH accelerometer is given.

A physical model of the system, including a microcontroller, three-axis digital LIS3DSH accelerometer, was designed and implemented, which is characterized by a low price of the technical solution. The interaction between the microcontroller and the accelerometer occurs through the SPI interface.

Specialized software of the system was developed and implemented, it includes a driver for setting up, collecting and processing data from the accelerometer and a corresponding software for plotting graphs of vibro acceleration signals in the time and frequency domains. The built-in software enables you to implement extensive functionality and is free to use.

The built system makes it possible to analyze vibration parameters in order to predict and prevent possible accidents, reducing the costs associated with the failure of expensive parts and components.

Key words: hardware and software complex; vibrations; accelerometer; Software; register; interface; microcontroller.

1 fig. Ref: 14 items.

УДК 551.501.7

Програмно-апаратний комплекс на базі мікроконтролера STM32F407VG для дослідження вібрацій акселерометром LIS3DSH / *В.В. Семенець, О.В. Григор'єв* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2024. Вип. 216. С. 81 – 86.

Приведено постановку задачі побудови програмно-апаратного комплексу на базі мікроконтролера STM32F407VG для дослідження вібрацій акселерометром LIS3DSH.

Спроєктовано та реалізовано фізичну модель системи, яка включає мікроконтролер, трьохосьовий цифровий акселерометр LIS3DSH, яка характеризується низькою ціною технічного рішення. Взаємодія між мікроконтролером та акселерометром відбувається через інтерфейс SPI.

Розроблено та реалізовано спеціалізоване програмне забезпечення системи, яке включає драйвер для налаштування, збору і опрацювання даних з акселерометра та відповідне програмне забезпечення для побудови графіків сигналів віброприскорення в часовій і частотній областях. Побудоване програмне забезпечення дає змогу реалізувати широкі функціональні можливості та є вільним для використовування.

Побудована система дає можливість проводити аналіз параметрів вібрації з метою передбачення і запобігання можливих аварій, зменшуючи затрати пов'язані з виходом із ладу дорогих деталей і вузлів.

Ключові слова: програмно-апаратний комплекс; вібрації; акселерометр; програмне забезпечення; регістр; інтерфейс; мікроконтролер.

Іл. 1. Бібліогр.: 14 назв.

MEANS OF TELECOMMUNICATIONS
ЗАСОБИ ТЕЛЕКОМУНІКАЦІЙ

UDC 621. 396.677.49

Early warning model of cyber threats in 5G networks using Markov processes / *Y.Y. Kolyadenko, V.O. Badeyev* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2024. № 216. P. 87 – 93.

Security of telecommunication networks, in which the transmission channel can be used by many users simultaneously, is a particularly important problem. In wireless metropolitan networks, this problem is compounded by the fact that the communication channel is publicly available. In other words, information transmitted in such networks can be easily intercepted by intruders. This can lead to theft of personal data, financial losses, or even to a breach of security of critical infrastructure.

Information security can be compromised by failures that affect the availability, integrity, or confidentiality of information. These failures can be caused by vulnerabilities, namely, defects in software or hardware that can be exploited by attackers to gain unauthorized access to information. Information security is one of the components of 5G networks reliability. The main security threat to such systems is vulnerabilities, primarily of software components. Despite the fact that information about vulnerabilities of software products is publicly available, there is not enough data to quantify the security of these products using a single general criterion. It is also impossible to predict how well they will be protected from attacks in the future. One of the main problems of choosing the most secure 5G configuration is the difficulty in quantifying the level of information security. In addition, it is difficult to choose adequate evaluation indicators that take into account all the factors affecting successful network penetration and the amount of potential damage.

The search for vulnerabilities in software components is an urgent and resource-intensive task that has recently been taken up by large companies and research centers. Analysis of vulnerability detection and remediation processes shows that they can be described by a mass service system with an infinite queue length.

A model for early warning of cyber threats in 5G networks using Markov processes has been developed. Using simulation modeling in the Matlab environment, a time diagram of the arrival of requests for vulnerability detection was obtained. The change in the probabilities of states was also obtained. Thus, knowing the intensity of the flows, it is possible to model and predict the processes of the arrival of requests for vulnerability detection in real time.

Key words: Cyber threat; 5G networks; Markov processes; Vulnerability detection and remediation.

5 fig. Ref.: 8 items.

УДК 621. 396.677.49

Модель раннього попередження про кіберзагрози у мережах 5G з використанням марківських процесів / *Ю.Ю. Коляденко, В.О. Бадеєв* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2024. Вип. 216. С. 87 – 93.

Безпека телекомунікаційних мереж, у яких канал передачі може використовуватися одночасно багатьма користувачами, є особливо важливою проблемою. У безпроводових міських мережах ця проблема ускладнюється тим, що канал зв'язку є загальнодоступним. Іншими словами, інформація, яка передається в таких мережах, може бути легко перехоплена зловмисниками. Це може призвести до крадіжки персональних даних, фінансових збитків або навіть до порушення безпеки критичної інфраструктури.

Інформаційна безпека може бути порушена відмовами, які впливають на доступність, цілісність або конфіденційність інформації. Ці відмови можуть бути викликані вразливостями – дефектами в програмному або апаратному забезпеченні, які можуть бути використані зловмисниками для отримання несанкціонованого доступу до інформації. Інформаційна безпека є однією із складових гарантоспроможності мережах зв'язку 5G. Ос-

новну загрозу безпеці таких систем становлять вразливості насамперед програмних компонентів. Незважаючи на те, що інформація про вразливості програмних продуктів є загальнодоступною, існуючих даних недостатньо для того, щоб кількісно оцінити безпеку цих продуктів за одним загальним критерієм. Також неможливо прогнозувати, наскільки вони будуть захищені від атак у майбутньому. Одна з основних проблем вибору найбільш захищеної конфігурації 5G полягає в складності кількісної оцінки рівня інформаційної безпеки. Крім того, важко обрати адекватні показники для оцінки, які враховують всі фактори, що впливають на успішне проникнення в мережу та розмір потенційних збитків.

Пошук вразливостей у програмних компонентах є актуальним та ресурсомістким завданням, яким останнім часом займаються великі компанії та дослідницькі центри. Аналіз процесів виявлення та усунення вразливостей показує, що вони можуть бути описані системою масового обслуговування з необмеженою довжиною черги.

Розроблено модель раннього попередження про кіберзагрози у мережах 5G з використанням марківських процесів. За допомогою імітаційного моделювання в середовищі Matlab отримано часову діаграму надходження заявок на виявлення вразливостей. Також отримано зміну ймовірностей станів. Таким чином, знаючи інтенсивність потоків можна в реальному масштабі часу моделювати та прогнозувати процеси надходження заявок на виявлення вразливостей.

Ключові слова: кіберзагроза; мережі 5G; марківські процеси; виявлення та усунення вразливостей.

Іл. 5. Бібліогр.: 8 назв.

UDC 621.38

Features of voice traffic transmission using IEEE 802.11ac wireless networks / *V.S. Lazebnyi, O.O. Omelyanets* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2024. № 216. P. 94 – 102.

The purpose of the research is to find out the features of voice traffic transmission for the organization of IP telephony service in office premises using the IEEE 802.11ac network to ensure the high-quality provision of the specified service for a sufficiently large number of users even in the case of intensive transmission of a mixed traffic. The analytical study is based on traditional probabilistic approaches to evaluating the operational characteristics of wireless networks of the 802.11 standard. The 802.11ac network with a channel bandwidth of 20 MHz in the mode with one spatial stream was studied. In the specified network, a scenario was considered in which, for the provision of IP-telephony services, prioritization was carried out in accordance with the IEEE 802.11e specification, with AC_VO priority given to a voice traffic, and AC_BK priority to other data transmitted over the same network. It is mathematically substantiated that if there are stations in the IEEE 802.11ac network transmitting low-priority traffic of the AS_BK class, even under saturated load conditions, the simultaneous operation of a large number of stations transmitting voice traffic is possible. Estimates of the effect of frame sizes of low-priority traffic, as well as the impact of collisions on conditions of voice traffic transmission are obtained. The work uses an original method of studying the conditions of transmission of high-priority traffic in networks with a mixed load. The research results will be useful to specialists in the field of planning and maintenance of IEEE 802.11 wireless networks to ensure high quality indicators of voice services.

Key words: codec; network; prioritization; quality; telephony; voice; wireless.

2 tabl. 5 fig. Ref.: 19 items.

УДК 621.38

Особливості передавання голосового трафіка засобами безпроводових мереж IEEE 802.11ac / *В.С. Лазебний, О.О. Омельянець* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2024. Вип. 216. С. 94 – 102.

Метою дослідження є з'ясувати особливості передавання голосового трафіку для організації послуги IP-телефонії в офісних приміщеннях засобами мережі IEEE 802.11ac, щоб забезпечити якісне надання зазначеної послуги для достатньо великої кількості користувачів навіть за умови інтенсивного передавання змішаного трафіку. Аналітичне дослідження ґрунтується на традиційних ймовірнісних підходах оцінювання експлуатаційних характеристик безпроводових мереж стандарту 802.11. Досліджено мережу 802.11ac з частотною смугою каналу 20 МГц у режимі з одним просторовим потоком. У зазначеній мережі розглянуто сценарій, за якого для надання послуг IP-телефонії здійснено пріоритизацію згідно зі специфікацією IEEE 802.11e з наданням голосовому трафіку пріоритету AC_VO, а іншим даним, що передають тією ж мережею – AC_BK. Математично обґрунтовано, що за наявності в мережі IEEE 802.11ac станцій, що передають низькопріоритетний трафік класу AC_BK навіть за умови насиченого навантаження можливе одночасне функціонування великої кількості станцій, що передають голосовий трафік. Отримано оцінки щодо впливу розмірів кадрів низькопріоритетного трафіку, а також впливу колізій на умови передавання голосового трафіку. В роботі застосовано оригінальний метод дослідження умов передавання високопріоритетного трафіку у мережах зі змішаним навантаженням. Результати досліджень будуть корисними фахівцям у сфері планування і обслуговування безпроводових мереж IEEE 802.11 для забезпечення високих якісних показників голосових послуг

Ключові слова: безпроводовий; голос; кодек; мережа; пріоритезація; телефонія; якість.

Табл. 2. Іл. 5. Бібліогр.: 19 назв.

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

UDC 621.3.082.62

Ways to increase the EMF of semiconductor elements based on thermoelectric effects / *O.V. Miagkyi, R.P. Orel, S.M. Meshkov, V.O. Storozhenko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2024. № 216. P. 103 – 107.

The paper examines the development of the thermovoltaic effect in varizone semiconductor multilayer structures. The effect of the occurrence of electromotive force (EMF) in semiconductor samples without isotype transitions and metal-semiconductor barriers when heated along the sample under the thermovoltaic effect is studied. The possibility of obtaining stable thermally stimulated EMF in semiconductor samples with a heterogeneous composition, in particular in varizone semiconductors when they are heated, is considered. A semiconductor with a heterogeneous composition is simulated, in which the concentration of charge carriers, both electrons and holes, is enough to excite a significant electric current. Cases of both a single varizone semiconductor layer and a combination of several layers under different temperature conditions are considered. Both the definition of the EMF and numerous process characteristics are analyzed. It is confirmed that the appearance of a thermo EMF is caused by the non-equilibrium state and heterogeneity of the environment, as well as its bipolarity. It is shown that in a closed circuit with heterogeneous doping and variable width under uniform heating of the entire circuit, the EFM appears. The equation that determines the EFM ratio in various semiconductors is received. A thermophysical model based on the nonstationary heat equation with boundary conditions of the 2nd and 3rd kind for thermal field calculations is developed. A thermophysical model is created that characterizes a two-layer structure with smoothly changing parameters. The results of the numerical experiment made it possible to obtain the recommended temperature limits for the operation of the considered elements taking into account the SiGe solid solution and to calculate the value of the additional EMF.

Key words: varizone semiconductor; SiGe structure; heterojunction; thermo EMF; Fermi level; thermophysical model; finite difference method.

2 fig. Ref.: 12 items.

УДК 621.3.082.62

Шляхи підвищення ЕРС напівпровідникових елементів на основі термоелектричних ефектів / *О.В. Мягкий, Р.П. Орел, С.М. Мешков, В.О. Стороженко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2024. Вип. 216. С. 103 – 107.

Розглянуто розвиток термовольтаїчного ефекту у варізонних напівпровідникових багатошарових структурах. Досліджено ефект виникнення електрорушійної сили (ЕРС) у напівпровідникових зразках без ізотипних переходів та бар'єрів типу метал-напівпровідник при їх нагріванні вздовж зразка при термовольтаичному ефекті. Розглянуто можливості отримання стабільної термостимульованої ЕРС у напівпровідникових зразках з неоднорідним складом, зокрема у варізонних напівпровідниках при їх нагріванні. Змодельовано напівпровідник з неоднорідним складом, у якому концентрації носіїв заряду – як електронів, так і дірок, достатньо для виникнення відчутного електричного струму за його збудженні. Розглянуто випадки одиничного варізонного шару напівпровідника та комбінації декількох шарів за різних температурних умов. Проаналізовано виникнення ЕРС і кількісні характеристики цього процесу. Підтверджено, що поява термоЕРС обумовлюється нерівноважністю стану та неоднорідністю середовища, а також його біполярністю. Показано, що у замкнутому контурі з неоднорідним легуванням та зі змінною шириною забороненої зони виникає ЕРС в умовах однорідного нагрівання всього контуру. Отримано рівняння, яке описує виникнення ЕРС у варізонних напівпровідниках. Для розрахунку теплового поля побудовано теплофізичну модель на основі нестаціонарного рівняння теплопровідності з граничними умовами 2-го та 3-го роду. Використовувана теплофізична модель характеризує двошарову структуру з параметрами, що плавно змінюються. Результати чисельного експерименту дозволили отримати рекомендовані межі температури до роботи розглянутих елементів з урахуванням твердого розчину SiGe і розраховувати величину додаткової ЕРС.

Ключові слова: варізонний напівпровідник; SiGe структура; гетероперехід; термоЕРС; рівень Фермі; теплофізична модель; метод кінцевих різниць.

Іл. 2. Бібліогр.: 12 назв.

RELATED PROBLEMS OF RADIO ENGINEERING
СУМІЖНІ ПРОБЛЕМИ РАДІОТЕХНІКИ

UDC 528.811 (1-021)

The role of oxygen in the process of modifying the state functionals of wheat seeds and lactobacilli by an electromagnetic field / *O.I. Kovalenko, S.V. Kalinichenko, N.I. Skiyar, S.M. Kulish, V.M. Levchenko, T.I. Antusheva* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2024. № 216. P. 108 – 119.

The possibilities to modify the functional characteristics of wheat seeds and lactobacilli using low-intensity electromagnetic fields (EMF) in frequency ranges associated with gas resonances are considered.

The objective of the work is to study the role of oxygen in the process of modifying the functional indicators of soft wheat seeds and lactobacilli strains state irradiating them with low-intensity EMF on the resonant absorption lines

of oxygen, hydrogen and ozone, additionally enriching water with oxygen during its irradiation and subsequent soaking of seeds in it, and creating conditions for cultivating bacteria in an environment with normal and reduced oxygen content.

To carry out electromagnetic effect, generators G4-141 and G4-142 were used. The enrichment of water with oxygen occurred during its irradiation with EMF, after which wheat seeds were soaked in it. Microaerophilic conditions for the cultivation of bacteria in microanaerostats.

The role of oxygen influence on the vital activity of biological objects of different classes (wheat seeds and lactobacilli) is shown. The possibility of stimulating seed germination by indirect irradiation with oxygen-enriched water at the 61,0 GHz oxygen resonance absorption line with a short exposure of the signal is shown. It has been found that by irradiating lactobacilli in the frequency ranges of 42,2 and 61,0 GHz, they can stimulate their absorption of glucose when cultivated under aerobic conditions, which, in turn, helps to increase the rate of population development. The conditions under which increasing production of high molecular weight peptide fractions (presumably plantaricins) by *L. Plantarum* strain and decreasing the share of low molecular weight proteins in the nutrient medium occur, which indicates, accordingly, an increasing the antagonistic activity of the *L. plantarum* strain and an improvement in its absorption of nutrients, were defined.

The results obtained open up the prospect of using electromagnetic technologies in agriculture when preparing seeds for sowing and in medicine, in particular in the development of new generation drugs based on lactobacilli with increased colonization and antagonistic properties towards pathogens.

Key words: electromagnetic field; oxygen; wheat seeds; lactobacilli; modification; germination energy; enzymatic activity; peptides.

4 tabl. 4 fig. Ref: 19 items.

УДК 528.811 (1-021)

Роль кисню у процесі модифікації функціоналів стану насіння пшениці та лактобактерій електромагнітним полем / *О.І. Коваленко, С.В. Калініченко, Н.І. Скляр, С.М. Куліш, В.Н. Левченко, Т.І. Антушева* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2024. Вип. 216. С. 108 – 119.

Розглянуто можливості за допомогою низькоінтенсивних електромагнітних полів (ЕМП) у частотних діапазонах, що пов'язані із резонансами газів, модифікувати функціональні показники насіння пшениці та лактобактерій.

Мета роботи – дослідити роль кисню в процесі модифікації функціональних показників стану насіння пшениці м'яких сортів і штамів лактобактерій за допомогою їх опромінення низькоінтенсивним ЕМП на лініях резонансного поглинання кисню, водню і озону, при додатковому збагаченні води киснем під час її опромінення й подальшому замочуванні в ній насіння, а також шляхом створення умов культивування бактерій у середовищі з нормальним та зниженим вмістом кисню.

Для проведення електромагнітного впливу використовувалися генератори Г4-141 та Г4-142. Збагачення води киснем відбувалося під час її опромінення ЕМП, після чого в ній замочувалося насіння пшениці. Мікроаерофільні умови культивування бактерій створювалися в мікроанаеростатах.

Показано роль кисню на життєдіяльність біологічних об'єктів різних класів: насіння пшениці та лактобактерій. Показано можливість стимуляції проростання насіння при його опосередкованому через воду, збагачену киснем, опроміненні на лінії резонансного поглинання кисню 61,0 ГГц при нетривалій експозиції сигналу. Встановлено можливість за допомогою опромінення лактобактерій у частотних діапазонах 42,2 та 61,0 ГГц стимулювати засвоєння ними глюкози при культивуванні в аеробних умовах, що, у свою чергу, сприяє збільшенню швидкості розвитку популяції. Відпрацьовано умови, за яких відбувається збільшення продукування штамом *L. plantarum* високомолекулярних пептидних фракцій (імовірно, плантарицинів) та зменшення питомої ваги низькомолекулярних білків живильного середовища, що вказує, відповідно, на збільшення антагоністичної активності штаму *L. plantarum* та покращення засвоєння їм поживних речовин.

Отримані результати відкривають перспективу застосування електромагнітних технологій у сільському господарстві при підготовці насіння до висіву та медицини, зокрема у розробці препаратів нового покоління на основі лактобактерій з підвищеними колонізаційними та антагоністичними властивостями стосовно патогенів.

Ключові слова: електромагнітне поле; кисень; насіння пшениці; лактобактерії; модифікація; енергія проростання; ферментативна активність; пептиди.

Табл. 4. Іл. 4. Бібліогр.: 19 назв.

RADAR AND RADIONAVIGATION
РАДІОЛОКАЦІЯ І РАДІОНАВІГАЦІЯ

UDC 004.89: 621.396

Methods for logical processing of images of radar objects marks based on semantic features / *V. Zhyrnov, S. Solonska* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2024. № 216. P. 120 – 125.

This paper considers a method for logical processing of radar images based on semantic features. Algorithms and programs for automatic detection and recognition of radar aerial objects in surveillance radars with processing of real signals recordings are also given. The relevance of this work is the development of automatic information processing

algorithm to ensure effective detection and recognition of radar object signals based on semantic features. The advantage of this method is the possibility to bring the image processing procedure of radar object images closer to the expert's logic. It implies involvement in analysis of various distinguishing features between reflections from aerial objects. The problem of detecting and recognizing images of radar objects is transformed into the problem of feature classification. Therefore, the essence of logical image processing method based on semantic features is a making decision about detection and recognition of radar objects based on comparative analysis of features, which are defined on the set of semantic, fluctuation, geometric and energy components of radar image. An algorithm for automatic decision-making on detection and recognition of aircraft radar signals, including point-moving and stationary aircraft such as airplanes, helicopters, UAVs, is given. This approach of forming semantic features of radar signals, as well as the automation of information processing operations, increases the effectiveness of detecting weak signals due to accumulation of signal (energy) and logical information. At the same time, logical information is accumulated from the analysis of dynamic map of radar signal intensities with tracking of changes occurring in it during several radar soundings.

Key words: semantic analysis; radar signal; identification; extended atmospheric formations; aerial object.

5 fig. Ref.: 11 items.

УДК 004.89: 621.396

Методи логічної обробки зображень відміток радіолокаційних об'єктів на основі семантичних ознак / *В.В. Жирнов, С.В. Солонська* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2024. Вип. 216. С. 120 – 125.

Наведено результати розробки метода логічної обробки зображень радіолокаційних об'єктів на основі семантичних ознак, створено алгоритми та програми автоматичного виявлення й розпізнавання радіолокаційних повітряних об'єктів в оглядових РЛС з обробкою реальних записів сигналів. Актуальність цих робіт полягає у створенні алгоритмів автоматичної обробки інформації для забезпечення ефективного виявлення й розпізнавання сигналів радіолокаційних об'єктів на основі семантичних ознак. Перевага даного методу пов'язана з можливістю наблизити процедуру обробки зображень радіолокаційних об'єктів до логіки експерта. Характерною особливістю цієї логіки є залучення до аналізу розрізнювальних ознак між зображеннями різних об'єктів. У такому разі проблема виявлення й розпізнавання зображень відміток радіолокаційних об'єктів трансформується у проблему ознакової класифікації. Таким чином метод логічної обробки радіолокаційних зображень на основі семантичних ознак зводиться до прийняття рішення з виявлення та розпізнавання радіолокаційних об'єктів на основі порівняльного аналізу простору семантичних ознак, який задано на множині смислової, процесної, геометричної та енергетичної складових радіолокаційного зображення. Наведено алгоритм автоматичного прийняття рішення з виявлення й розпізнавання радіолокаційних відміток літальних апаратів. Такий підхід до формування семантичних ознак радіолокаційних сигналів, а також автоматизація операцій обробки інформації підвищують ефективність виявлення слабких сигналів завдяки накопиченню сигнальної та логічної інформації. При цьому накопичується логічна інформація з аналізу динамічної карти інтенсивності радіолокаційних сигналів з відстеженням змін, що відбуваються в ній протягом кількох зондувань РЛС.

Ключові слова: семантичний аналіз; радіолокаційний сигнал; ідентифікація; повітряний об'єкт.

Іл. 5. Бібліогр.: 11 назв.

UDC 621.396.4

Research of the angular distribution of errors at different transmission speeds in the decameter range / *V.A. Bulaga* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2024. № 216. P. 126 – 130.

The paper states that the main factors that affect the reduction of bandwidth and reliability of communication channels in the decameter range are multiradiation and the level of interference from transmitters operating at close frequencies. It is known that one of the methods of combating such negative phenomena is the use of phased antenna arrays in communication systems. The paper evaluates the efficiency of the phased antenna system according to the information criterion "error coefficients – elevation angle". The angular distribution of errors at different transmission speeds in the short-wave range when using phased antenna arrays was studied according to the information criterion "error coefficients – angle of position". The results obtained in the work allow us to draw the following conclusions: the possibility of using error detection devices when testing the reliability of communication channels is fully confirmed communication of the decameter range; the use of controlled phased antenna arrays on the receiving side allows to solve a complex of trajectory tasks, and also allows to evaluate the effectiveness of communication systems that use beam distribution at the reception.

Key words: communication channel; decameter range; error; angular distribution; transmission speed; multiradiation; phased array antenna; bandwidth.

4 fig. Ref.: 10 items.

УДК 621.396.4

Дослідження кутового розподілу помилок при різних швидкостях передачі в декаметровому діапазоні / *В.А. Булага* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2024. Вип. 216. С. 126 – 130.

Зазначено, що основними факторами, які впливають на зменшення пропускної спроможності та надійності каналів зв'язку в декаметровому діапазоні, є багатопроменевість і рівень завад від передавачів, що працюють за близькими частотами. Відомо, що одним із способів боротьби з такими негативними явищами є застосування в системах зв'язку фазованих антенних решіток. Проведено оцінку ефективності фазованої антенної системи за

інформаційним критерієм «коефіцієнти помилок – кут місця». Досліджено кутовий розподіл помилок при різних швидкостях передачі в короткохвильовому діапазоні при використання фазованих антенних решіток за інформаційним критерієм «коефіцієнти помилок – кут місця». Отримані результати дозволяють зробити наступні висновки: повною мірою підтверджується можливість використання приладів виявлення похибок при випробуванні надійності каналів зв'язку декаметрового діапазону; застосування керованих фазованих антенних решіток на приймальній стороні дозволяє вирішувати комплекс траєкторних завдань, а також дозволяє дати оцінку ефективності систем зв'язку, що використовують на прийомі розподіл променів.

Ключові слова: канал зв'язку; декаметровий діапазон; помилка; кутовий розподіл; швидкість передачі; багатопроменевість; фазована антенна решітка; пропускна спроможність.

Іл. 4. Бібліогр.: 10 назв.

UDC 621.396.96

Evaluation of the quality of radar information of dependent cooperative surveillance systems / *I.V. Svyd, I.V. Ignatyuk, O.D. Shuniborov, G.V. Maistrenko, M.V. Tulenko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2024. №216. P. 131 – 136.

The work demonstrates that cooperative surveillance systems occupy a significant place in the information support of the airspace control and air traffic control system. The issues of assessing the quality of radar information from dependent cooperative surveillance systems have also been studied. These systems are shown to be promising surveillance systems for air traffic control. Authors' attention is focused on the importance of ensuring the integrity of information of dependent surveillance systems. The objective of this work is to formalize models for assessing the probability of an erroneous alarm and integrity risk. According to the results of the study, it is shown that the difference in the coordinates of two independent measurements of the same aircraft position is greater than some predetermined value, and therefore the quality of the coordinate information of the dependent surveillance system under consideration is unsatisfactory and leads to a warning alarm for the dispatcher. It has been demonstrated that the integrity of the coordinate information of dependent surveillance systems determines the likelihood that information about the coordinates of the aircraft transmitted in messages from dependent surveillance systems and used by the dispatcher for air traffic control purposes does not contain undetected errors exceeding the threshold of the established holding radius.

Key words: radar system; information; estimation; quality; cooperative system; dependent observation; aircraft; signal; detection probability; coordinate information; integrity.

Ref.: 25 items.

УДК 621.396.96

Оцінка якості радіолокаційної інформації систем залежного кооперативного спостереження / *І.В. Свид, І.В. Ігнатюк, О.Д. Шуніборов, Г.В. Майстренко, М.В. Туленко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2024. Вип. 216. С. 131 – 136.

Показано, що залежні кооперативні системи спостереження займають значне місце у інформаційному забезпеченні системи контролю повітряного простору та управління повітряним рухом. Також досліджено питання оцінки якості радіолокаційної інформації систем залежного кооперативного спостереження. Показано, що зазначені системи є перспективними системами спостереження для управління повітряним рухом. Акцентовано увагу на важливості питання забезпечення цілісності інформації залежних систем спостереження. Завданням даної роботи є формалізація моделей оцінки ймовірності помилкової тривоги і ризику цілісності. За результатами дослідження показано, що різниця координат двох незалежних вимірювань одного і того ж положення повітряного судна більше деякої наперед заданої величини, і тому якість координатної інформації залежної системи спостереження є незадовільною та призводить до подання попереджувального сигналу тривоги для диспетчера. Продемонстровано, що цілісність координатної інформації залежних систем спостереження визначає імовірність того, що інформація про координати повітряного судна, що передаються в повідомленнях залежних систем спостереження та використовуються диспетчером в цілях управління повітряним рухом, не містить невиявлених помилок, які перевищують поріг встановленого радіуса утримання.

Ключові слова: радіолокаційна система; інформація; оцінка; якість; кооперативна система; залежне спостереження; повітряне судно; сигнал; ймовірність виявлення; координатна інформація; цілісність.

Бібліогр.: 25 назв.