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 4

Kharkiv
Kharkiv National
University of Radio Electronics
2023

UDC 621.3

The collection is included in the List of scientific professional publications of Ukraine, category «Б», technical and physical-mathematical sciences (approved by orders of the Ministry of Education and Science from 17.03.2020 № 409; from 02.07.2020 № 886; from 24.09.2020 № 1188) by specialties: 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 № 9 dated 29.09.2023.

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

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ
УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ

РАДІОТЕХНІКА

Всеукраїнський
міжвідомчий науково-технічний збірник

ISSN 0485-8972
eISSN 2786-5525

Засновано в 1965 р.

В И П У С К 2 1 4

Харків
Харківський національний
університет радіоелектроніки
2023

УДК 621.3

Збірник включено до Переліку наукових фахових видань України, категорія "Б", технічні та фізико-математичні науки (затверджено наказами МОНУ від 17.03.2020 № 409; від 02.07.2020 № 886; від 24.09.2020 № 1188) за спеціальностями: 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 № 9 від 29.09.2023.

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

CONTENT

SYSTEMS AND METHODS OF INFORMATION PROTECTION

PHYSICS OF DEVICES, ELEMENTS AND SYSTEMS

INFORMATION METHODS OF RADIO ENGINEERING, SIGNAL PROCESSING

APPLICATION OF RADIO TECHNOLOGY METHODS

RADAR AND RADIONAVIGATION

ЗМІСТ

СИСТЕМИ І МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ

ФІЗИКА ПРИЛАДІВ, ЕЛЕМЕНТІВ І СИСТЕМ

ІНФОРМАЦІЙНІ МЕТОДИ РАДІОТЕХНІКИ, ОБРОБКА СИГНАЛІВ

ЗАСТОСУВАННЯ МЕТОДІВ РАДІОТЕХНІКИ

РАДІОЛОКАЦІЯ І РАДІОНАВІГАЦІЯ

УДК 004.056.55 **DOI:10.30837/rt.2023.3.214.01**

С.О. КАНДІЙ, І.Д. ГОРБЕНКО, д-р техн. наук

АНАЛІЗ ДСТУ 8961:2019 У МОДЕЛІ КВАНТОВОГО ВИПАДКОВОГО ОРАКУЛА

Вступ

Особливістю сучасної криптографії є доказова безпека. Для сучасних криптографічних перетворень (за певних модельних припущень) існують формальні докази відсутності ефективних атак за умови складності декількох теоретико-числових проблем [1]. Для схем асиметричного шифрування та механізмів інкапсуляції ключів прикладами таких моделей безпеки є моделі на основі нерозрізнювальності – IND-CPA,IND-CCA1,IND-CCA2 [1].

Моделі на основі нерозрізнювальності є стандартним засобом для отримання формальних доказів безпеки, проте якщо в конструкції використовуються геш-функції, то часто отримати доказ існуючими засобами стає неможливо. Зазвичай, для подолання подібних труднощів використовується модель випадкового оракула [2], у межах якої геш-функції замінюються на ідеалізовані аналоги – випадкові оракули. Хоча така модель і не враховує специфічні атаки, що направлені на структуру геш-функцій, вона є стандартним засобом для оцінки безпеки в сучасній криптографії.

З розвитком квантових комп’ютерів з’явилися нові загрози, які модель випадкового оракула не враховує. Перші спроби побудувати модель квантового випадкового оракула [3] приносили лише обмежений успіх, оскільки звичні техніки доказу переставали працювати. В останні роки з’явилося багато нових технік [4], що дозволяють отримати докази, які раніше неможливо було отримати.

При формальному аналізі механізмів інкапсуляції ключів задача, зазвичай, розбивається на дві підзадачі: аналіз асиметричного перетворення, що лежить в основі, та аналіз перетворення, що робить з асиметричної схеми безпечний механізм інкапсуляції ключів [1]. В літературі було запропоновано багато таких перетворень. Зокрема, варто виділити перетворення Фуджісакі – Окамото [5], перетворення Дента [6], перетворення SXY [7]. Для них можливо знайти в літературі аналіз як у моделі випадкового оракула, так і у моделі квантового випадкового оракула.

Стандарт ДСТУ 8961:2019 [8] визначає асиметричне перетворення та механізм інкапсуляції ключів на основі NTRU [9]. Для отримання механізму інкапсуляції ключів використовується перетворення власної розробки, формального аналізу якого в літературі існує доволі мало. Структурно воно схоже на перетворення SXY, проте має деякі відмінності. У межах роботи будемо називати це перетворення як SkelyaTransform.

Мета роботи – аналіз перетворення SkelyaTransform у моделі квантового випадкового оракула. Наш аналіз ґрунтується на роботах [10], у яких проводився аналіз доволі схожого на SkelyaTransform перетворення.

1. Позначення

Для позначення предикатів використовується нотація $[[\cdot]]$. Якщо b є деяким твердженням, то предикат $[[b]]$ приймає значення 1, якщо b є істинним, та 0 інакше. Якщо змінна x приймає значення детермінованим чином, то використовується знак «=». Якщо змінна x приймає значення з деякого випадкового процесу, то використовується символ «$\leftarrow$». Для визначеної множини X позначення $x \leftarrow X$ означає, що змінна x приймає випадкове значення з рівномірного розподілу над X. Символом «==» позначатимемо перевірку на рівність аргументів. Ймовірність деякої події W надалі позначатимемо символом Pr[W], математичне очікування для деякого розподілу S надалі позначатимемо як E[S]. Для заданої множини X

вираз |X| означає потужність множини. Для числа x вираз |x| означає абсолютне значення. Для заданої схеми асиметричного шифрування MSpace є множиною допустимих повідомлень, RSpace є множиною випадкових значень, CSpace є множиною допустимих шифротекстів, KSpace є множиною ключів.

2. Модель безпеки

Схема асиметричного шифрування є трійкою алгоритмів (Gen,Enc,Dec), де: $Gen:1^{\lambda}\to(pk,sk)$ – поліноміальний ймовірнісний алгоритм генерації ключової пари. Приймає параметр безпеки 1^{λ} та повертає ключову пару (pk,sk), $Enc:(pk,m)\to C$ – поліноміальний ймовірнісний алгоритм шифрування. Приймає публічний ключ pk, повідомлення m та повертає шифротекст C, $Dec:(sk,C)\to\{m,\perp\}$ – детермінований поліноміальний алгоритм розшифрування. Приймає секретний ключ *sk*, шифротекст C та повертає повідомлення m у разі вдалої декапсуляції та символ помилки $\perp$ у разі виникнення помилок.

Алгоритм *Enc* є ймовірнісним, тобто він має деяку внутрішню випадковість *r*. У межах аналізу зручно виносити цю випадковість у аргумент функції і вважати *Enc* детермінованим алгоритмом, що має сигнатуру $Enc:(pk,m,r)\to C$. Цей прийом має назву дерандомізація і широко використовується у формальних доказах.

Схема асиметричного шифрування має властивість відновлення випадковості, якщо існує алгоритм RandomRecovery, що приймає у якості аргументів таємний ключ *sk*, повідомлення m, відповідний шифротекст $c=Enc(pk,m)$ та повертає значення *r*, що використовувалося під час шифрування.

Схема асиметричного шифрування має властивість відновлення повідомлення, якщо існує алгоритм MessageRecovery, що приймає у якості аргументів відкритий ключ *pk*, випадкове значення *r* та шифротекст *c*, що використовує *r* під час шифрування. Алгоритм MessageRecovery повертає повідомлення *m*, що зашифроване у шифротексті *c*, або символ помилки розшифрування, якщо шифротекст є некоректним.

Якщо схема асиметричного шифрування має властивість відновлення випадковості та властивість відновлення повідомлення, то надалі казатимемо, що схема асиметричного шифрування має властивість однозначного відновлення.

Згідно з визначенням [1] протокол інкапсуляції ключів є трійкою алгоритмів (Gen,Encaps,Decaps), де: $Gen:1^{\lambda}\to(pk,sk)$ – поліноміальний ймовірнісний алгоритм генерації ключової пари. Приймає параметр безпеки 1^{λ} та повертає ключову пару (*pk*,*sk*), $Encaps:pk\to(K,C)$ – поліноміальний ймовірнісний алгоритм інкапсуляції ключа. Приймає публічний ключ *pk* і повертає випадковий ключ *K* та його інкапсуляцію (шифротекст) *C*, $Decaps:(sk,C)\to\{K,\perp\}$ – детермінований поліноміальний алгоритм декапсуляції ключа. Приймає секретний ключ *sk* та інкапсуляцію ключа *C* і повертає ключ *K* у разі вдалої декапсуляції та символ помилки $\perp$ у разі виникнення помилок.

Стандартна модель безпеки схем асиметричного шифрування та механізмів інкапсуляції ключів ґрунтується на понятті обчислювальної нерозрізнювальності. Загальний принцип полягає у тому, що якщо для будь-якого ефективного алгоритму неможливо відрізнити шифротекст від випадкового значення при заданих модельних припущеннях, то схема шифрування вважається безпечною у межах цієї моделі.

Реалізується цей принцип через ігри (експерименти) між супротивником (що реалізований довільним набором алгоритмів) та іспитувачем. Іспитувач готує експеримент та викликає алгоритми супротивника, що мають визначений моделлю інтерфейс. Супротивник окрім переданих аргументів може робити запити до оракулів – алгоритмів, про реалізацію яких супротивник нічого не знає. Якщо супротивник A може робити запити до оракула O, то надалі позначатимемо це як A^{O}.

Від схем асиметричного шифрування при побудові механізмів інкапсуляції ключів вимагається безпека у моделі IND-CPA (Indistinguishability under Chosen-Plaintext Attacks) або у моделі OW-CPA (One-Wayness under Chosen-Plaintext Attacks). Відповідні експерименти зображені на рис. 1.

GAME OW-CPA:

1. $(pk, sk) \leftarrow KeyGen(1^{\lambda})$
2. $m^* \leftarrow MSpace$
3. $c^* \leftarrow Enc(pk, m^*)$
4. $m' \leftarrow A(pk, c^*)$
5. $return\ [[m' == m^*]]$

GAME IND-CPA:

1. $(pk, sk) \leftarrow KeyGen(1^{\lambda})$
2. $b \leftarrow \{0,1\}$
3. $(m_0^*, m_1^*) \leftarrow A_1(pk)$
4. $c^* \leftarrow Enc(pk, m_b^*)$
5. $b' \leftarrow A_2(pk, c^*)$
6. $return\ [[b' == b]]$

Рис. 1. Ігри OW-CPA та IND-CPA для схем асиметричного шифрування

Перевагу супротивника А у іграх IND-CPA та OW-CPA для схеми асиметричного шифрування PKE позначимо як $Adv_{PKE}^{OW-CPA}(A)$ та $Adv_{PKE}^{IND-CPA}(A)$ відповідно. Стандартним визначенням для переваги супротивника є:

$$\begin{aligned} Adv_{PKE}^{OW-CPA}(A) &= \Pr[OW-CPA(A) == 1] \\ \mathrm{Adv}_{PKE}^{IND-CPA}(A) &= \left|\Pr[IND-CPA(A) == 1] - \frac{1}{2}\right|. \end{aligned} \tag{1}$$

Від механізмів інкапсуляції ключів зазвичай вимагається безпека у моделі IND-CCA (Indistinguishability under Chosen-Ciphertext Attacks). На рис. 2 зображено гру для IND-CCA.

GAME IND-CCA:

1. $(pk, sk) \leftarrow KeyGen(1^{\lambda})$
2. $b \leftarrow \{0,1\}$
3. $(K_0^*, c^*) \leftarrow Encaps(pk)$
4. $K_1^* \leftarrow KSpace$
5. $b' \leftarrow A^{Decaps}(pk, c^*, K_b^*)$
6. $return\ [[b' == b]]$

$Decaps(c \neq c^*)$:

1. $K = KEM.Decaps(sk, c)$
2. $return\ K$

Рис. 2. Гра IND-CCA для механізмів інкапсуляції ключів

У грі IND-CCA супротивник може звертатися до оракула декапсуляції, який проводить декапсуляцію будь-якої інкапсуляції, окрім завдання, що було видано іспитувачем. Перевага супротивника А визначається наступним чином:

$$\mathrm{Adv}_{KEM}^{IND-CCA}(A) = \left|\Pr[IND-CCA(A) == 1] - \frac{1}{2}\right|. \tag{2}$$

Схема асиметричного шифрування у загальному випадку може мати помилки дешифрування, тобто для деяких правильно обчислених шифротекстів розшифрування може давати неправильний результат. Існують різні підходи до врахування помилок дешифрування. У межах роботи ми будемо слідувати [10]. Для оцінки ймовірності виникнення помилок дешифрування введемо величину

$$\delta_{wc} = \underset{(pk,sk)}{E}\left[\max_{m \in M} \Pr_{c}[Dec(sk, c) \neq m\right]. \tag{3}$$

Величина δ_{wc} характеризує ймовірність появи помилок дешифрування у найгіршому випадку.

Для того щоб схема асиметричного шифрування була безпечною, необхідно, щоб рівень помилок був незначним. Для оцінки складності отримання помилки дешифрування введемо гру COR-RO на рис. 3. У цій грі супротивник має доступ до деякого випадкового оракула G. Задача супротивника полягає у тому, щоб повернути список повідомлень. Якщо хоча б одне повідомлення викликатиме помилку дешифрування, то супротивник перемагає.

Game COR-RO:

1. $(pk, sk) \leftarrow PKE.KeyGen(1^{\lambda})$
2. $L_M \leftarrow A^G(sk, pk)$
3. $for\ m \in L_M$
4. $\quad c \leftarrow Enc(pk, m)$
5. $\quad$ if $Dec(sk, c) \neq m$
6. $\quad\quad$ return 1
7. return 0

Рис. 3. Гра COR-RO для схем асиметричного шифрування

Перевага супротивника A відповідно визначається як

$$Adv_{PKE}^{COR-RO}(A) = \Pr[COR - RO(A) = 1]. \quad (4)$$

У роботі [10] отриманий важливий результат щодо оцінки ймовірності появи помилок дешифрування.

Л е м а 1 . Якщо PKE є δ_{wc}-коректною схемою асиметричного шифрування, тоді для будь-якого супротивника A, що робить q_G квантових запитів до оракула G та повертає одне повідомлення, має місце нерівність

$$Adv_{PKE}^{COR-RO}(A) \leq 8 \cdot (q_G + 1)^2 \cdot \delta_{wc}. \quad (5)$$

Важливою лемою при доказі тверджень у моделях на основі нерозрізнювальності є так звана лема Union Bound.

Л е м а 2 (Union Bound, [6]). Нехай A,B та E – події у деякому просторі ймовірностей. Якщо $\Pr[A|\neg E] = \Pr[B|\neg E]$, то має місце нерівність $|\Pr[A] - \Pr[B]| \leq \Pr[E]$.

3. Перетворення SkelyaTransform

У межах роботи досліджується перетворення SkelyaTransform, яке визначено (у неявному вигляді) стандартом ДСТУ 8961. Наведемо формальний опис цього перетворення для довільної схеми асиметричного шифрування.

Нехай λ – параметр безпеки, PKE=(Gen,Enc,Dec) – деяка схема асиметричного шифрування, що використовує простір повідомлень MSpace, простір шифротекстів CSpace, простір випадковості RSpace і задано геш-функції:

$$H : RSpace \to \{0,1\}^{\lambda}$$
$$BPGM : MSpace \to RSpace. \quad (6)$$
$$KDF : RSpace \to \{0,1\}^{\lambda}$$

Перетворення SkelyaTransform задано наступним чином (рис. 4):

$SkelyaTransform.Gen(1^\lambda)$:	$SkelyaTransform.Encaps(pk)$:	$SkelyaTransform.Decaps(C=(C_1,C_2),sk)$):
1. Return $(pk,sk)=PKE.Gen(1^\lambda)$	1. $m \leftarrow_R M$	1. $m' = PKE.Dec(C_1, sk)$
	2. $r = BPGM(m)$	2. If $m' == \perp$ return $\perp$
	3. $C_1 = PKE.Enc(m, r, pk)$	3. $r' = BPGM(m)$
	4. $C_2 = H(r)$	4. $C_2' = H(r')$
	5. $K = KDF(r)$	5. $C_1' = PKE.Enc(m, r, pk)$
	6. $C = (C_1, C_2)$	6. If $C_1' == C_1 \&\& C_2' == C_2$
	7. return (C, K)	7. return $K = KDF(r)$
		8. return $\perp$

Рис. 4. Перетворення SkelyaTransform для довільної схеми асиметричного шифрування

4. Модель квантового випадкового оракула

Класичний випадковий оракул є функцією $H:\mathrm{X}\to Y$ (де $X=\{0,1\}^m$ та $Y=\{0,1\}^n$ для деяких m,n), яка обрана з рівномірного розподілу над множиною усіх можливих функцій Ω_H [4]. Квантовий випадковий оракул задається наступним оператором:

$$\mathrm{H}^{St}:|x,y\rangle\to|x,y\oplus H(x)\rangle. \tag{7}$$

Модель квантового випадкового оракула передбачає, що кожна геш-функція замінюється на квантовий випадковий оракул. Супротивник А може робити запити у суперпозиції до відповідних оракулів.

У класичній моделі випадкового оракула типовою стратегією доказу є показати, що супротивник А не може відрізнити значення випадкового оракула від випадкового, якщо А не робив раніше відповідного запиту до оракула. Проте, у квантовому випадку цю стратегію важко реалізувати, оскільки А може робити запити в суперпозиції і з деякою незначною ймовірністю отримати відповідне значення. Щоб оцінити ймовірність успіху, А необхідно оцінити наскільки важко витягти цю інформацію з запиту. Одним з перших рішень для цієї проблеми була OW2H Лема. Нижче наведений варіант цієї леми, який є зручним для доказу.

Л е м а 3 (OW2H Лема [10]). Нехай $O:\{0,1\}^n\to\{0,1\}^m$ – квантовий випадковий оракул та А – деякий квантовий алгоритм, що робить не більше q_O квантових запитів до О, який у свою чергу робить не більше $q_{O_1},q_{O_2},...,\mathrm{q}_{O_N}$ запитів до оракулів $O_1,O_2,...,O_N$. Нехай E^A є алгоритмом, що на запит x^* робить наступне: обирає випадковим чином число i з множини $\{1,...,q_O\}$, змінну y з $\{0,1\}^m$ та запускає $A^O(input)$, де $input$ є деякими даними, що отримані з (x^*,y) за допомогою довільного алгоритму $GenInput(x^*,y)$, допоки не відбудеться i-й запит. Після цього алгоритм E^A вимірює аргумент запиту у обчислювальному базисі та повертає результат виміру. Якщо А робить менше i запитів, то E^A повертає $\perp\notin\{0,1\}^n$. Тоді виконується нерівність

$$\begin{aligned}&|\Pr[\mathrm{OW\,2\,H(A)}\Rightarrow 1]-1/2]|\le q_O\cdot\sqrt{p_{FIND}}\Rightarrow\\&|\Pr[\mathrm{OW\,2\,H(A)}\Rightarrow 1\,|\,b=0]-\Pr[\mathrm{OW\,2\,H(A)}\Rightarrow 1\,|\,b=1]|\le 2q_O\cdot\sqrt{p_{FIND}},\end{aligned} \tag{8}$$

де гра OW2H визначена на рис. 5 та

$$p_{FIND}=\Pr[x'=x^*], \tag{9}$$

де ймовірність взята над усіма можливими значеннями $x^*\leftarrow\{0,1\}^n, x'\leftarrow E^A(x^*)$.

Game $OW2H$:

1. $x^* \leftarrow \{0,1\}^n$
2. $y_0^* = O(x), y_1^* \leftarrow \{0,1\}^m$
3. $b \leftarrow \{0,1\}$
4. $b' \leftarrow A^O(x^*, y_b^*)$
5. $return\ [[b' == b]]$

Рис. 5. Гра OW2H

5. Аналіз перетворення SkelyaTransform

Основний результат цієї роботи сформульовано в теоремі 1.

Т е о р е м а 1 . Нехай PKE є OW-CPA безпечною та δ_{wc}-коректною схемою асиметричного шифрування з властивістю однозначного відновлення, тоді SkelyaTransfom[PKE] є IND-CCA безпечним механізмом інкапсуляції ключів. Більш формально – для кожного квантового алгоритму A у грі IND-CCA проти KEM=SkelyaTransform[PKE], що робить $q_H, q_{BPGM}, q_{KDF}, q_D$ запитів до оракулів H,BPGM,KDF та оракула дешифрування, існує квантовий алгоритм B у грі OW-CPA проти схеми асиметричного шифрування PKE, для якого виконується нерівність

$$Adv_{KEM}^{IND-CCA}(A) \le (2 \cdot q_H + 2 \cdot q_D + q_{KDF}) \cdot \sqrt{Adv_{PKE}^{OW-CPA}(B)} + 8 \cdot (q_{BPGM} + q_D + 1)^2 \cdot \delta_{wc} \quad (10)$$

Д о к а з .

Перед тим, як перейти безпосередньо до доказу, розглянемо загальну структуру доказу. Для доказу використовується стандартна техніка “game hopping”. Для того щоб довести нерівність (10), розглядається серія ігор GAME0 – GAME6. Гра GAME0 відтворює гру IND-CCA. Кожна наступна гра спрощується у тому сенсі, що значення змінних замінюються на дійсно випадкові або змінна взагалі виводиться з використання. При цьому фіксується зміна переваги супротивника. Цей процес відбувається до тих пір, допоки не буде простого способу оцінити ймовірність перемоги супротивника у поточній грі.

Гра GAME0 зображена на рис. 6.

$GAME0$:

1. $(pk, sk) \leftarrow PKE.KeyGen(1^\lambda)$
2. $b \leftarrow \{0,1\}$
3. $m^* \leftarrow \{0,1\}^n$
4. $r^* = BPGM(m^*)$
5. $c_0^* \leftarrow PKE.Enc(pk, m^*, r^*)$
6. $K_0^* = KDF(r^*); K_1^* \leftarrow \{0,1\}^n$
7. $K^* = K_b^*$
8. $c_1^* = H(r^*)$
9. $b' \leftarrow A^{Decaps}(pk, c^* = (c_0^*, c_1^*), K^*)$
10. $return\ [[b' == b]]$

$Decaps((c_0, c_1) \neq (c_0^*, c_1^*))$:

1. $m' = PKE.Dec(c_0, sk)$
2. $if\ m' == \perp$
3. $\quad return\ \perp$
4. $r' = BPGM(m')$
5. $c_1' = H(r')$
6. $if\ C_0 == PKE.Enc(m', r', pk)\ \&\&\ c_1 == c_1'$
7. $\quad return\ K = KDF(r')$
8. $return\ \perp$

Рис. 6. Гра GAME0

Ця гра в точності повторює IND-CCA гру для SkelyaTransfom[PKE], тому має місце рівність

$$Adv_{KEM}^{IND-CCA}(A) = |\Pr[GAME0(A) = 1] - 1/2|.$$

У грі GAME1 замість використання оракула BPGM генеруватимемо випадкове значення r^*. В оракулі декапсуляції відповідно замість BPGM використовуватимемо функцію RandomRecovery:

$GAME1$:

1. $(pk, sk) \leftarrow PKE.KeyGen(1^{\lambda})$
2. $b \leftarrow \{0,1\}$
3. $m^* \leftarrow \{0,1\}^n$
4. $r^* \leftarrow \{0,1\}^n$
5. $c_0^* \leftarrow PKE.Enc(pk, m^*, r^*)$
6. $K_0^* = KDF(r^*); K_1^* \leftarrow \{0,1\}^n$
7. $K^* = K_b^*$
8. $c_1^* = H(r^*)$
9. $b' \leftarrow A^{Decaps}(pk, c^* = (c_0^*, c_1^*), K^*)$
10. $return\ [[b' == b]]$

$Decaps\big((c_0, c_1) \neq (c_0^*, c_1^*)\big)$:

1. $m' = PKE.Dec(c_0, sk)$
2. $if\ m' == \perp$
3. $\quad return\ \perp$
4. $r' = RandomRecovery(m', c_0)$
5. $c_1' = H(r')$
6. $if\ c_0 == PKE.Enc(m', r', pk)\ \&\&\ c_1 == c_1'$
7. $\quad return\ K = KDF(r')$
8. $return\ \perp$

Рис. 7. Гра GAME1

Розглянемо наскільки зміниться перевага супротивника при переході від гри GAME0 до GAME1. Позначимо як $DIFF$ подію, яка полягає у тому, що супротивник зможе відрізнити ігри GAME0 та GAME1. З Леми 2 маємо:

$$|\Pr[GAME0(A)=1]-\Pr[GAME1(A)=1]|\le \Pr[DIFF]$$

$$|\Pr[GAME0(A)=1]-1/2-\Pr[GAME1(A)=1]+1/2|\le \Pr[DIFF]$$

$$|\Pr[GAME0(A)=1]-1/2|-|\Pr[GAME1(A)=1]-1/2|\le \Pr[DIFF]$$

$$Adv_{KEM}^{IND-CCA}(A) \le Adv_{KEM}^{GAME1}(A)+\Pr[DIFF]$$

Різниця між іграми буде помітна якщо супротивник зможе знайти повідомлення, яке викликає помилку дешифрування. Тобто, якщо супротивник А сформує запит $(c_0 = PKE.\mathrm{Enc}(\mathrm{pk}, \mathrm{m}, \mathrm{BPGM}(\mathrm{m})), c_1)$, для якого $PKE.Dec(sk, c_0) \neq m$. Тоді можливо побудувати супротивника D у грі COR-RO, що ідеально симулює середовище для супротивника А. Супротивник D симулює гру IND-CCA та усі оракули для А, використовуючи алгоритм гри GAME1, та записує усі запити А до оракулів BPGM та оракула дешифрування. Для супротивника А симуляція буде ідеальною, поки не станеться подія $DIFF$. Застосовуючи Лему 1 та Лему 2, отримуємо, що ймовірність події обмежена $8\cdot(q_{BPGM}+q_D+1)^2\cdot\delta_{wc}$. Отже, маємо:

$$\mathrm{Adv}_{KEM}^{IND-CCA}(A) \le Adv_{KEM}^{GAME1}(A)+8\cdot(q_{BPGM}+q_D+1)^2\cdot\delta_{wc}.$$

У грі GAME2 замінимо K^* та c_1^* на дійсно випадкові значення:

$GAME2$:

1. $(pk, sk) \leftarrow PKE.KeyGen(1^{\lambda})$
2. $m^* \leftarrow \{0,1\}^n$
3. $r^* \leftarrow \{0,1\}^n$
4. $c_0^* \leftarrow PKE.Enc(pk, m^*, r^*)$
5. $K^* \leftarrow \{0,1\}^n$
6. $c_1^* \leftarrow \{0,1\}^n$
7. $b' \leftarrow A^{Decaps}(pk, c^* = (c_0^*, c_1^*), K^*)$
8. $return\ [[b' == b]]$

$Decaps\big((c_0, c_1) \neq (c_0^*, c_1^*)\big)$:

1. $m' = PKE.Dec(c_0, sk)$
2. $if\ m' == \perp$
3. $\quad return\ \perp$
4. $r' = RandomRecovery(m', c_0)$
5. $c_1' = H(r')$
6. $if\ c_0 == PKE.Enc(m', r', pk)\ \&\&\ c_1 == c_1'$
7. $\quad return\ K = KDF(r')$
8. $return\ \perp$

Рис. 7. Гра GAME2

Застосовуючи визначення переваги супротивника, отримуємо вираз

$$Adv_{KEM}^{IND-CCA}(A) \le \frac{1}{2}\cdot|\Pr[GAME1(A)=1|b=0]-$$
$$-\Pr[GAME1(A)=1|b=0]|+8\cdot(q_{BPGM}+q_D+1)^2\cdot\delta_{wc}$$
$$Adv_{KEM}^{IND-CCA}(A) \le 8\cdot(q_{BPGM}+q_D+1)^2\cdot\delta_{wc}+ \quad \cdot$$
$$+\frac{1}{2}\cdot|\Pr[GAME1(A)=1|b=0]-\Pr[\text{GAME 2(A)}=1]$$
$$+\Pr[\text{GAME 2(A)}=1]-\Pr[GAME1(A)=1|b=0]|$$

Звідки витікає

$$Adv_{KEM}^{IND-CCA}(A) \le 8\cdot(q_{BPGM}+q_D+1)^2\cdot\delta_{wc}+$$
$$\frac{1}{2}\cdot|\Pr[GAME1(A)=1|b=0]-\Pr[\text{GAME 2(A)}=1]|+\cdot$$
$$\frac{1}{2}\cdot|\Pr[\text{GAME 2(A)}=1]-\Pr[GAME1(A)=1|b=0]|$$

Для оцінки значень $|\Pr[GAME1(A)=1|b=0]-\Pr[\text{GAME 2(A)}=1]|$ та $|\Pr[\text{GAME 2(A)}=1]-\Pr[GAME1(A)=1|b=0]|$ можна застосувати лему OW2H. Якщо покласти $O(\cdot)=H(\cdot)$, то гра OW2H буде ідентичною до гри GAME1, за умови, що b=1 і до GAME2 якщо y є випадковим. Аналогічно, якщо покласти $O(\cdot)=H(\cdot)\times KDF(\cdot)$, то гра OW2H буде ідентичною до гри GAME1, за умови, що b=0 і до GAME2 якщо y є випадковим. З Леми 3 маємо нерівності:

$$|\Pr[GAME1(A)=1|b=0]-\Pr[GAME2(A)=1]|\le 2\cdot(q_{KDF}+q_H)\cdot\sqrt{\Pr[GAME3(A)=1]}$$
$$|\Pr[GAME1(A)=1|b=1]-\Pr[GAME2(A)=1]|\le 2\cdot(q_{KDF}+q_H+q_{KDF})\cdot\sqrt{\Pr[GAME4(A)=1]},$$

де GAME3, GAME4 зображені на рис. 9, де позначення E^A позначає запуск алгоритму A до тих пір, доки не буде обрано випадково чергу з запитів до відповідних геш-функцій, над якою потім робиться вимір для того, щоб отримати повідомлення m', відповідно до формулювання леми 3.

Для того щоб оцінити ймовірність успіху супротивника, у іграх GAME3, GAME4 змінимо оракул декапсуляції таким чином, щоб він не використовував секретний ключ, а відповідні ігри, що використовують змінений оракул декапсуляції, позначимо як GAME5,GAME6. При побудові нового оракула декапсуляції NewDecaps використаємо той факт, що квантовий випадковий оракул, до якого робиться q запитів, є невідрізнимим від випадкового полінома степені $2q$ над відповідним полем Галуа [10]. Відповідно, множина усіх значень r, для яких H(r)=d, може бути розглянута як множина коренів полінома H(X)-d. Новий оракул декапсуляції NewDecaps представлений на рис. 8. Замість таємного ключа для розшифрування повідомлення використовується множина значень r, що були вже запитані у оракула H.

Розглянемо як зміниться перевага супротивника від GAME3 до GAME5 та від GAME4 до GAME6. Нехай супротивник A робить запит до оракула декапсуляції з деяким шифротекстом $(c_0,c_1)\neq(c_0^*,c_1^*)$. Оракул декапсуляції Decaps для цього шифротексту може повернути ключ декапсуляції або символ помилки декапсуляції $\perp$.

Припустимо, що Decaps повертає $\perp$ для шифротексту (c_0,c_1), тоді, якщо NewDecaps не повертає $\perp$ у іграх GAME5-GAME6, то існує значення r для якого виконується $H(r)=c_1$.

Різниця між іграми буде, якщо для c_0, r існує повідомлення m, для якого $m = MessageRecovery(c_0, r) \neq \perp$. Проте, якщо таке m існує, то Decaps не буде повертати $\perp$, маємо протиріччя. Отже, таких m не існує і ігри в цьому випадку є такими, що не відрізняються.

$NewDecaps\big((c_0, c_1) \neq (c_0^*, c_1^*)\big)$:

1. if $\exists r \in Roots(H(X) - c_1) : PKE.Dec(sk, c_0) = m$
2. return $K = KDF(r)$
3. return $\perp$

Рис. 8. Оракул декапсуляції NewDecaps

GAME3:

1. $(pk, sk) \leftarrow KeyGen(1^\lambda)$
2. $m^* \leftarrow \{0,1\}^n$
3. $r^* \leftarrow \{0,1\}^n$
4. $K^* \leftarrow \{0,1\}^n$
5. $c_1^* \leftarrow \{0,1\}^n$
6. $c_0^* \leftarrow Enc(pk, m^*, r^*)$
7. $m' \leftarrow E^{A,H}(pk, (c_0^*, c_1^*), K^*)$
8. $return\ [[m' == m^*]]$

GAME4:

1. $(pk, sk) \leftarrow KeyGen(1^\lambda)$
2. $m^* \leftarrow \{0,1\}^n$
3. $r^* \leftarrow \{0,1\}^n$
4. $K^* \leftarrow \{0,1\}^n$
5. $c_1^* \leftarrow \{0,1\}^n$
6. $c_0^* \leftarrow Enc(pk, m^*, r^*)$
7. $m' \leftarrow E^{A,H,KDF}(pk, (c_0^*, c_1^*), K^*)$
8. $return\ [[m' == m^*]]$

$Decaps\big((c_0, c_1) \neq (c_0^*, c_1^*)\big)$:

1. $m' = PKE.Dec(c_0, sk)$
2. $if\ m' == \perp$
3. $\quad return\ \perp$
4. $r' = RandomRecovery(m', c_0)$
5. $c_1' = H(r')$
6. $if\ c_0 == PKE.Enc(m', r', pk)\ \&\&\ c_1 == c_1'$
7. $\quad return\ K = KDF(r')$
8. $return\ \perp$

Рис. 9. Ігри GAME3-GAME4

Припустимо, що Decaps не повертає $\perp$. Тоді існує деяке *r*, що є коренем H і NewDecaps повертає $K = KDF(r)$. Ігри і в цьому випадку є невідрізнимими і має місце рівність

$$\Pr[GAME3(A) = 1] = \Pr[GAME5(A) = 1]$$
$$\Pr[GAME4(A) = 1] = \Pr[GAME6(A) = 1].$$

Тож, задача звелася до оцінки складності ігор GAME5, GAME6. Для кожної з ігор можливо побудувати супротивників B_1, B_2 у грі OW-CPA проти PKE, які є обгорткою над A. Супротивник B_i симулює середовище для A наступним чином:

- Генерує випадкові значення K^* та c_1^*.
- Викликає $E^{A,Oracles}(pk, (c^*, c_1^*), K^*)$, де $Oracles = H$ для i=1 і Oracles=H,KDF для i=0.
- Повертає будь-що, що поверне $A^{E,Oracles}$.

Зрозуміло, що:

$$Adv_{PKE}^{OW-CPA}(B_1) = Adv_{KEM}^{GAME5}(A), Adv_{PKE}^{OW-CPA}(B_2) = Adv_{KEM}^{GAME6}(A)$$

Нехай супротивник B у грі OW-CPA проти PKE паралельно викликає B_1, B_2 для OW-CPA проти PKE. Зрозуміло, що $Adv_{PKE}^{OW-CPA}(B) = \min(Adv_{PKE}^{OW-CPA}(B_1), Adv_{PKE}^{OW-CPA}(B_2))$. Поєднуючи формули, маємо результат:

$$Adv_{KEM}^{IND-CCA}(A) \le (2 \cdot q_H + 2 \cdot q_D + q_{KDF}) \cdot \sqrt{Adv_{PKE}^{OW-CPA}(B)} + 8 \cdot (q_{BPGM} + q_D + 1)^2 \cdot \delta_{wc}$$

Що і треба було довести.

Висновки

У роботі отримано оцінки IND-CCA безпеки перетворення SkelyaTransform у моделі квантового випадкового оракула для довільних схем асиметричного шифрування з врахуванням помилок дешифрування, що мають властивість однозначного відновлення. На нашу думку, робота дозволить краще розуміти захищеність стандарту ДСТУ 8961:2019 від квантових атак. Головним недоліком нашого доказу є вимога властивості однозначного відновлення у схеми асиметричного шифрування. Така властивість виконується для переважної кількості реальних схем асиметричного шифрування, проте ця вимога є нестандартною. З іншої сторони, інші роботи, що присвячені аналізу асиметричних перетворень, також часто використовують схожу нотацію та додаткові нестандартні вимоги. Для складних перетворень, особливо у межах моделі квантового випадкового оракула, існує доволі мало результатів, що не використовують додаткових припущень щодо схем асиметричного шифрування. Тож, на нашу думку, отриманий результат є суттєвим для оцінки та розуміння безпеки діючого стандарту ДСТУ 8961:2019.

Список літератури

1. Горбенко І. Д., Горбенко Ю. І. Прикладна криптологія. Теорія. Практика. Застосування : монографія. Харків : Форт, 2012. 880 с.
2. Bellare S., Rogaway P. Random oracles are practical: a paradigm for designing eifficient protocols. ACM 1993
3. Boneh D., Dagdelen Ö., Fischlin M., Lehmann A., Schaffner C., Zhandry M. Random oracles in a quantum world // ASIACRYPT 2011. P. 41–69
4. Zhandry M. How to record quantum queries, and applications to quantum indifferentiability // CRYPTO 2019. P. 239–268.
5. Hofheinz D., Hovelmanns K., Kiltz E. A modular analysis of the fujisaki-okamoto transformation // Lecture Notes in Computer Science. 2017. Vol. 10677. P. 341–371.
6. Dent A. A Designer's Guide to KEMs. Cryptography and Coding. Cryptography and Coding, 2003. Vol 28. P. 29-56.
7. Saito T., Xagawa K., Yamakawa T. Tightly-Secure Key-Encapsulation Mechanism in the Quantum Random Oracle Model // EUROCRYPT 2018 . EUROCRYPT 2018. https://doi.org/10.1007/978-3-319-78372-7_17
8. ДСТУ 8961:2019. Інформаційні технології. Криптографічний захист інформації. Алгоритми асиметричного шифрування та інкапсуляції ключів. Чинний від 21.12.2019. Вид. офіц. Київ : УкрНДНЦ, 2019. 72 с.
9. Hoffstein J., Pipher J., Silverman H. NTRU: a ring based public key cryptosystem // Algorithmic Nuber Theory. Third International Symposium. 1998. P. 267–288.
10. Bindel N., Hamburg M., Hövelmanns K., Hülsing A., Persichetti E. Tighter proofs of CCA security in the quantum random oracle model // Dennis Hofheinz and Alon Rosen, editors. TCC 2019. P. 61–90.
11. Don J., Fehr S., Majenz C., Schaffner C. Online-Extractability in the Quantum Random-Oracle Model // EUROCRYPT 2022.

Надійшла до редколегії 08.08.2023

Відомості про авторів:

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», молодший науковий співробітник, Україна; e-mail: sergeykandy@gmail.com; ORCID: https://orcid.org/0000-0003-0552-8341

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, головний конструктор АТ «Інститут інформаційних технологій»; Україна; e-mail: GorbenkoI@iit.kharkov.ua; ORCID: https://orcid.org/0000-0003-4616-3449

УДК 004.056.5 **DOI:10.30837/rt.2023.3.214.02**

М. О. БОДНЯ, М. В. ЄСІНА, канд. техн. наук, В. А. ПОНОМАР, канд. техн. наук

ОСНОВНІ ОСОБЛИВОСТІ ІНФРАСТРУКТУРИ ВІДКРИТИХ КЛЮЧІВ

Вступ

На сьогодні широко застосуються засоби мережевої інфраструктури та інформаційно-комунікаційні системи для організації спілкування та обміну даними між користувачами. Внаслідок цього виникло питання – як забезпечити автентифікацію всіх авторизованих користувачів. Сучасні криптографічні протоколи автентифікації базуються на криптографії з відкритим ключем. Системи захисту інформації та технічні засоби захисту не можуть повністю гарантувати запобігання несанкціонованому доступу до каналу зв'язку, внаслідок цього реалізовуються різноманітні протоколи та системи автентифікації, що ґрунтуються на асиметричній криптографії. Застосування технологій та процедур, що засновані на криптографії з відкритим ключем, широко впроваджуються в системи комерційних організацій та урядових установ, тому що вони забезпечують надійний механізм, який дозволяє підтвердити, що особа є тим, за кого себе видає, та реалізувати конфіденційність, цілісність, неспростовність та автентичність інформації.

Як показує практика, застосування асиметричної криптографії є недостатнім комплексом методів та технологій для забезпечення процедури достовірної автентифікації та обміну інформацією між авторизованими користувачами. Суб'єкти комунікації гіпотетично можуть використовувати паперові документи, які містять персональні дані та відкриті ключі авторизованих користувачів, підписані рукописним підписом та завірені нотаріусом. Але в такому випадку виникає проблема масштабності: проведення нотаріального завірення документів для великої множини суб'єктів спілкування потребує великої кількості аркушів паперу та займає багато часу. Інфраструктура відкритих ключів (ІВК) є надійним інструментом для розв'язання задач, пов'язаних з автентифікацією користувачів та визначенням легітимності, справжності відкритих ключів користувачів у цифровому середовищі.

Структура ІВК складається зі спеціалізованих компонентів, кожен з яких має власний напрям діяльності та фіксований спектр задач. При цьому забезпечуються всі процеси відносно управління цифровими сертифікатами, які включають: видачу, перевипуск, відкликання сертифікатів, управління життєвим циклом та ключами сертифікатів тощо. Такі сертифікати підтверджують факт належності певного відкритого ключа конкретному суб'єкту та наявності у відповідного суб'єкта секретного ключа. Завдяки цифровим сертифікатам всі сторони можуть ідентифікувати один одного та безпечно обмінюватись інформацією через мережу. Фальсифікувати облікові дані цифрового сертифіката, видані центром сертифікації, дуже важко, адже цифровий сертифікат підписується особистим ключем центру сертифікації, який відомий лише йому. Цифровий підпис забезпечує цілісність, автентичність та неспростовність відповідного сертифікату.

ІВК є комплексною системою, яка має раціональну структуру та широкий набір функцій, які спрощують процедуру автентифікації та забезпечують її справжність на підставі цифрових сертифікатів. Суб'єкти комунікації можуть повністю не довіряти один одному, але довіряти третій незалежній стороні, яка регулює механізм встановлення довіри між ними. Цей механізм базується на використанні цифрових сертифікатів і криптографії з відкритим ключем та є важливим елементом для забезпечення безпеки та конфіденційності інформації в Інтернеті та інших цифрових середовищах.

ІВК широко застосовується для проведення безпечних електронних транзакцій, банківських операцій, цифровізації та трансформації уряду, державних установ та організацій задля підвищення рівня якості надання послуг та організації комунікації між суспільством та державними органами. Міжнародна спільнота розгортає та модернізує ІВК у вигляді надійного механізму для забезпечення процесу обміну інформацією та комунікації.

Мета статі - аналіз можливих зовнішніх загроз сторонам комунікації в інформаційному просторі, методології їх виявлення та захисту за допомогою ІВК, концепції ІВК, дослідження компонентів ІВК, методів та апаратних засобів захисту інформації, які застосовуються в парадигмі ІВК.

1. Зовнішні загрози та методи їх вирішення за допомогою використання ІВК

1.1. Атака «людина посередині»

Атака «людина посередині» – це тип кібератаки, при якій зловмисник прослуховує та перехоплює інформацію суб'єктів комунікації, через отримання несанкційованого доступу до каналу зв'язку. Зловмисник симулює себе як суб'єкта комунікації та шляхом маніпуляцій нав'язує власний відкритий ключ сторонам комунікації. Всі сторони вважають, що вони здійснюють обмін інформацією один з одним, але насправді весь потік інформації проходить через зловмисника, який може вносити зміни та пересилати викривлену інформацію з метою обману. При передачі відкритого ключа від одного суб'єкта до іншого, зловмисник може перехопити відкритий ключ отримувача та надіслати власний відкритий ключ адресанту, як наслідок він зможе розшифрувати шифртекст власним особистим ключем та отримати доступ до інформації.

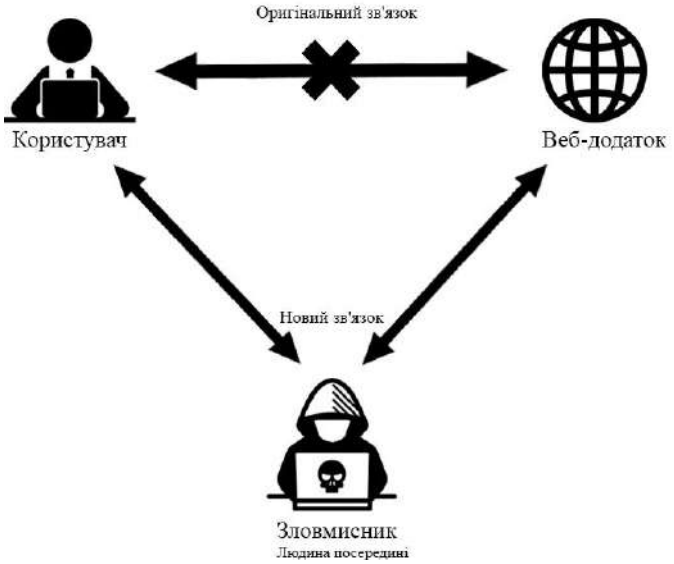


Рис. 1. Модель атаки «людина посередині»

Кібератака «людина посередині» представляє вагому загрозу для користувачів, адже сторони комунікації навіть не підозрюють, що їх прослуховує зловмисник. Механізм управління відкритими ключами ІВК дозволяє захиститися від атаки «людина посередині». Зловмисник може непомітно підмінити відкритий ключ сторони комунікації на свій відкритий ключ [1]. Ця проблема вирішується за допомогою цифрових сертифікатів. Кожна сторона має цифровий сертифікат, у якому наведено основні відомості про сторону та її відкритий ключ. Цифровий сертифікат підписується цифровим підписом центру сертифікації для забезпечення цілісності та справжності документа. Внаслідок цього одна сторона може однозначно ідентифікувати та автентифікувати іншу сторону, перевірити сертифікат на справжність відкритим ключем центру сертифікації та на основі цього вибудовувати довірчі відносини. ІВК допомагає виявити атаку типу «людина посередині». У разі виявлення кібератаки рекомендується використовувати альтернативний канал зв'язку для продовження комунікації. ІВК сприяє встановленню ланцюжка довіри між суб'єктами комунікації. Людина посередині не зможе сформувати цифровий сертифікат для заміни або підробки вихідного сертифіката, оскільки він не має відповідного особистого ключа для створення справжніх сертифіка-

тів. Крім того, зловмисник не зможе представитися однією з легітимних сторін, оскільки він не має доступу до їх особистих ключів. При передачі пакетів через мережу рекомендується використовувати цифровий підпис для забезпечення цілісності та автентичності даних. Якщо підпис перевіряється успішно, це свідчить про те, що переданий пакет не був модифікований.

1.2. Негативні аспекти самопідписаних сертифікатів, фальсифікація цифрових сертифікатів, компрометація особистого ключа

Самопідписаний сертифікат підписується не центром сертифікації, а самим суб'єктом, з використанням особистого ключа. Кожна зацікавлена сторона може перевірити справжність цифрового підпису за допомогою відкритого ключа підписника. Самопідписані сертифікати мають ряд обмежень та недоліків:

1. Відсутність довіри: сертифікат підписується суб'єктом, а не незалежним уповноваженим органом, тому немає гарантії, що сертифікат справжній, дійсний та належить очікуваному власнику.

2. Обмежена сфера застосування: більшість веб-браузерів і програм, які сприймають та довіряють цифровим сертифікатам не допускають самопідписані сертифікати придатними для використання в захищених з'єднаннях по протоколу безпечної передачі даних HTTPS.

3. Ризик безпеки: якщо зловмисник отримає доступ до секретного ключа, він матиме можливість видавати власні сертифікати за сертифікати очікуваного суб'єкта, що несе потенційну загрозу для конфіденційності інформації.

Недоліки самопідписаних сертифікатів доводять їх малоефективність, цим документам не можна повністю довіряти внаслідок відсутності стовідсоткової гарантії їх справжності. Зловмисник може використовувати самопідписані сертифікати, щоб імітувати себе як легітимну сторону. Рекомендується використовувати цифрові сертифікати, сформовані та підписані центром сертифікації, вони гарантують високий рівень довіри та безпеки. Реалізувати фальсифікацію цифрових сертифікатів виданих центром сертифікації дуже складно, бо вони підписані особистим ключем центру сертифікації. Сертифікат вказує на те, що суб'єкт володіє відкритим та особистим ключами, а також надає основні відомості про власника сертифіката. Цифровий підпис центру сертифікації гарантує цілісність, автентичність та справжність цифрового сертифіката.

Фальсифікація цифрових сертифікатів – це створення та використання сфабрикованих сертифікатів для представлення себе як легітимної сторони. Такі сертифікати можуть становити серйозну загрозу для конфіденційності та безпеки інформації. Зловмисники застосовують фальсифіковані сертифікати для кібератаки типу «людина посередині», перехоплення сертифікати, видані центром сертифікації, а також регулярно оновлювати сертифікати.даних, підміни ключів, шахрайства та інших видів атак, підмінюючи свою легітимність. Для запобігання подібним загрозам необхідно перевіряти ланцюжки довіри, використовувати

Компрометація особистого ключа означає, що зловмисник отримав несанкціонований доступ до особистого ключа, який використовується в криптографічних операціях. Коли зловмисник отримує доступ до особистого ключа, він може використовувати його для розшифрування зашифрованих даних, підпису повідомлень та документів від імені власника ключа, а також для інших махінацій. Зловмисник може видавати себе за власника особистого ключа та легітимну сторону, маючи доступ до особистого ключа. Для запобігання загрозі несанкціонованого доступу до особистого ключа неавторизованими користувачами, власнику особистого ключа потрібно використовувати захищені апаратні модулі, сховища та електронні пристрої, які містять блоки пам'яті для зберігання інформації. В ІВК передбачена процедура відкликання сертифікатів, якщо користувач втратив особистий ключ. Відкликання сертифіката автоматично зробить його недійсним, а також не придатним для побудови ланцюжка довіри. Механізм ІВК побудований таким чином, що виключається ймовірність підробки сертифіката або використання зловмисником сертифіката іншого суб'єкта.

2. Концепція ІВК та її компоненти

Інфраструктура відкритих ключів (ІВК) – сукупність процедур, методів, людського контингенту, програмного та апаратного забезпечення, які формують загальну систему, яка підтримує застосування криптографії з відкритим ключем для забезпечення безпеки комунікації. ІВК реалізує механізм, який включає комплекс процедур, алгоритмів, процесів та систему надання послуг. Для створення безпечного простору, в якому суб'єкти можуть в спрощеному порядку ідентифікувати один одного та обмінюватися інформацією між собою. ІВК являє собою надійну структуру третьої незалежної сторони, яка називається центром сертифікації [2]. ІВК складається з профільованих служб та матеріальних компонентів, які взаємодіють між собою та з користувачами або потенційними клієнтами. Всі складові ІВК функціонують та діють відповідно до регламенту системи. Механізм ІВК дозволяє регулювати управління відкритими ключами, цифровими сертифікатами та сприяє зменшенню кількості випадків фальсифікації сертифікатів. Методологія ІВК відносно створення, видачі та відкликання цифрових сертифікатів побудована таким чином, щоб мінімізувати ризики безпеки. ІВК є багатогранною структурою, яка охоплює не лише різноманітні інформаційні технології та електронні пристрої. Вона включає [3]: центр реєстрації, центр сертифікації, стратегії та підходи до забезпечення безпеки, системи поширення та зберігання цифрових сертифікатів, додатки та програми, які підтримують ІВК.

Рис. 2. Компоненти інфраструктури відкритих ключів

До складових ІВК відносяться наступні елементи:

1. Центр сертифікації (ЦС) – ключовий компонент ІВК, який відповідає за видання, керування та валідацію цифрових сертифікатів. ЦС може формувати цифрові сертифікати для кінцевих користувачів та підлеглих ЦС. ЦС є невід'ємною складовою ІВК, яка асоціюється з арбітром, якому повністю довіряють учасники комунікації. Основною метою ЦС є валідація та автентифікація різних сутностей [4], таких як веб-сайти, домени, сервери, організації або фізичні особи для забезпечення їхньої легітимності та безпеки. ЦС проводить перевірку ідентичності суб'єктів та сутностей, які подають запит на видачу сертифікатів. В ІВК, де присутній реєстраційний центр, саме він відповідає за перевірку ідентичності суб'єктів та сутностей, які подають запит на видачу сертифікатів. Після успішної перевірки ідентичності суб'єкта ЦС видає цифровий сертифікат, який містить відкритий ключ та інформацію про його власника. ЦС має наступні функції:

- створює, видає та перевидає цифрові сертифікати;
- здійснює управління цифровими сертифікатами: веде реєстр сертифікатів, відповідає за оновлення та відкликання сертифікатів;

- здійснює перевірку облікових даних суб'єктів для підтвердження їх ідентичності;
- проводить валідацію сертифікатів;
- виконує комплекс процедур та операцій, з метою встановлення довіри між суб'єктами.

2. Реєстраційний центр (РЦ) – компонент ІВК, який перевіряє ідентичність суб'єкта, надає дозвіл на створення цифрового сертифіката, збирає та передає ЦС необхідну інформацію для подальшої видачі сертифіката. ЦС та РЦ є структурами ІВК, які відокремлені одна від одної, але вони взаємодіють між собою та довіряють один одному. РЦ приймає запити, які надходять від серверів, користувачів та організацій на створення нового сертифікату або подовження сертифіката, після перевірки облікових даних та ідентифікації суб'єкта запит надходить до ЦС, який здійснює видачу сертифіката [5, 6]. По завершенню перевірки облікових даних суб'єкта РЦ підписує перевірену інформацію особистим ключем та передає ЦС, після чого ЦС перевіряє відповідну інформацію відкритим ключем РЦ [7]. Підписання даних цифровим підписом здійснюється з метою забезпечення цілісності, автентичності та неспростовності інформації.

3. Сутності з підтримкою ІВК – об'єкти, які підтримують та застосовують систему ІВК [3]. До таких сутностей відносяться: банкомати, платіжні термінали, системи електронного доставлення та платежів, державні установи, технологічні компанії, міжнародні корпорації, сервери, комп'ютерні й мережеві пристрої тощо. Копії цифрового сертифіката ЦС мають бути поширені серед усіх сутностей, які підтримують ІВК для встановлення довірчих взаємовідносин у цифровому просторі. Цифровий сертифікат ЦС є ознакою, яка визначає, що ЦС – це надійний та легітимний орган, який спеціалізується на сертифікації та не залежить від жодної сутності.

4. Сховище сертифікатів – це база даних, яка містить видані сертифікати, включаючи сертифікати, у яких закінчився термін дії, а також запити на отримання цифрового сертифіката, які очікують на розгляд або відхилені [3]. Захист сховища сертифікатів забезпечується шифруванням та різноманітними фізичними методами захисту інформації.

5. Політики сертифікатів – документи, спрямовані на визначення різних об'єктів ІВК, їх компетенцій та обов'язків в рамках здійснення етапів робочого процесу ІВК.

6. Список відкликаних сертифікатів (СВС) містить перелік цифрових сертифікатів, які відкликані ЦС до фактичної дати закінчення терміну дії [8].

7. Online Certificate Status Protocol (OCSP) [9] є альтернативою СВС, замість того, щоб завантажувати та перевіряти наявність конкретного цифрового сертифіката в повному СВС, протокол OCSP дозволяє запитувати сервер щодо статусу дійсності конкретного цифрового сертифіката в режимі реального часу.

3. Методи та засоби захисту інформації в парадигмі ІВК

3.1. Цифровий підпис та сертифікат

ІВК складається з різноманітних компонентів, які взаємодіють між собою. Центри, які входять до складу ІВК, використовують цифровий підпис, який базується на криптографії з відкритим ключем для побудови довірчих відносин. Цифровим підписом підписуються та завіряються цифрові сертифікати, електронні документи та списки, що надаються іншим організаціям для перевірки конкретних сертифікатів. Застосування цифрового підпису забезпечує безпеку взаємовідносин між внутрішніми структурами та зовнішніми сутностями. Цифровий підпис гарантує забезпечення цілісності, автентичності та неспростовності інформації, що є фундаментальними атрибутами для забезпечення безпеки та довіри в цифровому середовищі. Він є електронним аналогом рукописного підпису в паперовому документі. Основна роль цифрового підпису – підтвердити походження документа від першоджерела та зафіксувати вміст документа на момент підписання, тим самим забезпечити його цілісність. Цифровий підпис є ключовим елементом цифрового сертифіката, на базі якого суб'єкти встановлюють довірчі взаємовідносини в інформаційному середовищі.

Цифровий сертифікат є електронним документом, який містить ідентифікаційну інформацію щодо власника цього сертифікату, його відкритий ключ та цифровий підпис ЦС. Сертифікати використовуються сторонами комунікації для перевірки особистості один одного та для встановлення довіри між сторонами в інформаційному просторі. Також вони дозволяють захистити інформацію від несанкціонованого доступу або модифікації. Ідентифікаційна інформація щодо власника сертифіката та його відкритий ключ перетворюються в геш-значення за допомогою геш-функції. Особистим ключем ЦС виконується операція підписання геш-значення. Процес підписання здійснюється шляхом застосування криптографічної функції до геш-значення для створення цифрового підпису. Алгоритм підпису використовує особистий ключ ЦС для формування унікального цифрового підпису. Згенерований цифровий підпис додається до вихідних даних у цифровому сертифікаті.

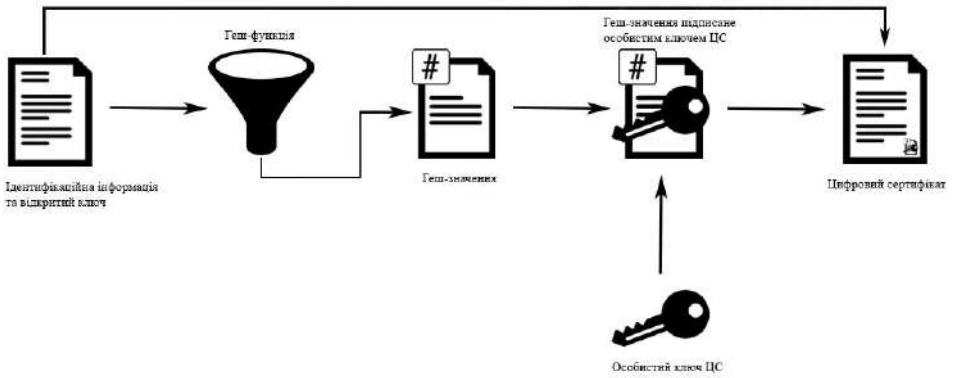


Рис. 3. Схема процедури підписання цифрового сертифіката

Цифровий підпис ЦС гарантує цілісність даних, наведених в сертифікаті, та підтверджує належність відкритого ключа конкретному суб'єкту. Формат та структура цифрових сертифікатів, використовуваних в ІВК, визначені в стандарті X.509. Цифровий сертифікат X.509 містить інформацію про суб'єкта, відкритий ключ, а також організацію, яка видала сертифікат та інші метадані. ЦС створює та підписує цифровий сертифікат, тому в сертифікаті містяться основні дані щодо ЦС, включаючи назву та відкритий ключ. При отриманні цифрового сертифіката інші сторони можуть перевірити справжність цифрового підпису, використовуючи відкритий ключ ЦС. Цифровий сертифікат містить дати початку та закінчення строку дії сертифіката. Після закінчення терміну дії сертифікат стає недійсним. Кожному цифровому сертифікату присвоюється унікальний ідентифікатор. Він дозволяє відрізнити сертифікати один від одного. В цифровому сертифікаті вказується криптографічний алгоритм, використаний для генерації цифрового підпису.

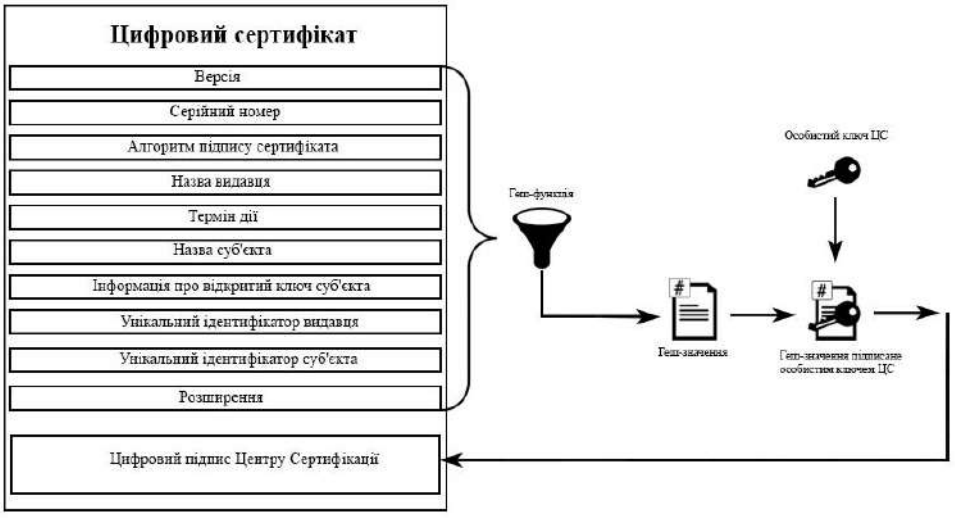


Рис. 4. Формат цифрового сертифіката X.509 V3 та модель побудови цифрового підпису

3.2. Смарт-карти

Смарт-карти – це маленькі пластикові карти, які оснащені вбудованим мікропроцесором, який здатний виконувати різноманітні обчислювальні та криптографічні операції. Смарт-карти також оснащені пам'яттю, що дозволяє зберігати відкриті, секретні ключі та цифрові сертифікати. Смарт-карта надає сховище для секретних ключів, які в більшості випадків використовуються виключно на смарт-карті й ніколи не залишають її для забезпечення максимальної безпеки. Смарт-картка застосовується для генерації цифрового підпису, обчислене геш-значення зберігається на смарт-карті та підписується особистим ключем. Криптографічні операції для валідації цифрового підпису, також проводяться на смарт-карті.

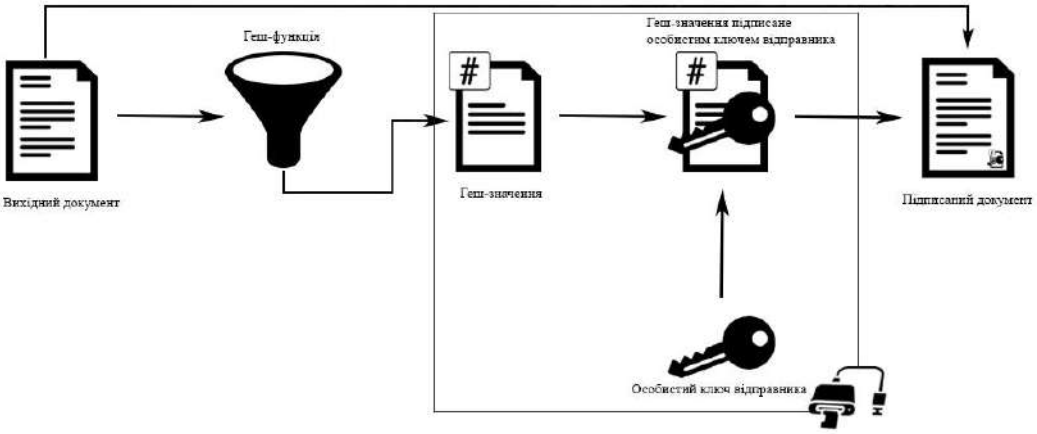


Рис. 5. Схема процедури підписання електронного документа за допомогою смарт-карти

Смарт-карти можуть генерувати відкритий та особистий ключі та здатні зберігати обмежені обсяги пам'яті. Смарт-карти використовуються для генерації цифрових сертифікатів, можна виділити два методи генерації цифрових сертифікатів [10]:

1. ЦС створює відкритий та особистий ключі в захищеному середовищі, формує, підписує цифровий сертифікат та імпортує його на смарт-карту (рис. 6).

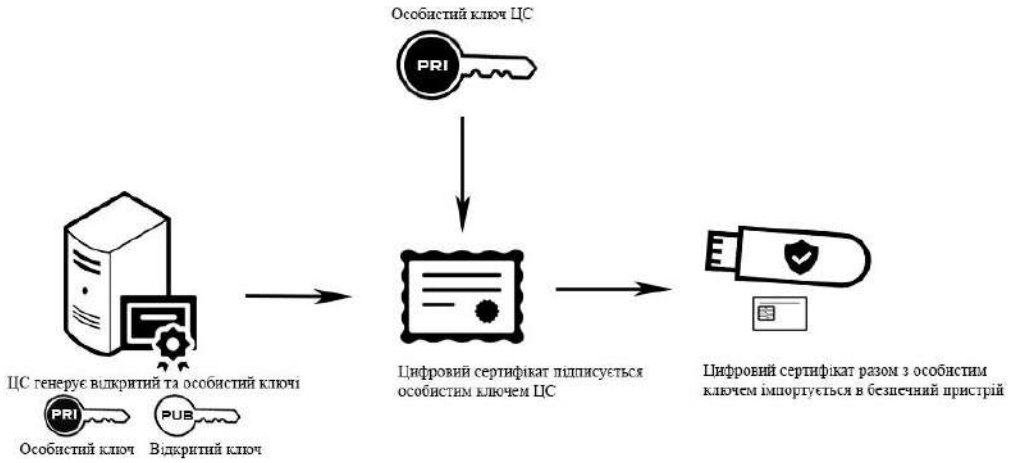


Рис. 6. Схема першого методу генерації цифрових сертифікатів

2. Генерація відкритого та особистого ключів здійснюється всередині смарт-карти (рис. 7).

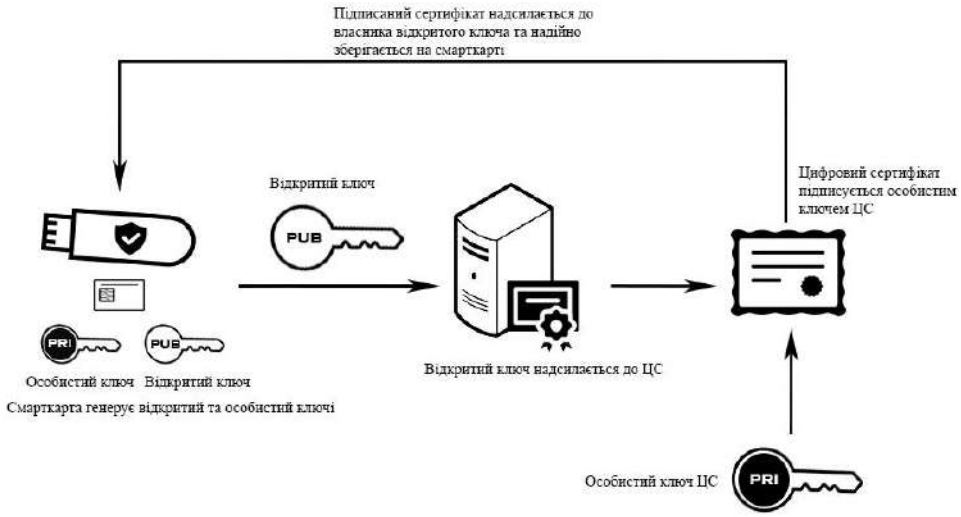


Рис. 7. Схема другого методу генерації цифрових сертифікатів

Смарт-карти є мобільними та компактними пристроями, оскільки за розмірністю відповідають стандартним банківським картам. Смарт-карта оснащена вбудованим механізмом безпеки для забезпечення конфіденційності, цілісності та автентичності даних, які зберігаються на смарт-карті. ПІН є важливим компонентом для забезпечення безпеки, він необхідний для отримання доступу до функцій смарт-карти та конфіденційної інформації. Здебільшого, ПІН – це послідовність цифр в діапазоні від 0 до 9 [11]. Користувач матиме можливість повторно ввести ПІН, якщо він неправильне ввів значення ПІН. Кількість спроб введення ПІН обмежена в основному до трьох спроб, щоб уникнути вичерпного пошуку. Смарткарта переходить в режим блокування у випадку, якщо максимальна кількість спроб введення перевищується. Розробниками смарт-карт передбачено додатковий механізм для розблокування смарт-карти. Користувачу необхідно ввести правильну комбінацію числового коду, яка називається персональний ключ розблокування (ПКР) для зняття режиму блокування. Система, також встановлює обмежену кількість спроб для введення значення ПКР. Порівняно з числовою послідовністю ПІН, яка складається з 4–6 цифр, ПКР представляє собою довгу послідовність, яка переважно складається з 10–20 цифр, яку дуже складно зафіксувати в пам'яті. Для використання особистого ключа, який міститься на смарт-карті, користувач повинен володіти двома компонентами: послідовністю ПІН та смарт-картою. У деяких смарт-картах біометрична авторизація використовується як альтернатива до авторизації за допомогою ПІН. Біометрична авторизація підвищує рівень безпеки особистих ключів, бо біометричні параметри не можуть бути передані іншим особам.

Висновки

1. Механізм управління відкритими ключами ІВК дозволяє виявити та захиститися від атаки типу «людина посередині» завдяки застосуванню криптографії з відкритими ключем та цифрових сертифікатів. Використання криптографії з відкритими ключами та цифрових сертифікатів грає ключову роль у забезпеченні конфіденційності, цілісності та автентичності даних та сприяє уникненню широкого спектра зовнішніх загроз, таких як кібератака типу «людина посередині», компрометація особистого ключа, фальсифікація цифрових сертифікатів тощо.

2. ІВК є комплексною системою, ключовим елементом якої є ЦС, який виконує роль третьої сторони в комунікаційному процесі групи сторін. ЦС сприяє встановленню ланцюжка довіри між сторонами для подальшої взаємодії в інформаційному просторі. Довірчі відносини між сторонами встановлюються на основі цифрових сертифікатів, виданих ЦС.

3. ІВК є рішенням для організації процедури ідентифікації та автентифікації конкретного суб'єкта в режимі онлайн. Цифровий сертифікат виконує роль посвідчення суб'єкта, яке

дозволяє іншим сторонам ідентифікувати та перевірити особистість в цифровому світі. ІВК регулює механізм управління цифровими сертифікатами, які є невід'ємним елементом для встановлення довіри та інформаційної безпеки в мережевих комунікаціях.

4. Сертифікати X.509 є структурованими, надійними та широко використовуються для забезпечення безпеки та автентифікації в мережевих протоколах та інформаційних системах.

5. Компоненти ІВК складають комплексну структуру та взаємодіють між собою, використовуючи різні механізми на основі криптографії з відкритим ключем для забезпечення інформаційної безпеки.

6. Всі процеси та процедури проходять згідно зі встановленим регламентом системи ІВК.

7. ІВК є регулятором процесів, пов'язаних з управлінням відкритими ключами та встановленням довіри між сторонами, які ініціюють комунікацію через мережу.

8. Для підвищення рівня безпеки необхідно використовувати апаратні засоби та електронні пристрої, які надають безпечне сховище для відкритих і особистих ключів та цифрових сертифікатів.

Список літератури:

1. Інфраструктура управління відкритими ключами PKI. [Електронний ресурс]. Режим доступу: http://infoprotect.net/varia/infrastruktura-otkrytyh-klyuchey-pki.

2. CCNA Cyber Ops (Version 1.1). Chapter 9: Cryptography and the Public Key Infrastructure. [Електронний ресурс]. Режим доступу: https://itexamanswers.net/ccna-cyber-ops-version-1-1-chapter-9-cryptography-and-the-public-key-infrastructure.html.

3. PKI for EMV cards compliant to PCI DSS. [Електронний ресурс]. Режим доступу: https://www.cryptomathic.com/news-events/blog/pki-for-emv-cards-compliant-to-pci-dss.

4. Certificate authority (CA). [Електронний ресурс]. Режим доступу: https://www.techtarget.com/searchsecurity/definition/certificate-authority.

5. PKI Fundamentals. [Електронний ресурс]. Режим доступу: https://pki.treas.gov/pki_funds3.htm.

6. What is a Registration Authority? [Електронний ресурс]. Режим доступу: https://www.primekey.com/wiki/what-is-a-registration-authority/.

7. Інфраструктура відкритих ключів. [Електронний ресурс]. Режим доступу: https://ru.wikipedia.org/wiki/Інфраструктура_відкритих_ключів.

8. Certificate Revocation List (CRL). [Електронний ресурс]. Режим доступу: https://www.techtarget.com/searchsecurity/definition/Certificate-Revocation-List.

9. Online Certificate Status Protocol. [Електронний ресурс]. Режим доступу: https://uk.wikipedia.org/wiki/Online_Certificate_Status_Protocol

10. Cryptography and Public Key Infrastructure. Режим доступу: https://downloads.acs.com.hk/technology/494-09-pki-and-middleware.pdf.

11. Johannes A. Buchmann, Evangelos Karatsiolis, Alexander Wiesmaier. Introduction to Public Key Infrastructures. 2013. P. 68–70.

Надійшла до редколегії 05.08.2023

Відомості про авторів:

Бодня Микита Олегович – Харківський національний університет імені В. Н. Каразіна, студент факультету комп'ютерних наук; Україна; e-mail: bodnia2020kb12@student.karazin.ua

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

Пономар Володимир Андрійович – канд. техн. наук, Харківський національний університет імені В.Н. Каразіна, старший науковий співробітник кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук, інженер-конструктор АТ "Інститут Інформаційних Технологій"; Україна; e-mail: Laedaa@gmail.com; ORCID: https://orcid.org/0000-0001-5271-2251

УДК 004.056.5 **DOI:10.30837/rt.2023.3.214.03**

С.О. КОЛОМІЙЦЕВ, О.В. СЄВЄРІНОВ, канд. техн. наук,
В.М. ФЕДОРЧЕНКО, канд. техн. наук, В.М. СУХОТЕПЛИЙ

АНАЛІЗ ПЛАГІНІВ ДВОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ ДЛЯ СИСТЕМИ WORDPRESS

Вступ

За даними компаній W3Techs і Website Rating, що займаються веденням статистики різних технологій в Інтернеті, станом на початок 2023 р. в світі нараховується приблизно 1,97 мілрд веб-сайтів і з кожним роком ця кількість зростає [1]. 68,4 % всіх сайтів працюють під управлінням якоїсь системи управління контентом (Content Management System, CMS) [2].

Найпопулярніші CMS представлені в табл. 1 [2].

Таблиця 1

Найпопулярніші системи управління контентом

№ з/п	CMS	Доля ринку	№ з/п	CMS	Доля ринку
1	WordPress	63.1%	6	Drupal	1.7%
2	Shopify	5.8%	7	Adobe Systems	1.6%
3	Wix	3.7%	8	PrestaShop	1.2%
4	Squarespace	3%	9	Google Systems	1.1%
5	Joomla	2.6%	10	Bitrix	1%

Всі інші CMS, яких налічується сотні, мають долю ринка менше 1 %. Як видно зі статистики, WordPress є найпопулярнішою в світі системою управління сайтом. Через таку популярність WordPress також є системою, на долю якої приходиться найбільша кількість атак. Кожного дня відбувається майже 30,000 атак на веб-сайти, 90 % з яких приходиться на WordPress [3, 4]. Для зламу цієї системи розроблено безліч спеціалізованого програмного забезпечення. Загалом, WordPress достатньо надійна і захищена система, але тим не менш, деякі недоліки роблять її вразливою перед такими типами атак, як атака зі словником і атака методом повного перебору. Якщо врахувати використання слабких або розповсюджених паролів, то успішність атак у більшості випадків це лише питання часу. У пошуку варіантів вирішення цієї проблеми, власники або адміністратори сайтів використовують додаткове стороннє програмне забезпечення (плагіни).

Плагін – це додаткове програмне забезпечення, яке написане сторонніми розробниками для додавання нового функціоналу або зміни існуючого [5]. В теорії, плагіни допомагають швидко і безкоштовно вирішити на сайті певні питання. Але на відміну від ядра системи, розробкою якого займається команда професіоналів, розробкою плагінів можуть займатися всі бажаючі. Тобто, програмісти з будь яким рівнем кваліфікації. Це призводить до того, що плагіни нерідко додають в систему нові вразливості і не вирішують або вирішують тільки частково ті задачі, для яких були створенні.

Тільки в офіційному репозиторії WordPress знаходиться близько 60,000 тисяч плагінів [6]. Працівники компанії фізично не мають змоги слідкувати за безпекою і якістю такої кількості плагінів. Під час додавання в репозиторій нового плагіна, співробітниками WordPress виконується лише поверхнева перевірка типових загроз в програмному коді. А після затвердження плагіна, його оновлення і будь які зміни в коді взагалі не перевіряються. Подальша модерація здійснюється лише постфактум, після скарг від користувачів, які вже постраждали.

Всі ці фактори спонукають до ретельного аналізу плагінів перед їх використанням. Особливо це стосується плагінів для двофакторної автентифікації (ДФА), на які покладають

надії у вирішенні питань, пов'язаних з захистом адміністративної частини сайту від несанкціонованого доступу [7].

Метою статті є аналіз існуючих плагінів двофакторної автентифікації для оцінки їх ефективності.

Захищеність WordPress від несанкціонованого доступу

Проведений аналіз показав, що після інсталяції на веб-сервер системи WordPress, за замовчуванням сайт не має суттєвого захисту від несанкціонованого доступу [8]. Крім відсутності механізмів захисту, деякі технічні рішення в цій системі навпаки допомагають зловмисникам пришвидшити процес отримання доступу.

Виявлено наступні проблеми:

1. Відсутність обмежень на кількість спроб авторизації.
2. Підказки на сторінці авторизації, що допомагають перевірити правильність вводу логіна.
3. Доступність до REST API, що допомагає знайти логіни користувачів.
4. XML-RPC, що допомагає перевірити логін і пароль в обхід сторінки авторизації.

Звісно, всі ці проблеми мають варіанти вирішення, але для цього, по-перше, треба знати про їх наявність, а по-друге, мати навички з програмування на PHP і досвід роботи з самою системою WordPress. А так як WordPress позиціонується як “рішення з коробки”, для людей без спеціальної технічної підґотовки всі його типові проблеми можна в повному обсязі виявити на абсолютній більшості веб-сайтів.

На рис. 1 зображено приклад того, як зловмисник може перевірити логін користувача на сторінці авторизації.

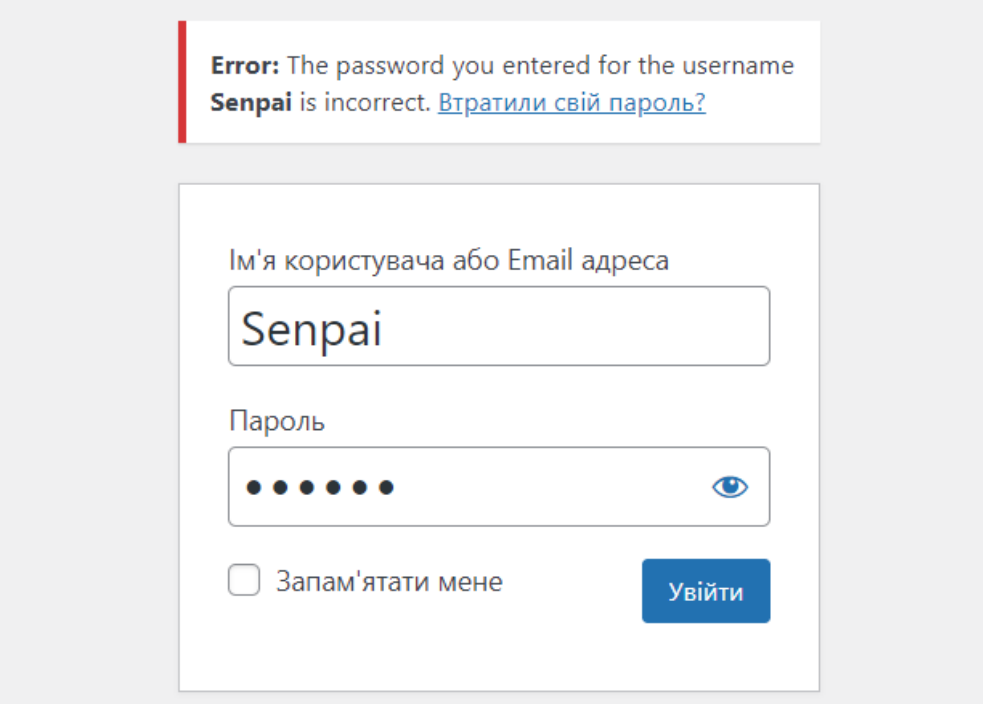


Рис. 1. Підказки на сторінці авторизації

Якщо було введено невірний і логін і пароль, зловмисник побачить повідомлення про те, що користувача з таким логіном в системі не існує. Але якщо логін вірний, то зловмисник побачить повідомлення про те, що для користувача з таким логіном введено невірний пароль. Таким чином, використовуючи підказки, зловмисник може дізнатися логіни всіх користувачів і адміністраторів сайту. Знаючи вірний логін і не маючи обмежень у кількості спроб авторизації, зловмисник отримує достатньо високу імовірність на підбір пароля і отримання несанкціонованого доступу.

Розробники WordPress знають про таку проблему, але навмисно її не виправляють. На їх думку, такі підказки допомагають справжнім користувачам, які забули свої дані, і користі від цих повідомлень більше ніж проблем.

На рис. 2 зображено приклад того, яким чином можна прямо в браузері перевірити існуючих користувачів, просто відкривши певну технічну сторінку.

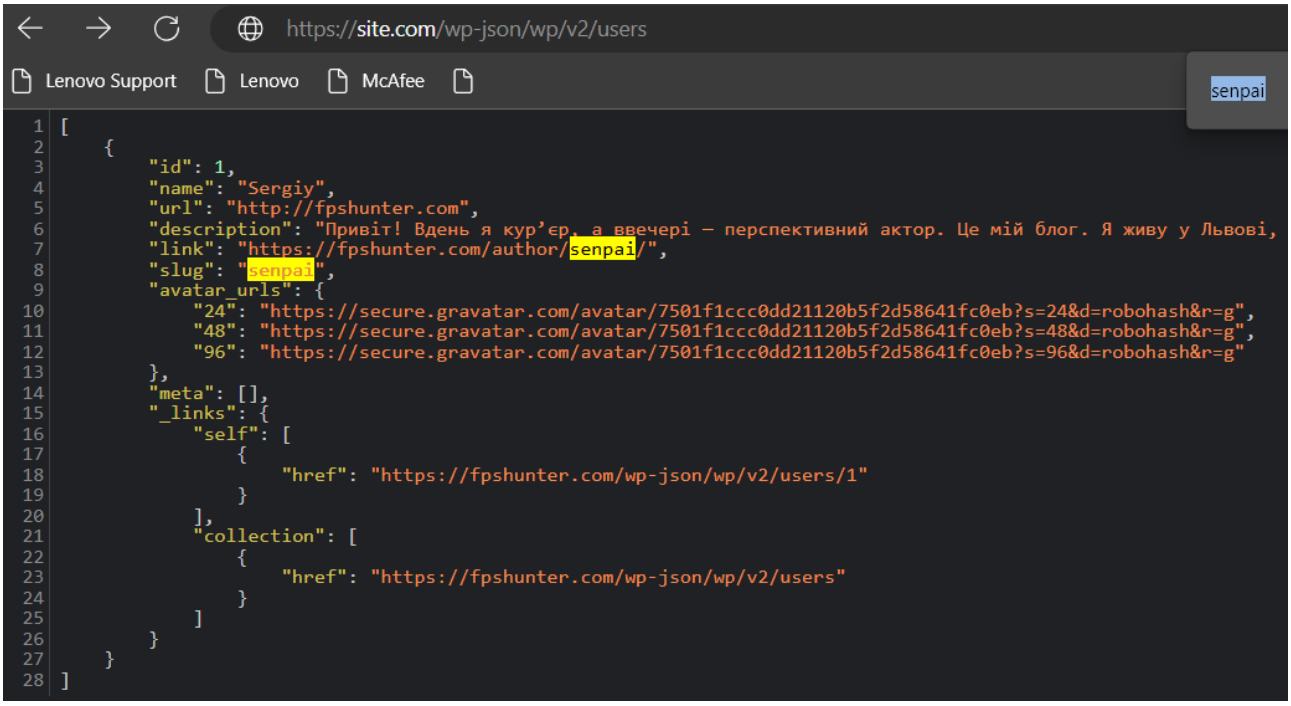


Рис. 2. Пошук логінів користувачів через REST API

Через REST API можна знайти логін користувача і його ідентифікатор в базі даних. Ідентифікатор під номером 1 вказує на те, що це перший зареєстрований користувач, який майже зі стовідсотковою імовірністю має роль адміністратора.

Аналіз плагінів для ДФА

Єдиний спосіб захистити сайт від несанкціонованого доступу – це використання плагінів, що додають двофакторну автентифікацію і виправляють вразливості системи.

Двофакторна автентифікація (ДФА) є типом багатофакторної автентифікації та представляє собою технологію, що забезпечує ідентифікацію користувачів за допомогою комбінації двох різних компонентів [9, 10].

WordPress має велику кількість ДФА плагінів. Але досліджувались тільки ті, що знаходяться в офіційному репозиторії, мають значну кількість користувачів і активно підтримуються розробниками. Кожен з розглянутих плагінів був встановлений на веб-сайт з останньою версією WordPress. Після чого були проведені дослідження з метою оцінити їх ефективність.

Список плагінів над якими проводились дослідження [5]:

1. WP 2FA.
2. Two Factor Authentication.
3. Defender Security.
4. Login Lockdown.
5. Wordfence Login Security.
6. Two Factor (2FA) Authentication via Email.
7. Trusona for WordPress.
8. DoLogin Security.

9. OTP Authenticator.
10. WebAuthn Provider for Two Factor.
11. 1-Click Login.
12. Orion SMS OTP Verification.
13. WP – SMS OTP Login.
14. OwnID Passwordless Login.

При дослідженні для пошуку загроз та вразливостей використовувалась програма WPScan, що входить до дистрибутиву Kali Linux.

WPScan – розроблена виключно для аналізу сайтів, що працюють на системі WordPress і має найбільшу базу загроз та вразливостей, що стосуються цієї системи. Програма створена для спеціалістів з кіберзбезпеки, але через свою ефективність, найбільшу популярність отримала саме серед кіберзлочинців.

Під час дослідження після встановлення кожного плагіна виконувались нова перевірка і спроба атаки зі словником. Мета – перевірити саму можливість проведення атаки, яку і повинні заблокувати ДФА плагіни. Тому, для зменшення часу роботи програми пароль навмисно обирався простим.

На рис. 3 зображено приклад налаштування і запуску WPScan.

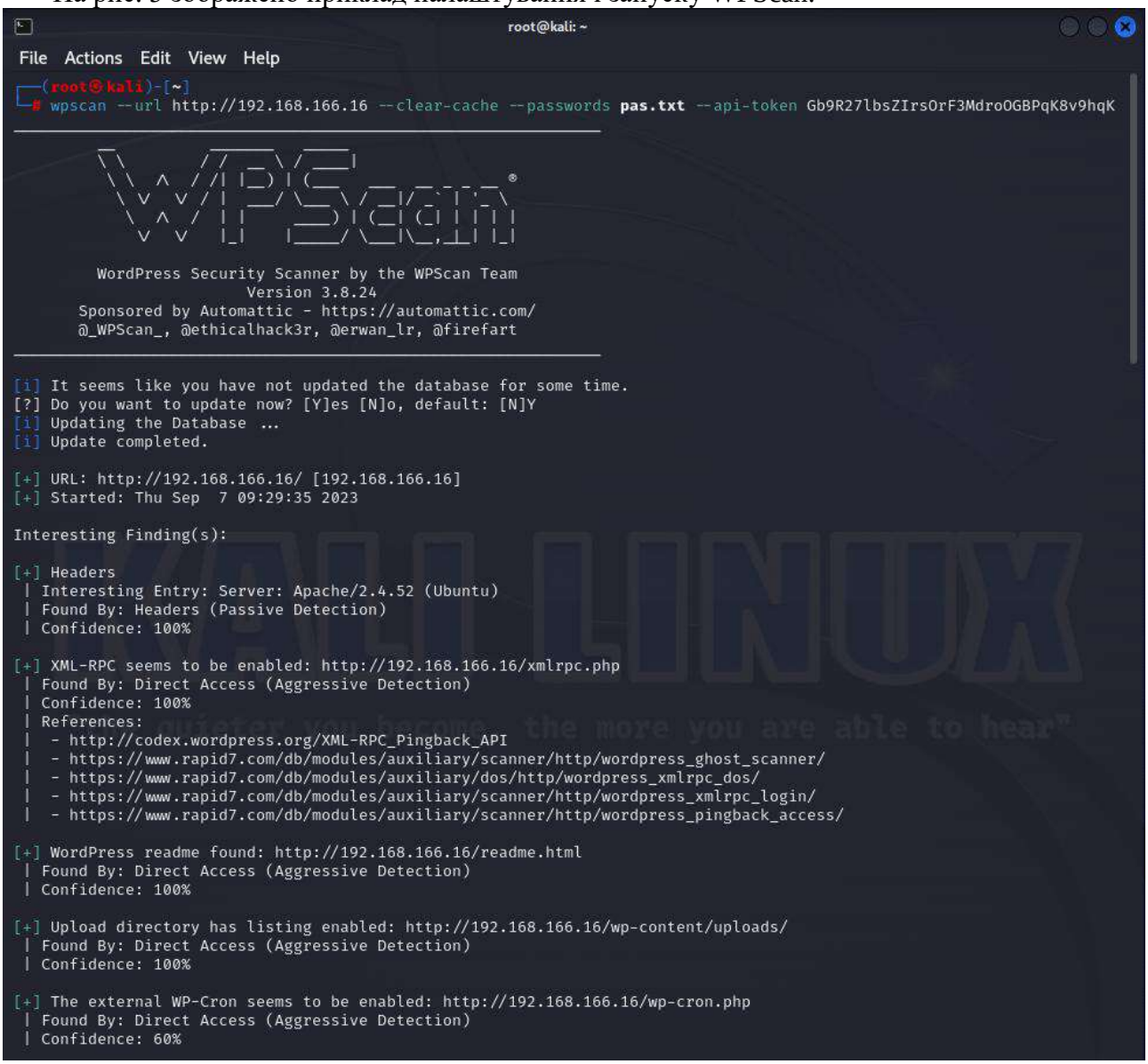


Рис. 3. Запуск роботи WPScan

WPScan вміє проводити атаку зі словником двома методами. Перший – атака безпосередньо на сторінку авторизації: відправка запитів на файл wp-login.php. Другий – атака через протокол XML-RPC: відправка запитів на файл xmlrpc.php. За замовчуванням, WPScan атакує сторінку авторизації, але якщо такий спосіб заблоковано, програма автоматично перемикається на другий метод. Можна обрати і конкретний метод проведення атаки.

На рис. 4 зображено результат успішної атаки.

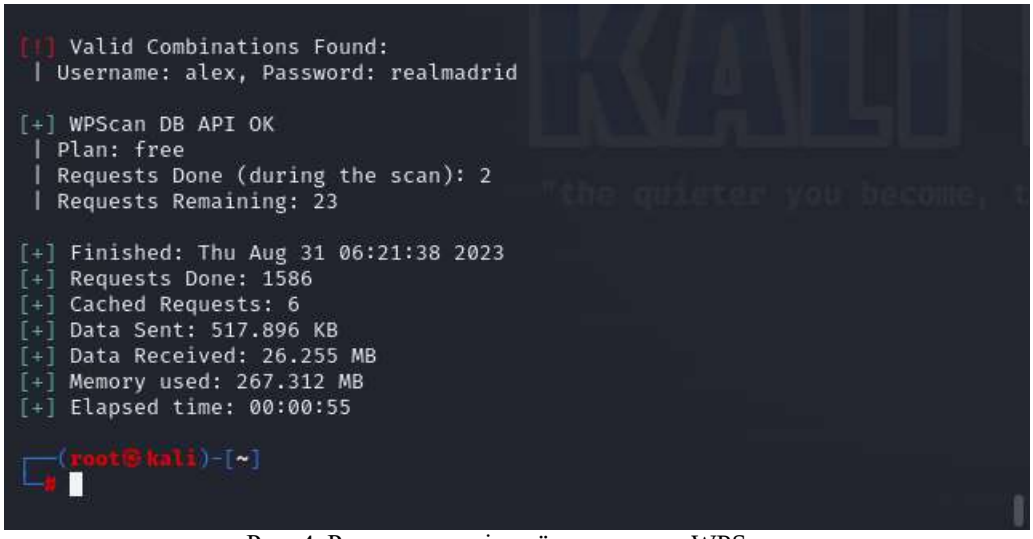


Рис. 4. Результат успішної атаки через WPScan

За результатами досліджень було виявлено наступне. Всі розглянуті плагіни в повній мірі захищають веб-сайт, якщо атака відбувається на сторінку авторизації. Але якщо атака відбувається через протокол XML-RPC, тільки один плагін, а саме Wordfence Login Security, здатен заблокувати таку атаку. У всіх інших випадках результат атаки був успішним.

XML-RPC – це протокол для віддаленого виклику процедур, він зберігся у WordPress з часів повільного інтернету, коли сайтом було простіше керувати через десктопні застосунки. Наразі XML-RPC використовується тільки в окремих випадках, а загалом системою не використовується. Сьогодні це лише додаткова вразливість, яку активно використовують кіберзлочинці. На файл xmlrpc.php можна без обмежень відправляти запити і отримувати відповіді про успішність авторизації. Таким чином, двофакторна автентифікація, яка додається плагінами на сторінку авторизації, ніяк не запобігає можливості провести атаку (рис. 5).

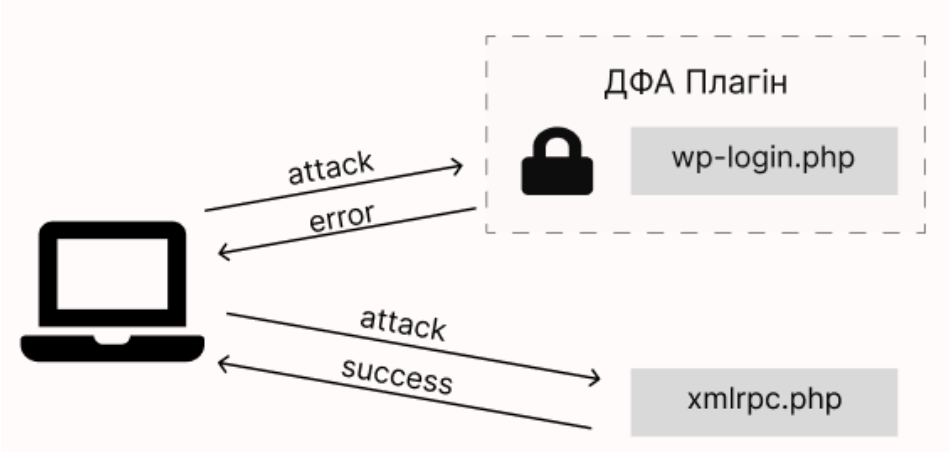


Рис. 5. Вектори атак

Для WordPress існують окремі плагіни, які вирішують виключно проблему XML-RPC. Але середньостатистичний користувач немає уявлення навіть про існування такої проблеми,

тому функціонал для відключення XML-RPC має бути присутнім саме у плагінах для двофакторної автентифікації, бо без цього їх використання не дає повноцінного захисту. Тільки розробники плагіна Wordfence Login Security врахували цю вразливість і реалізували функціонал для її вирішення.

Висновки

Динаміка зростання кількості веб-сайтів і велика доля ринку, що належить системі WordPress, спонукають до необхідності ретельного аналізу плагінів, які повинні забезпечувати захищеність цієї системи. Результати дослідження показали, що більшість ДФА плагінів не забезпечують захист системи в повній мірі. Більшість розробників концентрує увагу виключно на сторінці авторизації. Загалом, всі справляються з її захистом, але разом з цим ігнорують або не знають, як саме програми проводять атаки з технічної точки зору. Це пов'язано з тим, що розробка плагінів, як правило, не є комерційною діяльністю. Розробкою в основному займаються ентузіасти з різним рівнем кваліфікації на добровільній основі і без ретельного вивчення проблеми.

Кожен розглянутий плагін використовується на десятках, а в деяких випадках і на сотнях тисячах веб-сайтів. В результаті сотні тисяч власників сайтів переконані в тому, що вони в повній мірі захищені від несанкціонованого доступу, але як показало дослідження, це не відповідає дійсності.

Список літератури:

1. Website Rating [Електронний ресурс]. Режим доступу: https://www.websiterating.com/research/internet-statistics-facts/
2. W3Techs [Електронний ресурс]. Режим доступу: https://w3techs.com/technologies/overview/content_management
3. Website Rating [Електронний ресурс]. Режим доступу: https://www.websiterating.com/research/cybersecurity-statistics-facts/
4. Сєвєрінов О.В., Хрєнов А.Г., Поляков А.О. Аналіз сучасних методів атак на автоматизовані системи управління військами та інформаційні мережі // Системи обробки інформації. 2015. № 9. С. 101–104.
5. Developer WordPress [Електронний ресурс] Режим доступу: https://developer.wordpress.org/plugins/intro/what-is-a-plugin/
6. Репозиторій плагінів WordPress [Електронний ресурс]. Режим доступу: https://wordpress.org/plugins/
7. Сєвєрінов О.В.; Баклан Я.А. Аналіз рівня безпеки web-ресурсів. 2022. PhD Thesis.
8. Wordpress Codex [Електроний ресурс]. Режим доступа: https://codex.wordpress.org/Main_Page
9. Сєвєрінов О.В., Кліпоносова В.С. Автентифікації користувачів веб-ресурсів. 2022. PhD Thesis.
10. Ayoade O., Afolabi A. S., Awelewa A. T. A Review of Two Factor Authentication // International Journal of Computer Science and Information Security. 2018. Vol. 16, no. 6. P. 35–42,

Надійшла до редколегії 10.09.2023

Відомості про авторів

Коломійцев Сергій Олександрович – Харківський національний університет радіоелектроніки, студент, кафедра безпеки інформаційних технологій; Україна; e–mail: girbest@gmail.com

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

Федорченко Володимир Миколайович – канд. техн. наук, доцент, Харківський національний університет радіоелектроніки, доцент кафедри електронних обчислювальних машин, факультет комп'ютерної інженерії та управління, Україна; e-mail: volodymyr.fedorchenko@nure.ua; ORCID: https://orcid.org/0000-0001-7359-1460

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

УДК 004.056 **DOI:10.30837/rt.2023.3.214.04**

В.І. ЄСІН, д-р техн. наук, В.В. ВІЛІГУРА, І.І. СВАТОВСЬКИЙ, канд. техн. наук

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ У РОЗПОДІЛЕНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ: ОСНОВНІ АСПЕКТИ

Вступ

Забезпечення безпеки розподілених інформаційних систем (РІС) є критично важливим завданням, оскільки ці системи використовуються переважно для обробки та зберігання великого обсягу чутливої/конфіденційної інформації, такої як фінансові дані, медичні записи, персональні дані тощо. Інформація у світі є одним із найважливіших ресурсів суспільства, без необхідного захисту якої нові інформаційні технології здатні порушити приватне життя людей та діяльність різних організацій. В епоху Великих Даних проблема захищеності чутливих даних ще більше загострюється. Хоча глобальні витрати на безпеку, як очікується, перевищать 195 мільярдів доларів у 2025 р., зломи стають все масштабнішими, зухвалими, зачіпаючи все: від баз даних клієнтів і громадян до даних про вакцини і маршрутизатори Wi-Fi [1]. Згідно зі статистикою, останніми роками у світі неухильно зростає кількість витоків та обсяг скомпрометованих даних. Так, за даними досліджень Dell Technologies [2], у 2022 р. підприємства зіткнулися з великою кількістю інцидентів безпеки, ніж у попередні роки. Це призвело до збільшення часу простою, збільшення втрат даних та збільшення витрат на відновлення. Понад 1 мільйон доларів – це середня ціна втрати даних підприємства у 2022 р. На додаток до фінансових втрат і втрат репутації, що виникають внаслідок витоку даних, слід також враховувати, що сьогодні організації працюють в умовах дедалі більш суворого та швидко змінного нормативно-правового поля, в документах якого передбачено обов'язкове виконання відповідних приписів. Лише у Сполучених Штатах Америки діє понад 20 національних законів про конфіденційність та безпеку даних, а також додаткові закони, прийняті на рівні штатів [1]. Загальний регламент захисту персональних даних (General Data Protection Regulation – GDPR) [3] Європейського Союзу (ЄС) діє у державах-членах ЄС. Подібні правила та закони діють в Україні, Японії, Австралії, Новій Зеландії, Індії, Південній Кореї, Чилі, Бразилії. Таким чином, сьогодні можна однозначно говорити про те, що має місце проблема забезпечення безпеки РІС. Ось деякі її ключові аспекти:

– *безпека мережі*: РІС значною мірою покладаються на мережі для зв’язку між вузлами, тому безпека мережі є життєво важливою для захисту від таких загроз, як прослуховування, перехоплення даних і атаки типу «людина посередині»;

– *контроль доступу*: реалізація належного контролю доступу гарантує, що лише авторизовані користувачі або вузли можуть отримати доступ до певних ресурсів або виконувати певні дії в розподіленій системі;

– *цілісність даних*: мають бути вжиті заходи для виявлення та запобігання підробці даних під час передачі або зберігання;

– *шифрування даних*: чутливі конфіденційні дані, що передаються між вузлами, або зберігаються в розподіленій системі, повинні бути зашифровані, тобто перетворені на нечитану форму з використанням криптографічних примітивів;

– *пом'якшення наслідків розподіленої відмови в обслуговуванні* (distributed denial of service – DDoS): РІС чутливі до DDoS-атак, які можуть порушити їхню роботу, тому необхідні ефективні стратегії запобігання таким атакам;

– *безпечне кодування*: розробники повинні дотримуватися методів безпечного кодування, щоб звести до мінімуму вразливості програмного забезпечення, що працює в розподілених системах;

– *моніторинг та аудит*: безперервний моніторинг дій і подій безпеки в розподіленій системі та ведення журналів аудиту мають вирішальне значення для виявлення інцидентів безпеки;

– *реагування на інциденти*: наявність чітко визначеного плану реагування на інциденти має вирішальне значення для швидкого виявлення інцидентів безпеки, реагування на них і відновлення після них;

– *хмарна безпека*: якщо розподілена система використовує хмарні служби, забезпечення безпеки даних і програм у хмарі має важливе значення;

– *безпека з нульовою довірою* (zero trust security): впровадження моделі безпеки з нульовою довірою, де довіра ніколи не передбачається, може підвищити безпеку в розподілених системах;

– *відповідність нормативним та законодавчим актам*: у багатьох галузях існують спеціальні нормативні вимоги щодо безпеки та конфіденційності даних; дотримання відповідних законів і нормативних актів має вирішальне значення;

– *навчання з питань безпеки*: навчання користувачів і адміністраторів найкращим практикам безпеки та ризикам, пов’язаним із розподіленими системами, може допомогти запобігти порушенням безпеки.

Як видно з викладеного вище, без комплексного підходу до інформаційної безпеки, що поєднує в собі використання законодавчих, організаційних заходів, програмно-технічних засобів, політики та обізнаність користувачів, не обійтися. Регулярні оцінки безпеки, сканування вразливостей та тестування на проникнення можуть допомогти виявити та усунути слабкі місця у розподілених системах. Крім того, організаціям слід бути в курсі загроз, що виникають, і кращих практик забезпечення безпеки, щоб відповідним чином адаптувати свої заходи. У ситуації, що склалася, беручи до уваги сучасний стан розвитку технологій розподілених інформаційних систем, його швидкоплинний характер, науково-практичні досягнення в галузі інформаційної безпеки, кваліфікацію зловмисників, які постійно вдосконалюють можливості шкідливого впливу, положення та рекомендації різних нормативно-правових актів у багатьох випадках фахівцям з інформаційних систем, щоб забезпечити надійне безпечне функціонування останніх, потрібні відповідні знання з питань забезпечення безпеки. Тобто знання актуальних сучасних методів, прийомів та засобів забезпечення безпеки. Ця стаття якраз і націлена на надання таких знань. У ній у стислому викладі представлено достатньо широке коло питань, пов'язаних із безпекою розподілених інформаційних систем.

1. Ключові поняття інформаційної безпеки

Термін «*безпека*» є широко поширеним. Він використовується у політиці, військовій сфері, науці, техніці, освіті тощо. При цьому, як показує аналіз [4], його трактування, а отже і розуміння, буває різним. Причому розбіжності у трактуванні можуть бути дуже значними. Щоб виключити неоднозначність, представимо кілька визначень, даних у різних авторитетних джерелах, що дозволяють зрозуміти його суть з погляду аспектів, що розглядаються далі. В онлайн-словнику [5] дається достатньо загальне визначення безпеки (security) як якості або стану безпечного буття, такого як свобода від небезпеки, страху або тривоги, з іншого боку це щось, що захищає. Подібно цей термін визначають і автори [6]: «безпека – це стан безпечного буття та відсутності небезпеки чи шкоди. Крім того, це дії, вжиті для забезпечення безпеки когось чи чогось». У роботі [6] також формулюється, що «*безпека* – це захист», зазначаючи при цьому, що «захист від зловмисників – тих, хто навмисно чи іншим чином може завдати шкоди, є кінцевою метою безпеки». У роботі [7] безпека визначається з погляду системного підходу, тобто як системна властивість. При цьому констатується, що безпека – це набагато більше, ніж набір функцій та механізмів. А *безпека інформаційних технологій* – це характеристика системи, а також набір механізмів, які логічно і фізично охоплюють систему. Найбільш близькими до проблематики, що розглядається далі, є визначення *безпеки* (*security*), наведені в документах NIST [8, 9], що фактично повторюють суть визначення

інформаційної безпеки (*information security*), наведеного в стандарті ISO/IEC 27000 [10] та в іншому пізнішому документі NIST [11]. Так, відповідно до ISO/IEC 27000 [10] *інформаційна безпека* визначається як збереження конфіденційності, цілісності та доступності інформації. При цьому в стандарті ISO/IEC 27000 звертається увага на те, що крім зазначених вище можуть мати значення й інші властивості інформації, такі як: *автентичність* (*authenticity*); *підзвітність* (*accountability*); *невідмовність* (*non-repudiation*) та *надійність* (*reliability*).

Забезпечення безпеки розподілених інформаційних систем є надзвичайно важливим і водночас складним завданням. Так як навіть єдине слабке місце в системі може призвести до порушення безпеки всієї системи, і зробити заходи захисту її активів (актив – сутність, що імовірно представляє цінність для власника об'єкта оцінки [12]), що використовуються, марними. Основними активами будь-якої інформаційної системи є її обладнання, програмне забезпечення та дані. Безпеку у розподілених системах можна грубо розділити на дві частини [13, 14]. Одна частина стосується зв'язку між користувачами або процесами, які, можливо, знаходяться на різних машинах. Основним механізмом захисту передачі між вузлами мережі є організація безпечного каналу, що забезпечує автентифікацію взаємодіючих сторін, конфіденційність і цілісність даних, переданих повідомлень. Інша частина стосується авторизації, яка полягає у забезпеченні отримання процесом лише тих прав доступу до ресурсів у розподіленій системі, на яку він має право. Хоча для коректності, доцільно зазначити, що є ще деякі інші складові заходів безпеки, наприклад, резервне копіювання, моніторинг системи та інші. Говорячи про безпеку в комп'ютерній системі загалом, можна помітити, що вона тісно пов'язана з поняттям надійності. Неформально надійна комп'ютерна система – це система, якій ми по праву довіряємо у наданні послуг [14 – 16]. Надійність – це властивість системи, яка поєднує такі атрибути, як [15, 16]: доступність (availability), достовірність / безвідмовність (reliability), функціональну безпеку (safety) та ремонтопридатність (maintainability). Однак, якщо ми хочемо повною мірою довіряти комп'ютерній системі, слід враховувати й такі атрибути надійності, як конфіденційність і цілісність.

Конфіденційність (*confidentiality*) – це концепція заходів, що використовуються для забезпечення захисту секретності даних, об'єктів чи ресурсів (або інакше – властивість, що полягає в тому, що інформація не надається або не розкривається неавторизованим особам, організаціям або процесам). Метою захисту конфіденційності є запобігання або мінімізація несанкціонованого доступу до даних [17]. Конфіденційність відноситься до якості комп'ютерної системи, згідно з якою її інформація не надається або не розкривається неавторизованим особам, організаціям або процесам, вона розкривається лише уповноваженим сторонам. Широкий спектр заходів безпеки, що забезпечує захист конфіденційності, включає насамперед контроль доступу, шифрування та стеганографію.

Говорячи про конфіденційність, слід також відзначити деякі, пов'язані з нею, поняття та аспекти, а саме [17, 18]:

– *чутливість* (*sensitivity*) – відноситься до якості інформації, розкриття якої може завдати шкоди (harm) або збитків (damage). Збереження / підтримка (*maintaining*) конфіденційності чутливої інформації допомагає запобігти шкоді чи збитку;

– *обачність* / *обережність* (*discretion*) – це акт рішення, при якому оператор може впливати на розкриття інформації чи контролювати її, щоб мінімізувати шкоду чи збиток;

– *критичність* (*criticality*). Рівень, до якого інформація є критично важливою, є мірою її критичності. Чим вищий рівень критичності, тим більша ймовірність збереження конфіденційності інформації;

– *приховування* (*concealment*) – це дія з *приховування* / *хования* (*hiding*) або запобігання розкриття інформації. Часто приховування розглядається як *засіб укриття* (*cover*), *заплутування / обфускації даних* (*obfuscation*) чи *відволікання* (*distraction*). Поняття приховування пов'язане з безпекою через *безвісність* (*obscurity*), тобто зі спробою отримати захист за допомогою приховування (*hiding*), *мовчання* (відсутність відомостей – *silence*) чи *секретності* / *таємності* (*secrecy*). Хоча безпека через безвісність (неясність, невідомість) зазвичай

не вважається дійсною (valid) мірою безпеки, у деяких випадках вона все ж таки може мати значення;

– *приватність* (*privacy*) – означає збереження конфіденційності інформації, яка дозволяє встановити особистість, або яка може заподіяти будь-кому *шкоду (збиток, лихо, зло – harm*), *збентеження* / *незручності* (*embarrassment*) або *немилість* / *ганьбу* (*disgrace*) у разі її розкриття;

– *усамітнення* (*seclusion*) – має на увазі зберігання чогось у віддаленому місці. Це місце також може забезпечувати суворий контроль доступу;

– *ізоляція* (*isolation*) – це дія щодо збереження чогось окремо від інших. Ізоляція може використовуватися для запобігання змішування інформації або її розкриття.

Цілісність (*integrity*) – це концепція захисту *достовірності* / *надійності* (*reliability*) та *правильності* (*correctness*) даних. Захист цілісності запобігає несанкціонованій зміні даних. Це гарантує, що дані залишаються *правильними* (*correct*), *незмінними* (*unaltered*) та *збереженими* (*preserved*). Правильно реалізований захист цілісності надає засоби для авторизованих змін, одночасно захищаючи від намічених та зловмисних несанкціонованих дій (таких як віруси та вторгнення), а також від помилок, допущених авторизованими користувачами (таких як *помилки* (*mistakes*) чи *недогляди* / *упущення* (*oversights*)) [17]. Іншими словами, неправильні зміни в захищеній комп'ютерній системі повинні виявлятися та виправлятися. Цілісність можна розглядати з трьох точок зору: 1) запобігання (*preventing*) внесенню змін неавторизованими суб'єктами; 2) запобігання внесенню авторизованими суб'єктами несанкціонованих змін, наприклад, помилок; 3) підтримка (*maintaining*) внутрішньої та зовнішньої узгодженості об'єктів, щоб їх дані були правильним і істинним відображенням реального світу, а будь-які відносини / зв'язки (*relationship*) з будь-яким дочірнім, рівним (*peer*) або батьківським об'єктом були дійсними (valid), узгодженими (consistent) та такими, що піддаються перевірці (*verifiable*).

Для забезпечення цілісності в системі повинні бути передбачені елементи керування для обмеження доступу до даних, об'єктів та ресурсів. При цьому слід зазначити, що є інші поняття, аспекти, пов'язані з цілісністю, зокрема: *точність* (*accuracy*) – бути правильним / коректним (*correct*) та чітким (*precise*); *правдивість* (*truthfulness*) – бути справжнім відображенням дійсності; *справжність* (*автентичність – authenticity*) – бути справжнім (*authentic*) або непідробним (*genuine*); *дійсність* (*валідність – validity*) – бути фактично або логічно обґрунтованим; *невідмовність* / *неспростовність* (*non-repudiation*) – неможливість відмовитися від авторства, нездатність заперечувати здійснення дії; *підзвітність* (*accountability*) – бути відповідальним або тим, що має зобов'язання за дії та результати; *відповідальність* (*responsibility*) – бути відповідальним (мати обов'язки) або мати контроль над чимось чи кимось; *комплектність* (*completeness*) – наявність всіх необхідних компонентів або частин; *повнота* (всеосяжність – *comprehensiveness*) – бути повним за обсягом; повне включення всіх потрібних елементів.

Конфіденційність та цілісність залежать один від одного. Без цілісності об'єкта (тобто неможливості зміни об'єкта без дозволу) конфіденційність не може бути підтримана.

Третій принцип Тріади CIA (*Confidentiality, Integrity, Availability*) – це доступність, що означає, що авторизованим суб'єктам надається своєчасний та безперервний доступ до об'єктів. Часто засоби управління захистом доступності підтримують достатню пропускну здатність та своєчасність обробки, якщо це необхідно організації або спричинено ситуацією. Якщо механізм безпеки забезпечує доступність, він забезпечує високий рівень гарантії того, що дані, об'єкти та ресурси доступні авторизованим суб'єктам. Доступність передбачає ефективний безперервний доступ до об'єктів, у тому числі в умовах DoS атак. Доступність також передбачає, що підтримуюча інфраструктура, включаючи мережеві служби, засоби зв'язку та механізми контролю доступу, функціонує і дозволяє авторизованим користувачам отримувати авторизований доступ. Для підтримки доступності в системі повинні бути передбачені елементи керування для забезпечення авторизованого доступу та прийнятного рівня продук-

тивності, забезпечення необхідної надмірності, підтримання надійних резервних копій та запобігання втраті або знищенню даних. При цьому доступність залежить як від цілісності, так і конфіденційності. Без цілісності та конфіденційності доступність не може бути підтримана.

З іншого боку, безпеку інформаційних систем слід розглядати з точки зору необхідності захисту від різних загроз безпеці наданих ними служб (сервісів, послуг) та даних. Насамперед слід враховувати такі існуючі типи загроз безпеки (security threats), як [19, 20]: перехоплення (*interception*); переривання (*interruption*); модифікація (*modification*); фабрикація (*fabrication*).

Концепція *перехоплення* відноситься до ситуації, коли неавторизована сторона отримала доступ до служби або даних. Типовим прикладом перехоплення є випадок, коли зв'язок між двома сторонами був підслуханий кимось іншим. Перехоплення також відбувається, коли дані незаконно копіюються, наприклад, після злому облікового запису (account) користувача або каталогу суб'єкта у файловій системі. У загальному сенсі *переривання* належить до ситуації, у якій служба або дані стають недоступними, непридатними, знищеними тощо. У цьому сенсі атаки типу «відмова в обслуговуванні» (DoS), за допомогою яких хтось зловмисно намагається зробити службу недоступною для інших сторін, є загрозою безпеці, яка класифікується як переривання. *Модифікації* включають несанкціоновану зміну даних або підробку служби, щоб вона більше не дотримувалась своїх початкових специфікацій. Приклади модифікацій: перехоплення та подальша зміна даних, фальсифікація записів у базі даних, зміна програми тощо. Під *фабрикацією* розуміється ситуація, в якій генеруються додаткові дані або дії, які зазвичай не існують. Наприклад, зловмисник може спробувати додати запис до файлу пароля або бази даних, створити фальшиві профілі та опублікувати хибну інформацію в соціальних мережах, щоб вплинути на громадську думку, створити фальшиві вузли або надсилати фальшиві повідомлення. Слід звернути увагу, що модифікація і фабрикація можуть розглядатися як форма фальсифікації (*falsification*) даних.

2. Основні підходи щодо забезпечення безпеки розподілених систем

На даний момент фахівцями в галузі безпеки та розподілених інформаційних систем напрацьовано певні підходи та концепції у цьому напрямку. Як правило, спочатку в них рекомендується визначити вимоги до безпеки системи, тобто описати політики безпеки. Термін «політика комп'ютерної безпеки» (*computer security policy*) має кілька значень [21]. З одного боку, політика – це директиви вищого керівництва щодо створення програми комп'ютерної безпеки, встановлення її цілей та розподілу обов'язків. З іншого боку, термін політика використовується для позначення певних правил безпеки для певних систем. Крім того, політика може відноситися до зовсім інших питань, таких як конкретні управлінські рішення. Далі більшою мірою використовуватимуться аспекти поняття «політика безпеки» як політики інформаційної безпеки (information security policy), маючи на увазі під цим терміном сукупність законів, правил, методів, рекомендацій, що вказують порядок управління, захисту та розподілу інформації. Тобто в даному контексті політика безпеки (security policy) точно описує, які дії можна виконувати сутностям (entities) у системі, а які заборонено. Під сутностями розуміються користувачі, служби, дані, машини тощо. Після того, як політики безпеки будуть встановлені, стає можливим зосередитися на механізмах безпеки, за допомогою яких можна застосовувати певну політику. Механізм безпеки (security mechanism) – це пристрій або функція, призначена для надання однієї або декількох послуг безпеки, які зазвичай оцінюються з точки зору надійності обслуговування та гарантованості проекту [22]. Важливими механізмами безпеки вважаються [13, 14, 23]:

1. *Шифрування* (encryption). Шифрування має фундаментальне значення для комп'ютерної безпеки. Воно перетворює дані на те, що зловмисник не може зрозуміти. У контексті криптографії шифрування – це механізм, що забезпечує конфіденційність даних. Крім того, використовуючи різні криптографічні примітиви, можна забезпечити перевірку цілісності

даних (чи були дані змінені або ні). Маршрутизатор, сервер, кінцева система або виділений пристрій можуть виступати як пристрій шифрування / розшифрування. Дані, що зашифровуються, називаються зашифрованими даними (ciphered or encrypted data). Не зашифровані дані називаються простим або відкритим текстом (plain text or clear text).

2. *Авторизація* (authorization). Авторизація – це надання прав (привілеїв) конкретному учаснику процесу інформаційного обміну (автентифікованого або анонімного), що дозволяють їх власнику (людині, програмі або процесу) мати законний доступ до системи або до її об'єктів. Експерти з безпеки рекомендують використовувати принцип найменших привілеїв. Цей принцип ґрунтується на ідеї, що кожному користувачеві мають бути надані лише мінімально необхідні права для виконання певного завдання. Засоби авторизації користувачів можуть бути реалізовані за допомогою програмного коду та керувати не лише наданими користувачам правами доступу до системи чи об'єктів, але й набором операцій, які користувачі можуть виконувати з кожним об'єктом, який йому доступний.

3. *Автентифікація* (authentication). Термін «автентифікація» зазвичай стосується автентифікації користувачів, але також може стосуватися автентифікації пристроїв або програмних процесів. Тобто автентифікація може використовуватись для перевірки заявленої особи користувача, клієнта, сервера, хоста / вузла чи іншого об'єкта / сутності. Автентифікація згідно [24, 25] – це перевірка особи користувача, процесу або пристрою, часто як необхідна умова для дозволу доступу до ресурсів в інформаційній системі. У випадку з клієнтами основна передумова полягає в тому, що перед тим, як служба починає виконувати будь-яку роботу від імені клієнта, служба повинна впевнитись в особистості клієнта (якщо служба недоступна для всіх). Перевірка справжності (автентифікація) може проводитись різними методами та засобами, що використовують однофакторну та багатофакторну автентифікацію. Сьогодні широке застосування знайшли три типи / категорії факторів, що дозволяють пов'язати людину із встановленими повноваженнями [26 – 29]:

– фактори, що ґрунтуються на знанні (knowledge factors) – інформації, яка повинна зберігатися в секреті і яку може знати лише певний клієнт / користувач, наприклад, пароль, графічний пароль, парольна фраза (користувач «знає»);

– фактори, засновані на володінні (ownership / possession factors) – щось, що є у користувача, наприклад смарт-карти, смартфони, токени безпеки (користувач «має»);

– фактори невід'ємності / властивості (inherence factors) або біометричні фактори (biometric factor) – фізіологічні ознаки, властиві конкретним особам – біометричні дані або зразок поведінки, наприклад швидкість набору тексту, динаміка натискання клавіш, руху миші, сенсорні жести на сенсорних екранах і т. д. (користувач «є» або хто ви).

Хоча в літературі пропонуються й інші фактори (такі як автентифікація з використанням облікових даних людини в соціальних мережах та автентифікація на основі розташування), три перелічені вище категорії факторів є найбільш використовуваними [27]. Методи автентифікації, що стосуються різних факторів, можна комбінувати для підвищення безпеки, така автентифікація відома як багатофакторна [28]. Деякими прикладами багатофакторної автентифікації є комбінація факторів знання та володіння, комбінація факторів знання та приналежності, комбінація факторів володіння та приналежності, а також поєднання всіх трьох відомих факторів [27].

4. *Аудит* (auditing, audit). «Аудит» (audit) та «аудит» (auditing; коректніше, напевно, «аудиторська діяльність») – це досить близькі терміни, пов'язані з процесом перевірки та оцінки систем, процедур, даних та інших аспектів для забезпечення їх точності, надійності та дотримання стандартів. Вони можуть використовуватись у різних контекстах. Під терміном «audit», як правило, мають на увазі процес перевірки та оцінки чогось з метою визначення його правильності, відповідності стандартам або дотримання вимог, а під терміном «auditing» – дія або процес проведення аудиту («audit»). Ці терміни часто використовуються як взаємозамінні, але важливо розуміти різницю між ними. Процес аудиту може бути застосований у різних галузях та мати різні цілі. Аудит (audit) у сфері безпеки (security) –

це незалежний аналіз та перевірка записів та дій для оцінки адекватності системного контролю, забезпечення відповідності встановленим політикам та операційним процедурам, а також рекомендації необхідних змін у засобах контролю, політиках чи процедурах [22]. У контексті інформаційних технологій аудит (auditing) має вирішальне значення для оцінки безпеки систем і даних. IT-аудитори оцінюють засоби контролю / керування, вразливості та потенційні загрози для захисту від витоку даних та кібератак. У контексті розподілених інформаційних систем терміни «audit» та «auditing» мають аналогічне значення, що і в інших областях, але застосовуються спеціально до аудиту інформаційних систем. Аудит (audit) у розподілених інформаційних системах – це процес систематичної перевірки та оцінки компонентів та процесів розподіленої інформаційної системи з метою визначення точності, безпеки, надійності та дотримання стандартів та політик безпеки (приклади: аудит системи керування доступом, аудит мережевих протоколів, аудит захисту від вторгнення, аудит безпеки застосунків і т. д.). Аудит (auditing) у розподілених інформаційних системах – це виконання аудиту (audit). Auditing включає проведення перевірок, аналізу даних, реєстрації подій та виявлення аномалій у розподіленому інформаційному середовищі (приклади: діяльність аудиторів інформаційної безпеки, які аналізують журнали подій та проводять перевірки на рівні мережі та застосунків). Auditing сприяє забезпеченню підзвітності користувачів, запобіганню неналежних дій користувачів та розслідуванню підозрілої активності [30]. Аудит (auditing) розподілених інформаційних систем допомагає організаціям підтримувати надійність, безпеку та відповідність вимогам своєї IT-інфраструктури. Це критично важлива практика для захисту конфіденційних даних, запобігання вразливості та забезпечення правильного функціонування складних взаємопов'язаних систем. Інструменти аудиту (auditing) використовуються для відстеження того, які клієнти отримали доступ до чого і яким чином. Хоча аудит (auditing) насправді не забезпечує жодного захисту від загроз безпеки, журнали аудиту можуть бути надзвичайно корисними для аналізу злому системи безпеки та подальшого вжиття заходів проти зловмисників. З цієї причини зловмисники, як правило, прагнуть не залишати жодних слідів, які могли б зрештою призвести до розкриття їхньої особистості. У цьому сенсі реєстрація доступу в журналах робить атаку більш ризикованою.

Таким чином, очевидно, що безпека розподілених систем багато в чому залежатиме від застосовуваних у ній механізмів, що реалізують відповідні різні правила захисту (політики безпеки). При цьому, реалізуючи відповідні служби захисту, слід враховувати низку важливих аспектів [14, 31]: а) на чому, на кому необхідно сконцентруватися при розробці механізмів захисту: на даних, операціях або користувачах (загалом це часто називають фокусом контролю (focus of control) або об'єктом контролю / керування); б) на якому рівні комп'ютерної системи слід розміщувати механізми безпеки (як правило, комп'ютерну систему можна представити у вигляді деякої багаторівневої моделі, а отже, і організація механізмів безпеки також має бути багаторівневою); в) чому віддається перевага простоті (simplicity) та високому ступеню впевненості (higher assurance) або багатофункціональному середовищу безпеки. Для досягнення високого ступеня впевненості система безпеки має бути досліджена в деталях і якомога вичерпніше. Отже, існує компроміс між складністю та впевненістю. Чим вище рівень впевненості, до якого ви прагнете, тим простіше має бути ваша система. Як наслідок, можна помітити, що багатофункціональні системи безпеки та високий рівень упевненості не легко поєднуються один з одним; г) на кого доцільно покласти завдання щодо визначення та забезпечення безпеки: на центральний об'єкт або на окремі компоненти системи.

Щоб відповісти на ці питання, необхідно розібратися в ряді ключових концепцій та підходів, які допомагають захистити дані та ресурси у розподілених системах. Ось деякі основні з них, що є основою для розробки стратегій та заходів безпеки в розподілених системах і допомагають зменшити ризики та запобігти загрозам безпеці:

– *Об'єкт контролю*. Передбачає використання залежно від специфіки системи та вимог до неї одного з підходів, пов'язаних із концентрацією (фокусуванням) на таких аспектах як: захист безпосередньо асоційованих із застосунком даних; контроль доступу (точна вказівка

того, хто і як може використовувати операції доступу до даних або ресурсів); користувач (вжити заходів, щоб доступ до застосунку мали лише певні користувачі, незалежно від операцій, які вони планують виконувати).

– *Багаторівнева організація механізмів безпеки*. Цей підхід передбачає створення декількох рівнів захисту в системі, кожен з яких виконує конкретні функції, і на кожному з них можуть бути реалізовані відповідні механізми, щоб забезпечити комплексний захист даних та мережевих ресурсів.

– *Простота механізмів захисту.* Використовувати кілька простих механізмів, які легко зрозуміти та яким можна довіряти, завжди є найкращим вибором.

– *Використання криптографічних методів.* Використання криптографічних методів для захисту конфіденційності та цілісності даних під час передачі та зберігання. Наприклад, на рівні передачі зазвичай використовуються протоколи безпечного зв'язку, такі як SSL/TLS, на рівні зберігання – шифрування (у тому числі так зване прозоре шифрування – Transparent Data Encryption – TDE [32]).

– *Організація безпечних каналів* (*secure channels*). Безпечний канал у розподілених інформаційних системах є захищеним засобом зв'язку, який забезпечує конфіденційність і цілісність інформації, що передається між різними компонентами або вузлами РІС, а також здійснює перевірку справжності учасників інформаційного обміну та їх прав доступу до певних ресурсів системи. Тобто безпечний канал забезпечує захист відправників та одержувачів повідомлень від перехоплення (повідомлення не можуть бути підслухані зловмисниками), модифікації та фальсифікації / підробки (здійснюється за допомогою протоколів взаємної автентифікації та цілісності повідомлень). Безпечний канал повинен надавати захист від різних видів атак, таких як: людина посередині (man-in-the-middle), повторне відтворення (replay attack), відмова в обслуговуванні (DoS), перехоплення сеансу (session hijacking), фішингові атаки та інші. Зазвичай не потрібно вводити захист від переривання зв'язку. У РІС використовуються різні технології та протоколи для створення безпечних каналів. Важливо вибирати відповідні з них залежно від конкретних потреб і вимог системи. Нижче наведено деякі загальні технології та протоколи, які використовуються для створення безпечних каналів у розподілених системах: 1) TLS (Transport Layer Security) / SSL (Secure Sockets Layer) протоколи – забезпечують безпечний зв'язок через Інтернет та інші мережі; зазвичай використовуються для захисту веб-трафіку (HTTPS) та електронної пошти (SMTP з TLS/SSL); 2) віртуальні приватні мережі (VPN – Virtual Private Network) – створюють безпечне зашифроване з'єднання через загальнодоступну мережу, забезпечуючи конфіденційність та безпеку даних; 3) IPsec (Internet Protocol Security) – набір протоколів, що використовуються захисту зв'язку лише на рівні IP (Internet Protocol), часто як і в VPN; 4) SSH (Secure Shell) – криптографічний мережевий протокол для безпечного віддаленого доступу до систем та передачі даних; 5) Kerberos – мережевий протокол автентифікації, який використовує квитки (tickets) та криптографію з симетричним ключем (вимагає наявності довіреної третьої сторони – центру сертифікації / розподілу ключів) для забезпечення безпечної автентифікації в незахищеній мережі.

– *Контроль доступу* (access control). Контроль доступу відповідно до визначень [22, 24] – процес задоволення чи відхилення конкретних запитів на: 1) отримання та використання інформації та пов'язаних з нею послуг з обробки інформації; 2) вхід на певні фізичні об'єкти (наприклад, федеральні будівлі, військові об'єкти, прикордонні переходи). У контексті статті нас насамперед цікавитиме перша частина цього визначення, тобто, рішення про дозвіл або заборону суб'єкту доступу до об'єктів системи (мережі, даним, застосунку, сервісу тощо) [22].

– *Безпечне іменування* (secure naming). Основна ідея технології безпечного іменування полягає в тому, щоб вбудувати в самі імена ресурсів (наприклад, доменні імена, імена файлів, URL тощо) інформацію про безпеку та справжність цих ресурсів. Це робиться з метою покращення безпеки та забезпечення автентифікації ресурсів без необхідності покладатися

на зовнішні джерела або центральні установи. Ключовими концепціями та особливостями технології безпечного іменування є: а) самодостатність (ім'я ресурсу містить у собі інформацію про свою справжність або цифровий підпис; немає необхідності звертатися до центральних установ або сертифікаційних органів для перевірки справжності ресурсу); б) захист від підробки (від фальсифікації та атак, пов'язаних із зміною імен ресурсів); в) криптографічна безпека (дані, включені в ім'я ресурсу (наприклад, цифровий підпис), забезпечують криптографічний захист, який може бути перевірений клієнтським пристроєм або користувачем); г) складність організації атак (технологія ускладнює завдання зловмисникам, які намагаються атакувати ресурси, оскільки вони повинні підробити або обійти криптографічний захист, вбудований в імена ресурсів).

– *Управління безпекою.* За останні кілька десятиліть дисципліна управління IT-безпекою значно змінилася. Це сталося у відповідь на швидке зростання мережевих комп'ютерних систем та залежність від них, а також пов'язане з цим зростання ризиків для цих систем. Останнім часом було опубліковано низку національних та міжнародних стандартів (серія стандартів ISO 27000, NIST, у тому числі NIST SP 800-18 Rev.1, 2006 р., NIST SP 800-30 Rev.1, 2023 р., NIST SP 800-53, Rev. 5, 2020 р.). Вони є консенсусом щодо передової практики в цій галузі [33]. Управління безпекою загалом – це широка сфера управління, пов'язана з управлінням активами, фізичною безпекою та функціями безпеки людських ресурсів; це процес планування, організації, впровадження, контролю та безперервного поліпшення системи безпеки в організації. Управління безпекою означає відповідальність та дії, необхідні для управління середовищем безпеки, включаючи політики та механізми безпеки [34]. Управління безпекою є ключовим елементом будь-якої організації, особливо у контексті сучасних загроз, пов'язаних із кібербезпекою та тероризмом. Воно дозволяє мінімізувати ризики та забезпечити захист важливих ресурсів та інтересів організації. Управління інформаційною безпекою є важливим елементом у забезпеченні безпеки даних в організаціях, компаніях та установах, тому що воно допомагає: 1) захистити конфіденційність даних (таких як персональні дані клієнтів, банківські дані, інтелектуальну власність тощо); 2) запобігти кібератакам, зламам та іншим загрозам, які можуть призвести до витоку конфіденційних даних, порушення цілісності, доступності даних, завдаючи серйозної шкоди організації; 3) організаціям забезпечувати безпеку даних своїх клієнтів відповідно до вимог законів, нормативних документів та різних правил; 4) зберегти репутацію організації, шляхом запобігання порушенням безпеки даних, які можуть завдати їй серйозної шкоди; 5) підвищити ефективність функціонування організації, зменшити витрати на відновлення після інцидентів безпеки; 6) запобігти витоку інформації, незаконному використанню даних, шкідливим діям з боку співробітників тощо. Якщо говорити про *управління безпекою в розподілених системах*, то це комплекс заходів та процесів, спрямованих на безпеку розподілених систем, включаючи захист від несанкціонованого доступу, шкідливих програм, витоку інформації та інших загроз. Такий комплекс заходів та процесів включає різні аспекти, такі як: автентифікацію та авторизацію користувачів і пристроїв в системі; керування доступом до ресурсів та даних у розподіленій системі; моніторинг подій та виявлення загроз безпеці; управління ризиками; розроблення політик та процедур, що визначають правила та процеси, необхідні для забезпечення безпеки; реагування на загрози, що виникли, і їх запобігання; управління механізмами, що забезпечують конфіденційність, цілісність та доступність даних, що зберігаються в системі та передаються між пристроями в розподіленій системі; забезпечення відповідності розподіленої системи відповідним стандартам безпеки, нормам та галузевим вимогам, таким як GDPR, HIPAA або PCI DSS; навчання користувачів та адміністраторів системи передовим методам забезпечення безпеки та підвищення поінформованості про потенційні загрози та атаки соціальної інженерії та деякі інші.

– *Безпека з нульовою довірою* (*zero trust security*). *Нульова довіра* (zero trust – ZT) є набором концепцій та ідей, призначених для мінімізації невизначеності при забезпеченні правильних рішень про доступ з найменшими привілеями для кожного запиту до інформа-

ційних систем та служб в умовах, коли мережа вважається скомпрометованою [35]. *Архітектура нульової довіри* (zero trust architecture – ZTA) – це план кібербезпеки підприємства, який використовує концепції нульової довіри та включає взаємовідносини / взаємозв'язки компонентів, планування робочих процесів та політики доступу. Таким чином, підприємство з нульовою довірою – це мережева інфраструктура (фізична та віртуальна) та оперативні політики, які діють для підприємства як продукт плану архітектури з нульовою довірою. Принципи моделі «нульової довіри» є сучасним підходом до забезпечення інформаційної безпеки, який передбачає, що не можна довіряти жодному користувачеві, пристрою чи компоненту всередині або поза корпоративної мережі. Ця модель закликає до безперервної перевірки та автентифікації всіх суб'єктів та ресурсів, навіть тих, що знаходяться всередині мережі. Gartner [36] рекомендує організаціям впроваджувати концепцію нульової довіри, щоб насамперед покращити зниження ризиків для найважливіших активів, оскільки саме тут буде отримано найбільшу віддачу від зниження ризиків (при цьому фахівцями Gartner уточнюється, що цей підхід не вирішує всіх завдань безпеки). До 2026 р. Gartner прогнозує, що 10 % великих підприємств матимуть зрілу та вимірну програму нульової довіри [37]. У 2022 р. прибутки ринку ZTNA (zero trust network access) зросли на 80,6 % [38].

Далі розглянемо детальніше деякі з перерахованих вище ключових концепцій та підходів, які допомагають захистити дані та ресурси у розподілених системах.

2.1. Багаторівнева організація механізмів безпеки

Важливим моментом розробки безпечних систем є вирішення, скільки рівнів повинні мати механізми безпеки. Рівень у цьому контексті пов'язаний із логічною організацією системи, що складається з кількох шарів / рівнів. Якщо підійти до розгляду організації системи забезпечення безпеки в контексті рівнів еталонної моделі OSI (Open Systems Interconnection) як концептуальної основи, усвідомлюючи при цьому, що структура розподіленої системи включає окремі рівні для застосунків, проміжного програмного забезпечення, служб та ядра операційної системи, то в у цьому випадку механізми безпеки можуть бути розподілені за |рівнями таким чином:

1. Фізичний рівень. На цьому рівні можна впровадити заходи безпеки для захисту фізичної інфраструктури, такі як контроль доступу до центрів обробки даних, систем відеоспостереження та систем виявлення вторгнень у серверні приміщення.

2. Канальний рівень. На цьому рівні можуть застосовуватися механізми шифрування та автентифікації для захисту передачі даних мережевими каналами. Як приклади заходів безпеки можна навести VPN та протоколи шифрування на канальному рівні.

3. Мережевий рівень. На цьому рівні можна застосувати такі рішення, як використання міжмережевого екрану, сегментацію мережі, системи виявлення та запобігання вторгненням для захисту від мережевих атак.

4. Транспортний рівень. На цьому рівні можна застосувати криптографічні протоколи SSL/TLS для шифрування даних під час передачі.

5. Сеансовий рівень. На цьому рівні можуть застосовуватися механізми керування сеансами та автентифікації на основі сеансів для забезпечення безпеки сеансів зв'язку між об'єктами мережі.

6. Рівень представлення. Механізми безпеки на рівні представлення можуть включати перетворення формату, шифрування даних для їх захисту під час представлення.

7. Прикладний рівень. На цьому рівні заходи безпеки можуть включати автентифікацію користувачів, контроль доступу та захист від шкідливих програм.

Важливо відзначити, що вибір механізмів безпеки та їх реалізація мають бути адаптовані до конкретних вимог безпеки організації та ландшафту загроз (threat landscape). Крім того, чітко визначена політика безпеки та регулярні оцінки безпеки є найважливішими компонентами комплексної стратегії безпеки. Але, з іншого боку, як визначити, чи правильно політика визначає необхідний рівень та тип безпеки вузла розподіленої системи? Як відомо [39],

безпека ґрунтується на припущеннях, специфічних для необхідного типу безпеки та середовища, в якому вона має застосовуватися. Коли хтось зрозуміє припущення, на яких засновані його політики, механізми та процедури безпеки, він дуже добре розумітиме, наскільки ефективні ці політики, механізми та процедури. І в цьому випадку важливу роль грає поняття «довіри». Суб'єкт / сутність (entity) заслуговує на довіру, якщо є достатньо достовірних доказів, що дозволяють вважати, що система відповідатиме набору заданих вимог. Довіра – це міра надійності / достовірності (trustworthiness), заснована на наданих доказах [39]. Різниця між довірою та безпекою важлива. Система або безпечна, або ні (з урахуванням різних випадковостей), але питання про те, чи вважає користувач / клієнт систему безпечною, є питанням довіри [20].

На якому рівні розміщуються або повинні розміщуватись механізми безпеки, залежить від довіри користувача до того, наскільки безпечні служби на конкретному рівні. Безпека може бути забезпечена шляхом розміщення пристроїв шифрування на кожному магістральному комутаторі. Ці пристрої автоматично шифрують і розшифровують пакети, що відправляються між вузлами, але не забезпечують безпечного обміну даними між вузлами на одному й тому самому вузлі, тобто в межах однієї локальної мережі. Якщо Користувач 1 на вузлі A надсилає повідомлення Користувачеві 2 на вузол B і переймається тим, що його повідомлення буде перехоплено, він має бути впевненим у тому, що шифрування між вузлами працює коректно. Це означає, наприклад, що він повинен бути впевнений, що системні адміністратори на обох вузлах вжили належних заходів проти несанкціонованого доступу до пристроїв (втручання у роботу пристроїв, що шифрують).

Якщо тепер припустити, що Користувач 1 не довіряє захисту трафіку між вузлами, тоді він може прийняти рішення про необхідність використання власних заходів захисту. Наприклад, використовувати TLS (Transport Layer Security) для безпечного надсилання повідомлень через TCP-з'єднання. У цьому випадку Користувач 1, довіряючи TLS, вважає, що TLS є безпечним. У розподілених системах механізми безпеки часто розміщуються лише на рівні проміжного програмного забезпечення (ПЗ). Якщо Користувач 1 не довіряє TLS, він може використовувати локальну безпечну службу виклику віддалених процедур (Remote Procedure Call, RPC). Але йому, знову ж таки, доведеться довіряти службі RPC, у тому, що ця служба обіцяє, наприклад, запобігання витоку інформації або належну автентифікацію клієнтів та серверів. Хоча слід пам'ятати, що службам безпеки, розміщеним на рівні проміжного ПЗ розподіленої системи, можна довіряти тільки якщо служби, на які вони покладаються, є дійсно безпечними. Наприклад, якщо захищена служба RPC частково реалізована за допомогою TLS, то довіра до служби RPC залежить від того, наскільки довіряють TLS. Якщо TLS не є довіреною службою, то не може бути довіри і до безпеки служби RPC. Залежність між службами щодо довіри призводять до поняття довірена обчислювальна база (Trusted Computing Base, TCB). TCB – це набір всіх механізмів безпеки комп'ютерної системи (у тому числі й розподіленої), які необхідні для дотримання політики безпеки і яким слід довіряти. Тому, чим менше TCB (менше механізмів, які є критичними при їх компрометації, яка з великою ймовірністю поставить під загрозу безпеку системи в цілому), тим краще для безпеки (менше можливостей для атак). Якщо розподілена система побудована як проміжне ПЗ у існуючій мережній операційній системі, її безпека може залежати від безпеки базових локальних операційних систем. Тобто TCB в розподіленій системі може включати локальні операційні системи на різних вузлах.

2.2. Простота як переважний принцип проектування механізмів захисту

Ще одна важлива проблема проектування, пов'язана з ухваленням рішенням про те, на якому рівні розміщувати механізми безпеки, полягає у простоті. Проектування захищеної комп'ютерної системи вважається складним завданням, але якщо розробник системи зможе використовувати кілька простих механізмів, які легко зрозуміти і яким довіряють, це буде ефективніше. Однак слід враховувати, що для реалізації політик безпеки не завжди можливе

використання лише простих механізмів. Звернемося ще раз до випадку, коли Користувач 1 хоче надіслати повідомлення Користувачеві 2. Шифрування на канальному рівні – це простий та зрозумілий механізм захисту від перехоплення трафіку повідомлень між вузлами. Однак потрібно набагато більше, якщо Користувач 1 хоче бути впевненим, що тільки Користувач 2 отримає повідомлення. А саме потрібні послуги автентифікації на рівні користувача. При цьому Користувачеві 1, можливо, знадобляться знання про принципи роботи цих сервісів, щоб довіряти їм. Тому для автентифікації на рівні користувача може знадобитися хоча б уявлення про криптографічні ключі, електроні цифрові сертифікати, незважаючи на той факт, що багато служб безпеки автоматизовані та приховані від користувачів. В інших випадках сам застосунок є за своєю суттю складним, а впровадження безпеки додатково ускладнює його. Прикладом таких застосунків є застосунки, що включають складні протоколи захисту, зокрема, цифрові платіжні системи. Ідеальний список вимог для онлайн-платежів в електронній комерції може виглядати приблизно так [40]:

1. Конфіденційність. Механізм платежів повинен забезпечувати додаткові рівні конфіденційності, дозволяючи розкривати деталі транзакції лише сторонам, кого визначили покупець або продавець.

2. Цілісність. Повинна підтримуватись цілісність транзакції (фальсифікація або зміна деталей транзакції має бути практично неможливою).

3. Автентифікація. Повинні надаватися методи автентифікації взаємодіючих сторін та/або автентифікації повідомлень, які використовуються для авторизації платежів, щоб запобігти шахрайству.

4. Невідмовність. Повинна забезпечуватися така властивість інформаційної безпеки як невідмовність (щоб захистити як продавця, так і покупця від неправдивих заяв).

5. Доступність. Механізм платежів повинен дозволяти покупцям та продавцям брати участь у платіжних транзакціях, коли це необхідно.

6. Реалізація. Деталі реалізації мають бути абстраговані / приховані (з метою спрощення складності), а також забезпечувати інтерфейси (які повинні розроблятися на основі передових практик) із торговими системами.

7. Інтероперабельність. Механізм платежів має бути інтероперабельним, забезпечуючи максимально широкий доступ продавцям та покупцям.

8. Простота використання. Механізм платежів має бути простим для розуміння та використання покупцем.

9. Захист. Правила та політика механізму платежів повинні забезпечувати захист покупців від несумлінних продавців чи шахраїв.

Складність цифрових платежів часто пов'язана з тим, що для здійснення платежу потрібна взаємодія кількох дійових осіб. У цих випадках важливо, щоб базові механізми, що використовуються для реалізації протоколів (наприклад, таких як SSL/TLS – використовуються під час онлайн платежів через інтернет (електронна комерція через веб-браузер та SSL/TSL) та 3D Secure – ці протоколи додають додатковий рівень автентифікації під час онлайн платежів, зазвичай через введення пароля або одноразового коду), були відносно простими та зрозумілими. Простота сприятиме довірі користувачів, які працюють із застосунком, і що більш важливо, зможе переконати розробників у відсутності «дірок» у системі захисту.

2.3. Використання для захисту криптографічних методів

У захисті розподілених систем особливо важливу роль відіграє криптографія (галузь знань, що втілює в собі принципи, засоби та методи перетворення даних з метою приховування їх семантичного змісту, запобігання їх несанкціонованому використанню або запобігання їх невиявленій модифікації [22, 41]). Справді, створення захищеної системи неможливе без застосування криптографічних методів, що надають у розпорядження розробника засоби, що забезпечують певні гарантії ступеня захисту. Основна ідея застосування цих методів є

простою. Розглянемо відправника B, який хоче передати повідомлення m одержувачу O. Щоб захистити повідомлення від загроз безпеки, відправник спочатку зашифровує його в повідомлення m', а потім надсилає повідомлення m' одержувачу O. O, у свою чергу, повинен розшифрувати отримане повідомлення та отримати оригінал m. Шифрування та розшифрування здійснюються шляхом застосування криптографічних методів з використанням ключів. Вихідне повідомлення називається відкритим текстом (plaintext – P). Зашифроване повідомлення називається зашифрованим текстом (ciphertext – C), яке формально можна подати у такому вигляді: $C = E_K(P)$, де K – ключ для шифрування/розшифрування. Аналогічно можна представити операцію розшифрування: $P = D_K(C)$. При цьому слід пам'ятати, що при передачі повідомлення у вигляді зашифрованого тексту C можливі три різні атаки, від яких необхідно захищатись. По-перше, зловмисник може перехопити повідомлення, причому про це можуть не бути обізнані ні відправник B, ні одержувач O. Зрозуміло, якщо надіслане повідомлення було зашифровано таким чином, що його неможливо розшифрувати, не маючи відповідного ключа, перехоплення буде марним: зловмисник побачить лише незрозумілі дані. Хоча в деяких випадках самого факту передачі повідомлень буває достатньо, щоб зловмисник міг зробити відповідні висновки (наприклад, у період економічних криз, воєнних дій тощо). По-друге, можлива модифікація повідомлення. Змінити відкритий текст легко, але модифікувати зашифрований текст, який був належним чином зашифрований, набагато складніше, тому що зловмиснику спочатку доведеться розшифрувати повідомлення, перш ніж він зможе суттєво змінити його. Крім того, зловмисник також повинен правильно зашифрувати його, інакше одержувач може помітити, що повідомлення було підроблено. Третій тип атаки – це коли зловмисник вставляє зашифровані повідомлення у систему комунікації, намагаючись переконати одержувача O в тому, що це повідомлення отримано від відправника B. І знову, шифрування може допомогти захиститися від подібних атак. При цьому, слід зазначити, що якщо порушник може змінювати повідомлення, він може вставляти повідомлення. Тому сьогодні існують різні криптографічні примітиви та системи (у тому числі симетричні, асиметричні (з відкритим ключем) системи, геш-функції та деякі інші), що дозволяють успішно боротися з переліченими типами атак. Це окрема тема для обговорення, подробиці якої у цій роботі не розглядатимуться.

Як відомо, дані можуть перебувати в трьох станах (рис. 1) [42]: *у стані спокою* (at rest), *в дорозі* або *в русі* (in transit або in motion) та *у використанні* (in use). Дані в дорозі або дані в русі – це дані, що активно переміщаються з одного місця в інше, наприклад через Інтернет або через приватну мережу (надсилання електронної пошти, здійснення онлайн-купівлі, доступ до веб-сторінки, передача файлів по мережі). Дані в стані спокою – це неактивні дані, які фізично розміщуються у комп'ютерних сховищах даних у будь-якій цифровій формі (наприклад, файли на жорсткому диску комп'ютера, дані в базі даних, у хмарному сховищі, архіви, дані на USB-накопичувачі, до якого не здійснюється активний доступ, резервні копії за межами офісу (на дисках, стрічках) або в хмарі тощо), і які в даний час не використовуються. Дані у використанні – це дані, які активно обробляються або використовуються комп'ютером або застосунком (наприклад, перегляд інформації на екрані комп'ютера, обробка даних за допомогою програмного забезпечення, виконання запитів до бази даних («активні дані» в контексті знаходження в базі даних або маніпулювання ними з боку застосунку), потокове відео в реальному часі тощо) в даний момент. Кожен із цих трьох станів даних обробляється за допомогою певного набору технологій, що надаються рішеннями щодо запобігання втраті, витоку, спотворенню даних. Безпека даних у дорозі забезпечується за рахунок шифрування даних перед передачею, реалізації різних протоколів автентифікації, перевірки цілісності даних та

Рис. 1. Три стани даних

деяких інших механізмів, що захищають дані при їх передачі по мережах і запобігають їх підслуховування або перехоплення. Ідея захисту даних у дорозі була розглянута вище, нижче також будуть розглянуті деякі заходи їх захисту.

Захист даних у стані використання зазвичай включає контроль доступу, автентифікацію, шифрування даних під час обробки (захищає дані в пам'яті від злому або крадіжки [42]) і забезпечення безпеки середовища обчислень. Технології, такі як апаратні модулі безпеки (hardware security modules – HSM) [43], можуть використовуватися для захисту криптографічних ключів, коли вони знаходяться у використанні. Захист даних у стані спокою включає заходи, такі як шифрування, контроль доступу, автентифікація та фізична безпека (наприклад, закриті шафи, безпечні сховища). Наприклад, комплексна стратегія безпеки Google включає шифрування в стані спокою, яке допомагає захистити вміст клієнтів від зловмисників. Зашифровується весь контент клієнтів Google, що зберігається, без будь-яких дій з боку останніх. У Google Cloud Spanner є три рівні шифрування. Дані в стані спокою розбиваються на фрагменти підфайлів для зберігання і кожен фрагмент шифрується на рівні сховища за допомогою окремого ключа шифрування [44]. Розмір кожного фрагмента може досягати кількох гігабайт. Ключ, який використовується для шифрування даних у блоці, називається ключем шифрування даних (DEK – data encryption key). Два фрагменти не будуть мати однаковий DEK, навіть якщо вони належать одному і тому ж клієнту або зберігаються на одному комп'ютері. Якщо фрагмент даних оновлюється, він шифрується за допомогою нового ключа, а не повторним використанням існуючого ключа. Такий поділ даних, у кожному з яких використовується свій ключ, обмежує ризик потенційної компрометації ключа шифрування даних лише цим блоком. Через великий обсяг ключів у Google та необхідності малої затримки та високої доступності ці ключі зберігаються поруч із даними, які вони шифрують. DEK зашифровуються («обгортаються») за допомогою ключа шифрування ключів (KEK – key encryption key). Нарешті, кожен KEK шифрується ключем шифрування, яким керує клієнт (customer-managed encryption key). Google за допомогою алгоритму AES шифрує дані перед записом їх у систему зберігання БД або на апаратний диск. Шифрування вбудовано у всі системи зберігання. Кожен блок даних має унікальний ідентифікатор. Списки контролю доступу (ACL – access control lists) допомагають гарантувати, що кожен фрагмент може бути розшифрований лише службами Google, які працюють з авторизованими ролями, яким надається доступ лише в даний момент часу. Це обмеження доступу допомагає запобігти доступу до даних без авторизації, зміцнюючи безпеку та конфіденційність даних [45].

Широке поширення для забезпечення безпеки баз даних набула так звана технологія «прозорого шифрування даних» (TDE) [32]. Завдання TDE полягає у забезпеченні захисту даних, що зберігаються на таких носіях, як диски та магнітні стрічки, який необхідний відповідно до багатьох національних та/або міжнародних нормативних документів та правил, таких як Закон Сарбейнза – Окслі (Sarbanes-Oxley) [46], який значно посилює вимоги до фінансової звітності та процесу її підготовки, Закон про переносимість та відповідальність медичного страхування (HIPAA) [47], стандарт безпеки даних індустрії платіжних карток (PCI DSS) [48] тощо. TDE – це технологія шифрування баз даних на жорсткому диску та на будь-якому носії резервного копіювання на рівні файлів. Вона може використовуватися для забезпечення високого рівня безпеки стовпців, таблиць та табличних просторів. Прозоре шифрування даних використовується для шифрування та розшифровування даних та файлів журналів, відповідно, шифруючи дані перед їх записом на диск і розшифровує дані перед їх поверненням у застосунок. Цей процес виконується лише на рівні SQL, він повністю прозорий для застосунків і користувачів. При цьому TDE не захищає ні дані під час передачі, ні дані під час використання. Техніка TDE властива різним системам керування базами даних (СКБД). Прозоре шифрування даних використовується у продуктах компаній Microsoft, IBM, Oracle та деяких інших для шифрування файлів бази даних. Приклад прозорого шифрування даних для таблиць БД Oracle наведено на рис. 2.

Рис. 2. Приклад прозорого шифрування даних в БД Oracle

Суть прозорого шифрування полягає в тому, що використовується поєднання двох ключів: ключа для кожної таблиці бази даних, який є унікальним та майстер-ключа, що зберігається поза базою даних у гаманці [49]. Технологія прозорого шифрування передбачає, що підмножина стовпців для шифрування відома. Наприклад, якщо в табл. 4 стовпця, як показано на рис. 2, і шифруються стовпці 2 і 3, то Oracle згенерує ключ і використовує його для шифрування даних стовпців. На диску стовпці 1 і 4 будуть збережені у відкритому вигляді, а два інших стовпці – у зашифрованому. При виборі користувачем зашифрованих стовпців Oracle непомітно витягує ключ із «гаманця», розшифровує стовпці та показує їх користувачеві. Якщо диск із даними викрадено, їх неможливо витягти без ключів, які зберігаються в «гаманці», зашифрованому майстер-ключом, який сам по собі теж не зберігається у вигляді відкритого тексту. Внаслідок цього зловмисник не зможе розшифрувати дані, навіть якщо викраде диски або скопіює файли. Також за допомогою прозорого шифрування даних можна зашифрувати табличний простір (в якому зберігаються спільно такі об'єкти бази даних, як індекси, таблиці та інші). Усі об'єкти, створені в зашифрованому табличному просторі, шифруються автоматично, тобто всі дані в зашифрованому табличному просторі зберігатимуться на диску в зашифрованому вигляді. Шифрування табличного простору за допомогою прозорого шифрування є корисним, якщо ви хочете захистити всю таблицю, а не тільки окремі стовпці [50].

У NewSQL БД NuoDB підтримується прозоре шифрування даних, аналогічно використовуваному в Oracle Database, Microsoft SQL Server. TDE гарантує, що дані користувача, що зберігаються в архіві, журналі, резервних копіях, spill-файлах (файли для збереження проміжних даних, коли в пам'яті недостатньо пам'яті для виконання запиту) будуть зашифровані перед записом на диск. Інформація NewSQL БД SingleStore, включаючи файли даних, резервні копії та журнали, також захищається за допомогою прозорого шифрування CipherTrust Transparent Encryption від Thales [45].

Однак слід знати і пам'ятати, що TDE не є повномасштабною системою шифрування і не повинна використовуватись у такій якості. Для отримання комплексного рішення слід створити власний інструмент, зокрема, використовуючи можливості конкретної СКБД.

2.4. Безпечні канали

При розгляді питань безпеки у розподілених системах доречно звернутися до базової моделі їх організації – моделі клієнт-сервер. Це пов'язано, в першу чергу, з тим, що забезпечення безпеки розподіленої системи зводиться до двох основних аспектів [14]. Перший з них полягає в тому, як забезпечити безпеку зв'язку між клієнтами та серверами. Безпечний зв'язок у загальному випадку вимагає автентифікації взаємодіючих сторін, забезпечення цілісності повідомлень, а також конфіденційності. При цьому є особливості у принципах захисту зв'язку між клієнтом та групою реплікованих серверів, які також необхідно враховувати. Другий аспект – авторизація, яка пов'язана з проблемою контролю доступу клієнта до ресурсів сервера.

Питання захисту зв'язку між клієнтами та серверами доцільно розглядати з точки зору створення так званого безпечного каналу між сторонами, що взаємодіють. Безпечний канал (secure channel) – це шлях передачі даних між двома об'єктами або компонентами, який забезпечує конфіденційність, цілісність та захист від повторного відтворення, а також взаємну автентифікацію між об'єктами або компонентами. Безпечний канал (іноді його називають довіреним каналом (trusted channel) [51]) може бути забезпечений за рахунок використання прийнятих криптографічних, фізичних чи процедурних методів або їх комбінації. Далі

коротко розглянемо питання, пов'язані з автентифікацією взаємодіючих сторін, конфіденційністю повідомлень, їх цілісністю, а також особливості безпечної групової взаємодії з кількістю учасників більше двох.

Автентифікація як важливий компонент безпеки інформаційних систем.

Автентифікація є одним із важливих компонентів безпеки інформаційних систем. Згідно з нормативними документами [22, 25] *автентифікація* – це перевірка особи користувача, процесу або пристрою, часто як попередня умова для надання доступу до ресурсів в інформаційній системі. Іншими словами, автентифікація полягає у перевірці автентичності користувача, процесу або пристрою за пред'явленим ідентифікатором. Така перевірка повинна унеможливлювати фальсифікацію сутностей (користувачів, процесів, пристроїв) у системі та їх компрометацію. Без автентифікації зловмисник може отримати доступ до конфіденційної інформації або виконати небажані дії у системі від імені іншого користувача. При цьому слід зазначити, що автентифікація та цілісність повідомлень пов'язані один з одним та їх доцільно розглядати в сукупності.

Автентифікація на основі загального секретного ключа.

Розглянемо спочатку протокол автентифікації на основі спільного секретного ключа, який вже використовується Користувачем 1 та Користувачем 2. І поки неважливо, яким безпечним способом вони отримали цей спільний секретний ключ. Для опису протоколу введемо деякі позначення.

Для стислості позначимо Користувачів 1 і 2 як $U1$ і $U2$ відповідно. Їхній спільний ключ позначимо як $K_{U1,U2}$. Протокол використовує загальний підхід, при якому одна сторона запитує в іншої відповідь, яка може бути правильною, тільки якщо інша знає спільний секретний ключ. Такі рішення відомі як протоколи «виклик-відповідь».

У випадку автентифікації на основі спільного секретного ключа протокол виконується, як показано на рис. 3. Спочатку Користувач 1 надсилає свій ідентифікатор Користувачеві 2 (повідомлення 1), вказуючи, що він хоче встановити канал зв'язку між ними. Користувач 2 відповідно надсилає виклик Користувачеві 1 (повідомлення 2). Такий виклик може набувати форми випадкового числа. Користувач 1 повинен зашифрувати запит за допомогою секретного ключа $K_{U1,U2}$, яким він ділиться з Користувачем 2, та повернути зашифрований виклик Користувачеві 2 (повідомлення 3). Коли Користувач 2 отримує відповідь $K_{U1,U2}(R_{U2})$ на свій виклик R_{U2}, він може знову розшифрувати повідомлення, використовуючи спільний ключ, щоб переглянути, чи воно містить R_{U2}. Якщо це так, він знає, що Користувач 1 знаходиться на іншій стороні, тому що ніхто більше не міг зашифрувати R_{U2} за допомогою $K_{U1,U2}$.

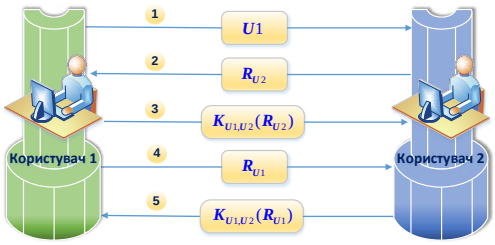


Рис. 3. Автентифікація на основі загального секретного ключа

Іншими словами, Користувач 2 тепер переконався, що він дійсно контактує з Користувачем 1. Однак, зверніть увагу, що Користувач 1 ще не підтвердив, що це дійсно Користувач 2 з іншого боку каналу. Тому він надсилає виклик R_{U1} (повідомлення 4), на який Користувач 2 відповідає, повертаючи $K_{U1,U2}(R_{U1})$, (повідомлення 5). Коли Користувач 1 розшифрує його

за допомогою $K_{U1,U2}$ та побачить свій R_{U1}, він буде впевнений, що контактує з Користувачем 2. Слід зазначити, що, налаштовуючи цей протокол для покращення його продуктивності, можна порушити його коректність, що позначиться на безпеці. Про це свідчать дослідження, які проводять розробники криптографічних протоколів протягом багатьох років [14].

Автентифікація з використанням центру розподілу ключів.

Однією із проблем використання спільного секретного ключа для автентифікації є масштабованість. Якщо розподілена система містить N хостів і кожному хосту потрібно спільно використовувати секретний ключ з кожним з решти $(N-1)$ хостів, системі в цілому необхідно керувати $N(N-1)/2$ ключами, і кожен хост може керувати $(N-1)$ ключами. Для великих N це стає проблемою. Виходом із цієї ситуації може бути рішення використати Центр розповсюдження ключів (ЦРК). ЦРК розділяє секретний ключ з кожним з хостів, при цьому жодній парі хостів спеціальний спільний секретний ключ не потрібний. Іншими словами, використання ЦРК вимагає управління всього N ключами замість $N(N-1)/2$, що явно є прогресом. Тобто, якщо Користувач 1 хоче встановити безпечний канал з Користувачем 2, він може це зробити за допомогою довіреного ЦРК. Ідея в цілому полягає в тому, що ЦРК роздає ключ Користувачам 1 та 2, який вони можуть використовувати для спілкування один з одним (рис. 4).

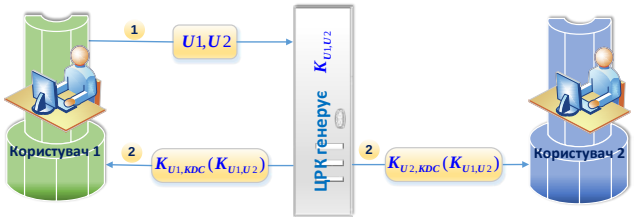


Рис. 4. Принцип використання Центру розповсюдження ключів

Користувач 1 спочатку надсилає повідомлення до ЦРК, вказуючи, що він $(U1)$ хоче спілкуватися з Користувачем 2 $(U2)$. ЦРК повертає повідомлення, що містить спільний секретний ключ $K_{U1,U2}$, який він може використовувати. Повідомлення шифрується секретним ключем $K_{U1,KDC}$, який є спільним для Користувача 1 та ЦРК. Крім того, ЦРК відправляє $K_{U1,U2}$ також Користувачеві 2, але тепер він зашифровується секретним ключем $K_{U2,KDC}$, який є спільним для Користувача 2 та ЦРК. Слід зазначити, що основним недоліком такого підходу є те, що Користувач 1 може захотіти розпочати налаштування безпечного каналу з Користувачем 2 ще до того, як Користувач 2 отримає спільний ключ від ЦРК. Крім того, ЦРК потрібно знайти Користувача 2, щоб передати йому відповідний ключ у цьому циклі налаштування. Ці проблеми можна обійти, якщо ЦРК просто передає повідомлення $K_{U2,KDC}(K_{U1,U2})$ назад Користувачеві 1 і дозволяє йому потурбуватися про з'єднання з Користувачем 2. Це призводить до протоколу, показаному на рис. 5. Повідомлення $K_{U2,KDC}(K_{U1,U2})$ також відоме як квіток. Задача Користувача 1 – передати цей квіток Користувачеві 2.

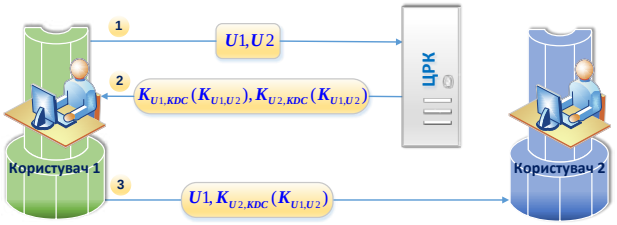


Рис. 5. Протокол встановлення з'єднання між користувачами з використанням талону

Зверніть увагу, що Користувач 2, як і раніше, єдиний, хто може осмислено використовувати квіток, оскільки він єдиний, крім ЦРК, який знає, як розшифрувати інформацію, що міститься в ньому. Протокол, показаний на рис. 5 є варіантом добре відомого протоколу автентифікації з використанням ЦРК – протоколу автентифікації Нідхема – Шредера (Needham-Schroeder) [52].

Автентифікація з використанням криптографії з відкритим ключем.

Автентифікацію користувачів можна здійснювати і без ЦРК, використовуючи можливості криптосистеми з відкритим ключем.

Цілісність та конфіденційність повідомлень.

Як зазначалося вище, крім автентифікації, безпечний канал також повинен забезпечувати цілісність і конфіденційність повідомлень. Конфіденційність легко встановлюється шляхом простого шифрування повідомлення перед його надсиланням. Шифрування може здійснюватися через секретний ключ, наданий одержувачу, або, альтернативно, через відкритий ключ одержувача. Однак забезпечити цілісність повідомлення дещо складніше. А саме, крім автентифікації, є принаймні дві проблеми, пов'язані із забезпеченням цілісності повідомлення, які слід вирішувати. Перша проблема пов'язана з тим, щоб одержувач не міг зловмисно змінювати на свою користь отримане повідомлення і стверджувати, що воно було таким, яким було представлено ним. Друга проблема пов'язана з відправником – щоб він не міг заперечувати, що повідомлення, яке він надіслав, було зовсім іншим, а не таким, яким його представив відправнику одержувач (тобто відправник фактично відмовляється від того, що сам написав). Ці дві проблеми можуть бути вирішені, якщо відправник (Користувач 1) підписує повідомлення у цифровій формі таким чином, що його підпис однозначно пов'язаний з його змістом. Унікальний взаємозв'язок між повідомленням та його підписом запобігає тому, що модифікації повідомлення залишаться непоміченими. Крім того, якщо підпис відправника може бути перевірений на автентичність, він не зможе згодом заперечувати той факт, що він підписав повідомлення. Існує кілька проблем із цією схемою, хоча сам по собі протокол правильний. По-перше, дійсність підпису Користувача 1 (відправника) зберігається лише доти, доки закритий / секретний (private) ключ Користувача 1 залишається секретом. Якщо Користувач 1 хоче відмовитись від повідомлення навіть після відправки Користувачеві 2 свого підтвердження, він може заявити, що його особистий ключ був викрадений до того, як повідомлення було надіслано. Інша проблема виникає, коли Користувач 1 вирішує змінити свій закритий ключ (це сприяє підвищенню безпеки). Але як тільки Користувач 1 змінив ключ, його повідомлення, надіслане Користувачеві 2, стає марним. У таких випадках може знадобитися центральний орган, який відстежує зміну ключів на додаток до використання міток часу під час підписання повідомлень.

Ще однією проблемою подібної схеми є те, що Користувач 1 шифрує все повідомлення своїм закритим ключем. Таке шифрування може бути дорогим з точки зору вимог до обробки (або навіть математично нездійсненним, оскільки передбачається, що повідомлення, яке інтерпретується як двійкове число, обмежене заздалегідь певним максимумом), і при цьому насправді в ньому немає необхідності. А в чому є необхідність, то це в тому, щоб унікально пов'язати підпис з єдиним конкретним повідомленням. Дешевшою та практичною схемою є використання дайджесту повідомлення (message digest). Дайджест повідомлення – це результат застосування геш-функції до повідомлення (також відомий як «геш-значення») [53]; геш-значення – бітовий рядок фіксованої довжини, створений геш-функцією [54]; тобто під дайджестом повідомлення можна розуміти бітовий рядок фіксованої довжини h, який був обчислений з повідомлення m довільної довжини за допомогою криптографічної геш-функції H. Якщо m змінити на m', його геш $H(m')$ відрізнятиметься від $h = H(m)$, щоб можна було легко виявити, що відбулася модифікація.

Для цифрового підпису повідомлення Користувач 1 може спочатку обчислити дайджест повідомлення, а потім зашифрувати дайджест своїм закритим ключем, як показано на рис. 6.

Зашифрований дайджест надсилається разом із повідомленням Користувачеві 2. Слід зауважити, що саме повідомлення надсилається у вигляді відкритого тексту (кожен може його прочитати). Якщо потрібна конфіденційність, повідомлення має бути зашифроване відкритим ключем Користувача 2.

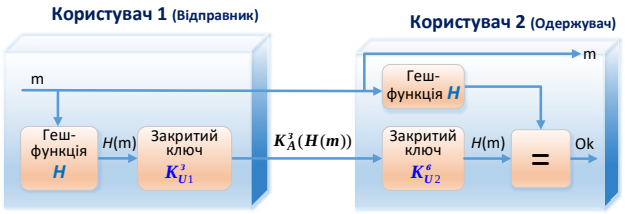


Рис. 6. Цифровий підпис повідомлення за допомогою дайджеста повідомлення

Коли Користувач 2 отримує повідомлення та його зашифрований дайджест, йому потрібно просто розшифрувати дайджест за допомогою відкритого ключа Користувача 1 та окремо розрахувати дайджест повідомлення. Якщо дайджест, отриманий із повідомлення, та розшифрований дайджест збігаються, Користувач 2 знає, що повідомлення було підписано Користувачем 1.

2.5. Контроль доступу

Для кращого розуміння проблем, пов'язаних з контролем доступу (керуванням доступу), доцільно звернутися до простої моделі, наведеної на рис. 7.

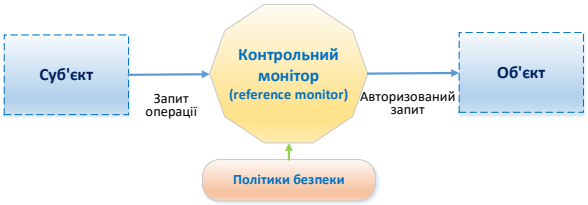


Рис. 7. Загальна модель керування доступом до об'єктів

Модель складається із суб'єктів, які видають запит на доступ до об'єкта. Об'єкт дуже схожий на об'єкти, які розглядалися досі (сервери, пристрої, програми, процеси, дані тощо). Об'єкт можна уявити як інкапсуляцію власного стану та реалізацію операцій над цим станом. Операції об'єкта, які можуть запросити суб'єкти, виконуються через інтерфейси. Суб'єкти найкраще розглядати як процеси, що діють від імені користувачів, але вони також можуть бути об'єктами, які потребують послуг інших об'єктів для виконання своєї роботи. Керування доступом до об'єкта полягає у захисті об'єкта від викликів суб'єктів, яким не дозволено виконувати певні (або ніякі) методи. Крім того, захист може включати питання управління об'єктами, такі як створення, перейменування або видалення об'єктів. Захист забезпечується так званим контрольним монітором / монітором звернень (reference monitor).

На підставі встановлених політик безпеки контрольний монітор визначає, чи може суб'єкт виконувати конкретну операцію. Монітор викликається (наприклад, базовою операційною системою) щоразу, коли викликається об'єкт. Отже, дуже важливо, щоб контрольний монітор сам по собі був захищений від злому, тобто зловмисник не повинен мати доступу до нього. Забезпечити безпеку легше, якщо є чітка модель того, що потрібно захищати та кому і що дозволено робити [14]. Тому невід'ємною частиною будь-якого проекту створення безпеки комп'ютерних систем є наявність моделі безпеки (security model), під якою розуміється формальне уявлення політики безпеки [55]. Сьогодні в комп'ютерних системах знайшли широке поширення моделі безпеки на основі дискреційної, мандатної, рольової політики, а також політики атрибутів.

2.5.1. Дискреційний контроль доступу

Роботи з моделей дискреційного (вибіркового) керування доступом (discretionary access control – DAC) до даних інформаційних систем (ІС) з'явилися ще в 60 – 70-х роках минулого століття. Вони досить широко висвітлені у науковій літературі. Одна з перших таких моделей була розроблена Лемпсоном (Lampson) [56, 57], а потім удосконалена Грехемом (Graham) і Деннінгом (Denning) [58]. Модель Грехема – Деннінга сформувала основу для наступних систем безпеки, наприклад для широко поширеної моделі Харрісона – Руццо – Ульмана – HRU (Harrison – Ruzzo – Ullman) [59]. Крім того, також відомі такі моделі як модель ADEPT-50 [60], п'ятивимірний простір Хартсона [61], модель Take-Grant [62] та деякі інші. Авторами цих моделей було внесено значний внесок у теорію безпеки комп'ютерних систем. Їхні роботи заклали основу для подальшого створення та розвитку захищених ІС.

У теоретичному та практичному плані найбільшого розвитку та застосування отримали дискреційні моделі, засновані на матриці доступу (матриці контролю доступу) – M, яка описує права доступу суб'єктів (S) до об'єктів (O), рядки якої відповідають суб'єктам доступу $s_1, s_2, ..., s_m$, стовпці об'єктам доступу $o_1, o_2, ..., o_n$, а в елементах матриці $M[s_i, o_j]$ записуються дозволені операції (види доступу) $op_1, op_2, ..., op_L$ (наприклад, читання (r_d), запис з модифікацією (w), запис без модифікації (тільки з новим записом або дописуванням у файл) (a), запуск об'єкта на виконання (e)) відповідного суб'єкта над відповідним об'єктом. Як зазначається в монографії [63], за потреби елементи матриці можуть містити вказівники на процедури. Ці процедури виконуються під час кожної спроби доступу до заданого об'єкта. Тим самим рішення про доступ може прийматися на підставі складніших залежностей, не настільки очевидних, як у простій матриці доступу. Ця модель передбачає, що усі спроби доступу до об'єктів перехоплюються і перевіряються спеціальним керуючим процесом. Таким чином, суб'єкт s_i отримає ініційований ним доступ op_l до об'єкта o_j лише у випадку, якщо елемент матриці $M[s_i, o_j]$ має значення op_l. Однак, враховуючи, що системі може знадобитися підтримка тисяч суб'єктів (користувачів) та мільйонів об'єктів, які потребують захисту, реалізація матриці контролю доступу в якості істинної матриці не є підходящим способом. Багато записів у матриці будуть порожніми: один суб'єкт, як правило, матиме доступ до відносно невеликої кількості об'єктів. У цьому випадку доцільно використовувати більш ефективний спосіб. Один із широко застосовуваних підходів полягає в тому, що кожен об'єкт підтримує список прав доступу суб'єктів, які хочуть отримати доступ до об'єкта. По суті це означає, що матриця розподілена по стовпцях по всіх об'єктах, а порожні записи пропущені (рис. 8). Цей тип реалізації призводить до того, що називається списком контролю доступу (ACL). Передбачається, що кожен об'єкт має свій власний ACL, тобто для кожного об'єкта ACL перераховані суб'єкти та їх дозволені права доступу. Інший підхід полягає у розподілі матриці по рядках шляхом надання кожному суб'єкту списку можливостей (capability list), які він має для кожного об'єкта (рис. 9). Іншими словами, можливість відповідає запису в матриці контролю доступу. Відсутність можливості (capability) для конкретного об'єкта означає, що суб'єкт немає прав доступу до цього об'єкту.

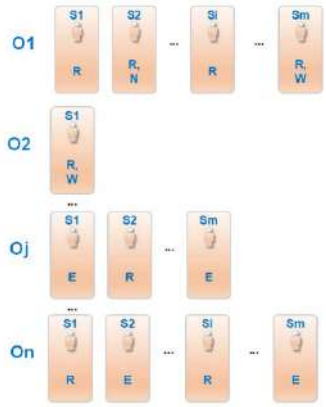


Рис. 8. Список контролю доступу

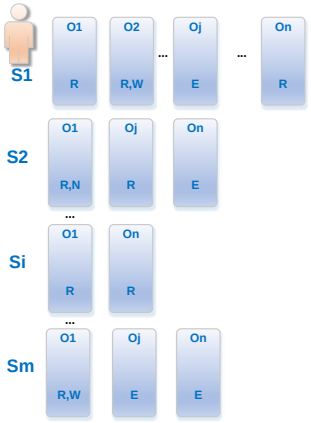


Рис. 9. Список можливостей

Можливість можна порівняти з квитком: її власнику надаються певні права, пов'язані з цим квитком. При цьому квиток має бути захищений від змін його власником. Один підхід, який особливо застосовується у розподілених системах, полягає у захисті списку можливостей за допомогою підпису. Різниця між тим, як контроль доступу ACL та список можливостей використовуються для захисту доступу до об'єкта, показано на рис. 10.

Коли клієнт надсилає запит на сервер, серверний контрольний монітор, використовуючи ACL, перевіряє, чи він знає клієнта і чи дозволено виконувати запитану операцію, як показано на рис. 10, *a*. У разі використання списку можливостей клієнт просто передає свій запит разом зі списком можливостей на сервер. Сервер не зберігає відомостей про клієнта, оскільки вся потрібна йому інформація для відповідних дій міститься у переданій можливості. Отже, серверу потрібно лише перевірити, чи дійсна ця можливість і чи вказана запитана операція у списку можливостей. Цей підхід до захисту об'єктів (на підставі можливостей) показано на рис. 10, *b*.

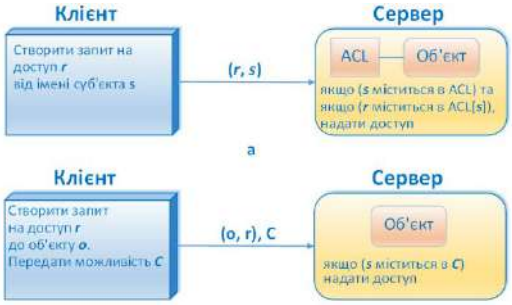


Рис. 10. Порівняння варіантів захисту за допомогою ACL та списку можливостей:
a) використання ACL;
b) використання можливостей

ACL та можливості допомагають ефективно реалізувати матрицю контролю доступу, ігноруючи всі порожні записи. Проте ACL або список можливостей також може стати досить великим, якщо не буде вжито додаткових заходів. Одним із загальних способів скорочення списків контролю доступу є використання доменів захисту (protection domain – набір пар <*об'єкт, права доступу*>). Кожна пара визначає для даного об'єкта, які саме операції дозволено виконувати. Отже, кожного разу, коли суб'єкт запитує виконання операції над об'єктом, контрольний монітор спочатку шукає домен захисту, пов'язаний із цим запитом. Потім, з урахуванням домену, монітор може перевірити, чи дозволено виконання запиту. Існують різні варіанти використання доменів захисту, наприклад, створення груп користувачів (у тому числі ієрархічних), ролей. В цілому ж, існують різні підходи, а також їх комбінації, які використовуються для керування доступом.

2.5.2. Контроль доступу на основі мандатної політики

Якщо в дискреційних моделях керування доступом відбувається шляхом надання суб'єктам повноважень для здійснення певних операцій над конкретними об'єктами, то мандатні моделі керують доступом неявним чином – за допомогою призначення всім сутностям системи (суб'єктам, об'єктам) рівнів безпеки, які визначають всі допустимі взаємодії між ними. Отже, мандатна модель керування доступом (mandatory access control – MAC) не розрізняє сутностей, яким присвоєно однаковий рівень безпеки, і на їх взаємодії обмеження відсутні. Тобто мандатний підхід до розмежування доступу, ґрунтуючись лише на парадигмі ранжо-

ваної довіри, без урахування специфіки інших характеристик суб'єктів і об'єктів, призводить в більшості випадків до надмірності прав доступу для конкретних суб'єктів в межах відповідних класів безпеки, що суперечить самому поняттю розмежування доступу. Тому в тих ситуаціях, коли керування доступом вимагає більш гнучкого підходу, мандатний принцип розмежування доступу доповнюється дискреційним всередині відповідних класів безпеки. У теоретичних моделях для цього вводять матрицю доступу, що розмежовує дозволений за мандатним принципом доступ до об'єктів одного рівня безпеки. Наприклад, у СКБД Oracle реалізація технології мандатного доступу накладається на реалізацію дискреційної моделі. Так, реалізація технології мандатного доступу, що ґрунтується на механізмі OLS (Oracle Label Security), спирається не лише на дискреційну модель доступу (спочатку перевіряються права суб'єкта на виконання відповідної операції над таблицею), а й на механізм VPD (якщо суб'єкт має відповідні привілеї, перевіряється, чи не прикріплені до таблиці будь-які політики VPD – Virtual Private Database). Після всього цього перевіряється наявність політик OLS, призначених таблиці, що захищається: порівнюються мітки, присвоєні окремим рядкам, з авторизацією міток користувачів, дозволяючи або забороняючи доступ [64, 65].

Найбільш широке поширення серед моделей мандатного керування доступу (багаторівневого захисту) отримала модель Белла – ЛаПадули (Bell-LaPadula model) [66]. Графічне представлення моделі Белла – ЛаПадули показано на рис. 11. На рис. 11 суцільна стрілка від об'єкта до суб'єкта показує, що суб'єкт здійснює читання об'єкта (інформаційний потік йде від об'єкта до суб'єкта). Пунктирна стрілка від суб'єкта до об'єкта показує, що суб'єкт здійснює запис в об'єкт (інформаційний потік йде від суб'єкта до об'єкта). Таким чином, направлення інформаційних потоків вказуються стрілками (наприклад, суб'єкт B може читати дані з об'єкта 1, але не може зчитувати дані з об'єкта 3).

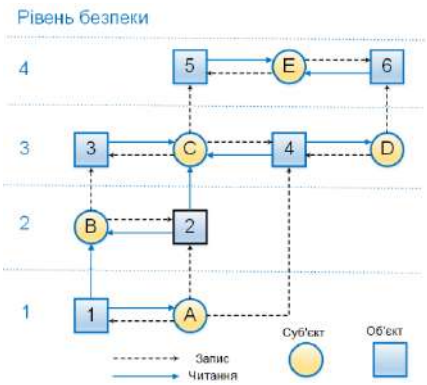


Рис. 11. Багаторівнева модель безпеки Белла-ЛаПадули

Модель Белла – ЛаПадули зіграла величезну роль у розвитку теорії комп'ютерної безпеки, і її положення були введені в якості обов'язкових вимог до систем, що обробляють інформацію, що містить державну таємницю, в стандартах захищених інформаційних систем. Однак при практичній реалізації моделі Белла – ЛаПадула виникає ряд проблем, наприклад, таких як [64]: завищення рівня безпеки; запис наосліп; привілейовані суб'єкти. Розширення моделі Белла – ЛаПадули, пов'язані з пошуком умов і обмежень, що підвищують її безпеку, також не знімають всіх недоліків мандатної доступу. Зокрема, мандатний доступ знімає проблему «троянських програм», але тільки з точки зору небезпечних потоків «зверху вниз».

В цілому ж основним недоліком багаторівневих моделей є неможливість керування доступом до конкретних об'єктів на основі врахування індивідуальних особливостей кожного з суб'єктів. Таким чином, обидва розглянуті вище підходи не в повній мірі можуть ефективно і гнучко управляти безпечним доступом до даних. Отже, обидва підходи як би припускають пошук різних компромісів між ефективністю, гнучкістю і безпекою. Очевидно, що оптимальне вирішення питань безпеки має здійснюватися із застосуванням обох видів моделей.

2.5.3. Керування доступом на основі ролей

Неважко бачити, що розглянуті підходи передбачають пошук різних компромісів між ефективністю, гнучкістю та безпекою. Очевидно, що для забезпечення безпеки систем необхідно використовувати можливості обох розглянутих вище моделей. Такі можливості можна реалізувати, використовуючи модель керування доступом на основі ролей (role-based access control – RBAC) [67]. Основою моделі RBAC є додатково введена в суб'єктно-об'єктну модель системи категорія активних сутностей – роль. Модель керування доступом на основі ролей визначає особливий тип політики, заснований на компромісі між гнучкістю керування

доступом, характерною для дискреційних моделей, і жорсткістю правил контролю доступу, властивою мандатним моделям. У RBAC моделі класичне поняття суб'єкт розділяється на дві складові: користувач і роль. Користувач – це людина, що працює з системою і виконує певні службові обов'язки. Роль – це активно діюча в системі абстрактна сутність, з якою пов'язується певний набір повноважень (привілеїв), необхідних для здійснення певної діяльності. Керування доступом при використанні рольової політики здійснюється в два етапи: 1) створення ролей і визначення їх повноважень (прав доступу до об'єктів); 2) призначення ролей користувачам системи. Слід зазначити, що користувач може бути асоційований з декількома ролями. Дана можливість значно спрощує адміністрування складних систем. Керування доступом на основі ролей вимагає розбиття процесу функціонування системи і роботи користувача на сеанси. RBAC модель описує систему у вигляді наступних множин [67]: U – множина користувачів; R – множина ролей; P – сукупність повноважень на доступ до об'єктів (реалізована, наприклад, у вигляді матриці доступу); C – множина сеансів роботи користувачів з системою. Взаємозв'язок користувачів, ролей, повноважень (привілеїв) і сеансів показаний на рис. 12.

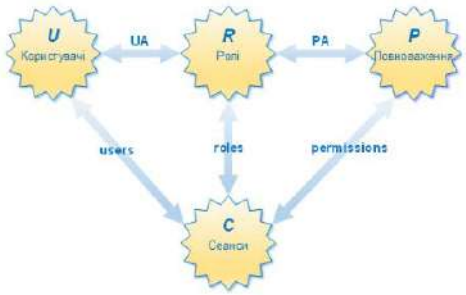


Рис. 12. Взаємозв'язок ролей, повноважень, користувачів і сеансів

Основне правило (критерій безпеки) рольового доступу визначається наступним чином: система вважається безпечною, якщо і тільки якщо будь-який користувач $u \in U$ в системі, що працює в сеансі $c \in C$, може здійснювати дії, що вимагають повноважень $p \in P$, тільки в тому випадку, якщо $p \in permissions(c)$, де $permissions(c)$ – набір доступних у сеансі c повноважень. До переваг моделі керування доступом на основі ролей можна віднести гнучкі, що динамічно змінюються в процесі функціонування систем правила розмежування доступу до ресурсів PIC з великою кількістю користувачів та об'єктів, у тому числі завдяки можливості побудови ієрархій ролей. Оперувати ролями набагато зручніше ніж суб'єктами, оскільки це більш відповідає поширеним технологіям обробки інформації, що передбачають розділення обов'язків і сфер відповідальності між користувачами. Однак для систем керування, доступ в яких ґрунтується на механізмі ролей, немає строгих доказів безпеки відповідно до визначених формалізованих критеріїв. Такий підхід дозволяє отримувати прості і зрозумілі правила контролю доступу, які легко можуть бути застосовані на практиці, але позбавляє систему теоретичної доказової бази. Тому безпека RBAC моделі ґрунтується на контрольних механізмах дискреційних або мандатних моделей, засобами яких регулюється доступ рольових суб'єктів (суб'єктів-ролей) до об'єктів системи.

2.5.4. Керування доступом на основі атрибутів

Керування доступом на основі атрибутів (attribute-based access control – ABAC) – це модель, яка еволюціонує з моделі RBAC. В останні роки цей підхід до керування доступом привернув значну увагу з боку бізнесу, наукових кіл та органів стандартизації. Системи, що підтримують механізм керування доступом на основі атрибутів, здатні реалізовувати концепції як дискреційного контролю доступу (DAC), так і мандатного контролю доступу (MAC). Більш того, системи ABAC можуть забезпечувати рішення керування доступом з адаптацією до ризиків (risk-adaptable access control – RAdAC – контроль доступу, що адаптується до ризику), при цьому значення ризику виражаються у вигляді змінних атрибутів [68]. ACL і RBAC у певному сенсі є особливими випадками ABAC з погляду використовуваних атрибутів [69]. Але при цьому, на відміну від керування доступом на основі ролей, керування доступом на основі атрибутів може виражати складні набори правил (у цьому підході немає обмежень на складність бізнес-правил), що включають можливість оцінки безлічі різних атрибутів. Кожна ситуація оцінюється не з точки зору ролі користувача та дії, яку він хоче вчинити, а з погляду атрибутів, які до них відносяться. Шляхом визначення узгоджених

атрибутів суб'єкта та об'єкта у політиках безпеки ABAC усуває необхідність у явних авторизаціях окремих суб'єктів, необхідних у методі доступу, відмінному від ABAC, що знижує складність керування списками та групами доступу. ABAC визначає доступ (допустимі операції/дії над об'єктами) шляхом зіставлення поточних значень атрибутів сутностей (суб'єкта та об'єкта) та умов середовища з вимогами, зазначеними у правилах керування доступом [69]. Атрибути можна розглядати як характеристики всього, що може бути визначено і чому може бути присвоєно значення. Правила або політики, які можуть бути реалізовані в моделі ABAC, обмежені лише мовою обчислень та безліччю доступних атрибутів. Ця гнучкість дозволяє найбільшій кількості суб'єктів отримати доступ до найбільшої кількості об'єктів без вказівки індивідуальних відносин між кожним суб'єктом і кожним об'єктом, що робить цей підхід керування доступом, ідеальним для багатьох розподілених або швидко мінливих середовищ [70]. ABAC забезпечує підвищену точність визначення політики порівняно з попередніми моделями, дозволяючи використовувати більше вхідних даних для ухвалення рішення щодо контролю доступу, надаючи більший набір можливих комбінацій цих факторів, щоб відобразити ширший та більш визначений набір можливих правил для вираження політики. В результаті можна легко налаштовувати та змінювати політики ABAC у міру зміни потреб.

Хоча в даний час не існує єдиного узгодженого визначення ABAC, існують загальноприйняті визначення з авторитетних джерел та опис його функцій. Одне з таких визначень наведено в роботі [69]: «Керування доступом на основі атрибутів (ABAC) – метод керування доступом, при якому запити суб'єкта на виконання операцій з об'єктами дозволяються або відхиляються на основі призначених атрибутів суб'єкта, призначених атрибутів об'єкта, умов середовища та набору політик, визначених з погляду цих атрибутів та умов». Крім того, у цій же роботі визначаються основні поняття, що містяться у наведеному визначенні та мають безпосереднє відношення до суті даного підходу (моделі) до керування доступом. А саме: атрибути – це характеристики суб'єкта, об'єкта або умов середовища; атрибути містять інформацію, задану парою «ім'я-значення». Суб'єкт – це людина-користувач або не фізична особа (non-person entity – NPE, наприклад, автономна служба або програма, яка видає запити доступу для виконання операцій з об'єктами). Суб'єктам надається один або кілька атрибутів. Передбачається, що суб'єкт та користувач є синонімами. Об'єкт – це системний ресурс, доступ до якого керується системою ABAC, наприклад, пристрої, файли, записи, таблиці, процеси, програми, мережі або домени, які містять або отримують інформацію. Це може бути ресурс або запитаний об'єкт, а також усе, над чим може бути виконана операція суб'єктом, включаючи дані, застосунки, служби, пристрої та мережі. Операція (дія) – це виконання функції на запит суб'єкта над об'єктом. Операції включають читання, запис, редагування, видалення, копіювання, виконання та зміну. Політика – це подання правил або відносин, які дозволяють визначити, чи слід дозволити запитаний доступ, враховуючи значення атрибутів суб'єкта, об'єкта і, можливо, умов середовища. Умови середовища (environment conditions) – операційний чи ситуативний контекст, у якому виникають запити доступу. Умови середовища – це зумовлені показники середовища. Характеристики середовища не залежать від суб'єкта або об'єкта і можуть включати поточний час, день тижня, місцезнаходження користувача або поточний рівень загрози.

Сьогодні існує кілька моделей (базова ABAC [69], HGABAC (Hierarchical Attribute-Based Access Control) [71], LaBAC (Label-Based Access Control) [72] та деякі інші [73]), стандартів (стандарт розширюваної мови розмітки керування доступом (Extensible Access Control Markup Language – XACML) [74], стандарт контролю доступу наступного покоління – NGAC (Next Generation Access Control) [75 – 77], дослідницьких прототипів та продуктів, що втілюють концепції ABAC. У сукупності ці концепції визначають ABAC як систему контролю доступу, яка включає: дані контролю доступу для вираження атрибутів і політик; набір адміністративних операцій (мовою політики) для налаштування даних контролю доступу; набір функцій для реалізації політики щодо запитів на виконання операцій над об'єктами та

для вироблення рішень про доступ для задоволення або відхилення цих запитів на основі поточного стану даних керування доступом. Ця система охоплює чотири рівні функціональної декомпозиції: виконання, ухвалення рішення, адміністрування, дані керування доступом, а також кілька компонентів, що працюють разом. Спільними для всіх моделей ABAC є два типи атрибутів [78]: 1) *атрибут суб'єкта*; кожному суб'єкту призначається набір атрибутів, які можуть представляти особистість суб'єкта, вік, ролі, належність або інші загальні характеристики політики, наприклад рівень допуску; 2) *атрибути об'єкта*; кожному об'єкту призначається набір атрибутів. Атрибути об'єкта (їх іноді називають атрибутами ресурсу [69]) характеризують дані та інші ресурси шляхом ідентифікації колекцій об'єктів, наприклад пов'язаних з певними проектами, застосунками або класифікаціями безпеки.

Атрибути суб'єкта та об'єкта можуть бути призначені їх сутностям або за допомогою адміністративних дій, або за допомогою властивостей або метаданих, які підтримуються системою. На додаток до атрибутів суб'єкта та об'єкта існують атрибути середовища (також відомі як умови середовища), які є загальними для кількох, але не для всіх моделей. Атрибути середовища / навколишнього середовища (environment/environmental attributes) – це атрибути, які залежать від наявності системних датчиків, які можуть виявляти та повідомляти значення. Вони дещо відрізняються від атрибутів суб'єкта та об'єкта (ресурсу), оскільки не є властивостями останніх, а є вимірними характеристиками, що належать до оперативного чи ситуаційного контексту, у якому виникають запити на доступ.

Керування доступом на основі атрибутів показано на рис. 13, де:

1) суб'єкт (користувач) запитує доступ до об'єкта (деякого ресурсу);

2) механізм контролю доступу ABAC ACM (access control mechanism), отримавши запит від суб'єкта, оцінює: а) правила (на основі яких приймається рішення на доступ до об'єкту); б) атрибути суб'єкта (атрибути суб'єкта у профілі користувача можуть включати, наприклад, ідентифікатор, посаду, членство у групах, членство у підрозділах та організаціях, рівень керівництва, рівень допуску та інші критерії ідентифікації; ці дані часто беруться із системи, відділу кадрів чи іншим чином); в) атрибути об'єкта (наприклад, дата створення файлу, його власник, ім'я та тип файлу, конфіденційність даних); г) умови середовища для прийняття рішення (всі атрибути навколишнього середовища пов'язані з контекстуальними факторами, такими, як час і місце спроби доступу, місцезнаходження та пристрій суб'єкта, протокол зв'язку і надійність шифрування; контекстна інформація також може включати сигнали ризику, встановлені організацією, такі як ступінь надійності автентифікації, звичайні моделі поведінки суб'єкта тощо). Потім ABAC ACM визначає, які операції / дії суб'єкт може виконувати з об'єктом;

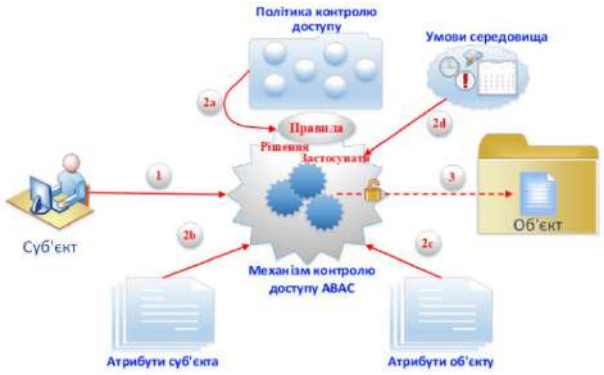


Рис. 13. Керування доступом на основі атрибутів

3. Суб'єкту надається доступ до об'єкта, якщо його авторизовано.

ABAC добре адаптований для керування доступом до розподілених систем, оскільки ABAC надає докладні визначення та мета-атрибути, які підтримують призначення привілеїв на основі структури PIC, яка потребує управління федерацією та автономією між скоординованими системами в PIC [78].

Загалом до переваг ABAC можна віднести: а) гнучкість (дозволяє реалізувати різні політики контролю доступу, обмежені лише широтою спектру доступних атрибутів та можливостями, які може виразити комп'ютерна мова); б) точність контролю доступу (дозволяє більш точно, на відміну від розглянутих вище моделей (MAC, DAC, RBAC), визначити, хто має доступ до яких ресурсів залежно від конкретних атрибутів); в) зниження рівня ризику (завдяки точнішому контролю доступу); г) легкість керування (атрибути та політики можуть

бути легше змінені відповідно до потреб організації без необхідності зміни всієї системи та перевірені); д) можливість задоволення складних вимог безпеки (ABAC може допомогти організаціям дотримуватись нормативних вимог, таких як GDPR або HIPAA, шляхом більш детального контролю доступу до конфіденційних даних).

До недоліків ABAC можна віднести: а) складність реалізації. Реалізація ABAC може бути складною та вимагати значних зусиль на етапі проектування та впровадження. Особливо це актуально для великих та складних систем (адміністраторам необхідно вручну визначати атрибути, призначати їх кожному компоненту та створювати політики на основі різних умов); б) складність адміністрування. Керування політиками ABAC та атрибутами може вимагати високої кваліфікації адміністраторів та спеціалістів з безпеки; в) продуктивність. Використання багатьох атрибутів для прийняття рішень про доступ може вплинути на продуктивність системи, особливо при великій кількості запитів на доступ.

Більш детально з різними модифікаціями моделей ABAC та їх можливостями при розгортанні ABAC у різних архітектурах застосунків (великі дані, веб-сервіси, робочі процеси) та у комерційних продуктах можна ознайомитись у роботі [78].

2.5.5. Використання міжмережевого екрану

Викладені вище моделі контролю доступу можуть чудово застосовуватися при розробці автономної розподіленої системи, яка більш менш ізольована від решти світу. Однак, коли доступ до ресурсів відкривається стороннім користувачам (наприклад, надсилання пошти, доступ до веб-сайтів, надання локальних ресурсів тощо), завдання забезпечення його контролю суттєво ускладняються. Щоб захистити ресурси в цих умовах, потрібен інший підхід. На практиці зовнішній доступ до будь-якої частини розподіленої системи контролюється спеціальним монітором, відомим як міжмережевий екран / брандмауер (firewall). Міжмережевий екран (МЕ) – це частина комп'ютерної системи або мережі, призначена для блокування несанкціонованого доступу та дозволу зовнішнього зв'язку [22]. Використовуючи МЕ для контролю підключення, організація може запобігти несанкціонованому доступу до своїх систем і ресурсів. МЕ – це міжмережевий шлюз (inter-network gateway), який обмежує трафік передачі даних в одну з підключених мереж та з неї (та, яка, як кажуть, знаходиться «всередині» МЕ) і, таким чином, захищає системні ресурси цієї мережі від загроз з іншої мережі (тієї, яка знаходиться, як кажуть, «за межами» брандмауера) [79, 80]. Брандмауери – це пристрої або програми, які контролюють потік мережевого трафіку між мережами або вузлами, що використовують різні заходи безпеки [81]. Брандмауери можна використовувати для логічного застосування користувацьких наборів правил до мережевого трафіку. МЕ, які зазвичай розміщуються на межах мережі, можуть обмежувати як вхідний, так і вихідний трафік на основі різних характеристик даних [80]. Проста маршрутизована мережа з брандмауером представлена на рис. 14.

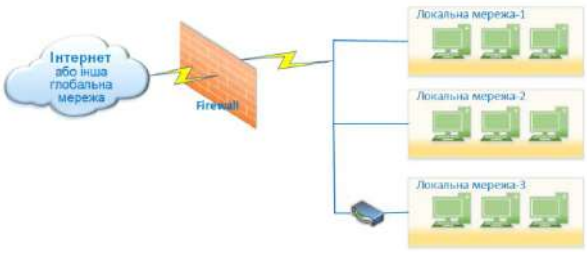


Рис. 14. Проста маршрутизована мережа з брандмауером

Можна виділити такі типи технологій міжмережевих екранів [81 – 84]: *МЕ із фільтрацією пакетів* (packet filtering firewall); *шлюз рівня каналу* (circuit-level gateway); *шлюз рівня програми* (application-level gateway) – також відомий як проксі-брандмауер (proxy firewall); *МЕ з відстеженням / перевіркою стану* (stateful inspection firewall); *МЕ наступного покоління* (next-generation firewall – NGFW).

Міжмережевий екран із фільтрацією пакетів працює як маршрутизатор і приймає рішення щодо того, чи слід передавати мережевий пакет на основі адреси джерела та одержувача, що міститься в заголовку пакета. Він безпосередньо перевіряє поточний мережевий трафік на

рівнях OSI 3 (мережевий рівень) та 4 (транспортний рівень), з метою ухвалення рішення про те, чи слід відкидати або пересилати пакети до місця призначення.

Фільтр має набір налаштованих правил на основі IP-адреси призначення та джерела, номера порту та іншої інформації. Якщо пакет не відповідає жодному з цих правил, він або автоматично відкидається, або генерується повідомлення ICMP (Internet Control Message Protocol), що повідомляє джерело відкинутого пакета. МЕ з фільтрацією пакетів є досить простими і не споживають багато ресурсів. Однак вони не є найефективнішими МЕ, оскільки їх легко оминути. У таких МЕ відсутня можливість аналізу протоколів вищих рівнів мережевої моделі OSI. Крім того, недоліком методу, що використовується в них, є те, що можуть існувати конфліктуючі правила, які необхідно вирішити для деяких пакетів.

Шлюзи рівня каналу працюють лише на рівні TCP. TCP-з'єднання передаються через комп'ютер, що по суті діє як провідник [82]. Для виявлення шкідливого контенту, шлюзи на рівні каналу відстежують TCP-рукостискання та інші повідомлення про ініціювання сеансу мережевого протоколу по всій мережі, коли вони встановлюються між локальним та віддаленим вузлами, щоб визначити, чи є сеанс, що ініціюється, законним (чи вважається віддалена система довіреною). Однак вони не перевіряють самі пакети, тому не є найкращим способом запобігання проникненню шкідливого програмного забезпечення в мережу. Хоча шлюзи на рівні каналів забезпечують більш високий рівень безпеки, ніж МЕ з фільтрацією пакетів, їх слід використовувати спільно з іншими системами. Наприклад, шлюзи рівня каналу зазвичай використовуються разом із шлюзами рівня застосунку.

Проксі-брандмауер (*шлюз рівня застосунку*) є одним із найбезпечніших типів МЕ [84]. Він знаходиться між захищеною мережею та рештою світу, функціонуючи як єдина точка входу в мережу та точка виходу з неї. Проксі-брандмауер блокує запит від системи у внутрішній мережі перед його відправкою за призначенням. Він веде себе як сервер при взаємодії з хостом клієнта і як клієнт – при надсиланні або отриманні даних від хоста сервера [83]. При цьому сервер та клієнт ніколи не мають прямого з'єднання. Шлюзи рівня застосунків мають перевагу, яка в деяких середовищах дуже важлива – весь вхідний та вихідний трафік легко реєструвати та контролювати. Проксі-брандмауер встановлює з'єднання з джерелом, а потім перевіряє вміст пакета (у тому числі наявність шкідливого ПЗ). Пошту можна перевірити на наявність «брудних» слів (dirty words), що вказують на те, що через шлюз проходять конфіденційні або обмежені дані. Веб-запити можна перевірити на відповідність політикам компанії, а небезпечні поштові вкладення можна видалити [82]. Таким чином, тільки якщо дані схвалені, вони надсилаються за призначенням. Таким чином, проксі-сервери додають рівень захисту, забезпечуючи анонімність пристроїв усередині мережі. Однак, хоча шлюзи, що здійснюють фільтрацію на рівні застосунків, забезпечують значну безпеку даних, вони можуть суттєво вплинути на продуктивність мережі (можливе уповільнення швидкості передачі) і ними може бути складно керувати.

Міжмережевий екран з відстеженням стану – це тип МЕ, що поєднує в собі технології, що раніше обговорювалися (фільтрації пакетів і шлюзів рівня каналу), для забезпечення більшої безпеки. Насправді перевірка стану є дуже складною версією пакетного фільтра [84]. Даний тип МЕ може відстежувати стан мережевих підключень, таких як потоки TCP, дейтаграми UDP та повідомлення ICMP, і може зберігати важливі властивості кожного з'єднання в пам'яті. У сукупності ці властивості називаються станами з'єднання і можуть включати такі відомості, як IP-адреси та порти, що беруть участь у з'єднанні, а також порядкові номери пакетів, що проходять через з'єднання. Для відстеження стану з'єднань використовуються спеціальні таблиці сеансів. Точність роботи МЕ цього залежить від обробки відповідних таблиць сеансів, а також від механізму фільтрації пакетів. Брандмауери з відстеженням стану використовують дані як про минулі, так і про поточні мережеві з'єднання при прийнятті рішень щодо фільтрації, тим самим пропонуючи більше можливостей (у тому числі високий рівень контролю над тим, який контент потрапляє до мережі або виходить із неї), але зі збільшенням обчислювальних витрат [81].

Міжмережеві екрани наступного покоління розширюють можливості брандмауерів із перевіркою стану, додаючи такі функції, як фільтрація застосунків, глибока перевірка пакетів (DPI – deep packet inspection), відстеження VPN-трафіку, адаптивні правила та виявлення загроз [80]. Згідно з визначенням аналітиків Gartner [85], NGFW – це міжмережеві екрани з глибокою перевіркою пакетів, які виходять за рамки перевірки та блокування портів / протоколів та додають перевірку на рівні застосунків, запобігання вторгненням та отримання відомостей ззовні брандмауера. NGFW не слід плутати з автономною системою запобігання вторгненням в мережу (IPS – intrusion prevention system), яка включає стандартний або некорпоративний МЕ, або МЕ і IPS в одному пристрої, які не є тісно інтегрованими. Як мінімум, на думку фахівців Gartner, NGFW має забезпечувати [86]: без переривання роботи, вбудовану, bump-in-the-wire (BITW) конфігурацію (BITW – це клас пристроїв зв'язку, які можуть бути вставлені в існуючі (успадковані) системи для підвищення цілісності, конфіденційності або надійності зв'язку існуючим логічним каналом без зміни кінцевих точок зв'язку); стандартні можливості брандмауера першого покоління (наприклад, перетворення мережевих адрес (NAT – network address translation), SPI (stateful packet inspection – перевірка пакетів з відстеженням стану) та віртуальна приватна мережа (VPN) тощо; інтегрований механізм IPS на основі сигнатур; поінформованість про застосунки, повна видимість трафіку і детальний контроль (це означає, що NGFW повинні блокувати або дозволяти пакети в залежності від того, до якого застосунку вони прямують, аналізуючи трафік на рівні 7 еталонної моделі OSI – на рівні застосунків; традиційні МЕ не мають такої можливості, оскільки вони аналізують трафік лише на рівнях 3 та 4 моделі OSI [87]); можливість включати інформацію ззовні брандмауера (наприклад, чорні та білі списки); способи оновлення, щоб мати можливість включати майбутні інформаційні потоки та загрози безпеці; розшифрування SSL для ідентифікації небажаних зашифрованих програм (інспекцію трафіку).

NGFW можуть забезпечувати інтелектуальний аналіз та контроль застосунків, запобігання вторгненням, захист від шкідливих програм та перевірку SSL на мультигігабітних швидкостях, масштабованість для підтримки мереж із найвищою продуктивністю [86]. Порівняно з попередніми поколіннями NGFW мають перевагу в тому, що вони динамічні. Вони можуть використовувати методи машинного навчання для виявлення невідомих раніше загроз шляхом розпізнавання моделей поведінки. Ключовими розробниками цих продуктів експерти називають Fortinet, Palo Alto Networks, Check Point, Cisco та деякі інші [88, 89]. МЕ наступного покоління в даний час відносяться до категорії зрілих рішень. Однак перехід діючих інформаційних систем на хмарні платформи IaaS (Infrastructure-as-a-Service), такі, як Amazon Web Services, Microsoft Azure Google Cloud Platform, змушує задуматися над розширенням можливостей МЕ нового покоління. Таким чином, сьогодні МЕ можуть бути розгорнуті як апаратні пристрої, бути програмними або надаватися як послуга. Апаратний брандмауер – це пристрій, що діє як безпечний шлюз між пристроями всередині периметра мережі та за його межами. Програмний брандмауер або хост-брандмауер працює на сервері або іншому пристрої. Програмне забезпечення хост-брандмауера має бути встановлене на кожному пристрої, що потребує захисту. Хмарний брандмауер – це продукт безпеки, який, як і традиційний брандмауер, фільтрує потенційно шкідливий мережевий трафік. На відміну від традиційних МЕ, міжхмарні хмарні екрани розміщуються в хмарі. Ця хмарна модель брандмауерів також називається брандмауер як послуга (FWaaS – Firewall-as-a-Service) [90]. Хмарні екрани між мережами утворюють віртуальний бар'єр навколо хмарних платформ, інфраструктури та застосунків, так само, як традиційні МЕ утворюють бар'єр навколо внутрішньої мережі організації. Зважаючи на те, що схильність до загроз тієї чи іншої організації різна, для кожного конкретного випадку необхідно шукати відповідне рішення щодо використання МЕ.

Виходячи з сказаного вище, можна зробити висновок, що брандмауери утворюють один із найбільш часто використовуваних механізмів захисту в мережевих системах. При цьому слід пам'ятати, що важливим аспектом також є те, що сам брандмауер має бути надійно захищений від будь-яких загроз безпеці, зокрема він ніколи не повинен виходити з ладу.

Не менш важливо, щоб правила, що наказують, що може проходити, були несуперечливі та встановлювали наміри. Як відомо [91], правильне налаштування МЕ є серйозною проблемою.

Висновки

1. Забезпечення безпеки розподілених інформаційних систем, в яких безліч компонентів може знаходитися в різних місцях і взаємодіяти один з одним за допомогою мережі, що створює вразливості та ризики для безпеки, які не існують у традиційних централізованих системах, є однією з ключових проблем сучасності, що охоплює безліч технологій, методів та процедур, спрямованих на захист систем від різноманітних загроз. Важливість та необхідність її вирішення зростає у зв'язку зі збільшенням обсягу інформації, що зберігається та обробляється в таких системах та передається по мережах зв'язку.

2. Внаслідок шкідливих дій з боку зловмисника, що асоціюються з перехопленням, перериванням, модифікацією та фабрикацією, мають місце такі основні загрози для розподілених систем: несанкціонований доступ до даних, ресурсів і мережі (це може статися, якщо зловмисники отримають доступ до облікових записів або мережевих з'єднань); недостатній захист даних (якщо дані не захищені належним чином, це може призвести до несанкціонованого доступу до них); вразливості у програмному забезпеченні (розподілені системи можуть використовувати велику кількість програмного забезпечення, яке може містити вразливості, які можуть бути використані зловмисниками для атак на систему); неправильна конфігурація системи (може створювати вразливість атак на систему); відмова компонентів системи. Регулярні оцінки безпеки, сканування вразливостей та тестування на проникнення можуть допомогти виявити та усунути слабкі місця у розподілених системах. Особи, які відповідають за безпеку в організаціях, компаніях, повинні завжди бути в курсі актуальних загроз та передових методів забезпечення безпеки, щоб відповідним чином адаптувати існуючі заходи безпеки.

3. Для забезпечення безпеки у розподілених системах доцільно використовувати комплексні заходи, такі як: механізми автентифікації та авторизації (це дозволяє засвідчити легітимність користувачів, процесів та компонентів системи, а також керувати доступом до ресурсів та даних у системі; дані механізми є основою для створення безпечних каналів, що забезпечують безпечну взаємодію користувачів та процесів у системі); механізми контролю доступу та політики безпеки (кожен із ресурсів може підтримувати власний список доступу, в якому перераховуються права доступу всіх користувачів або процесів; крім того, процес може мати сертифікат, який точно встановлює його права на певний набір ресурсів); шифрування даних (як тих, що зберігаються у відповідних сховищах, базах даних системи, так і тих, що передаються через мережу); моніторинг та протоколювання дій / ведення журналу (це дозволяє відстежувати дії користувачів та компонентів системи для виявлення незвичайних або підозрілих активностей); резервне копіювання (регулярне створення резервних копій даних з метою швидкого їх відновлення у разі втрати або ушкодження); регулярне оновлення програмного забезпечення (це допомагає виявляти та виправляти вразливості в системі, які можуть бути використані зловмисниками для атак на систему) та деякі інші. Усі ці заходи повинні бути застосовані відповідно до конкретних вимог та особливостей розподіленої системи, щоб забезпечити надійний захист від різноманітних загроз безпеці, так як навіть єдине слабке місце в системі може призвести до порушення безпеки всієї системи, і зробити заходи захисту її активів, що використовуються, марними. Тому розробка та правильне комплексне застосування цих механізмів для забезпечення ефективного захисту елементів РІС є непростим, нетривіальним завданням, що потребує знання як теоретичних положень, так і кращих практик у галузі інформаційної безпеки та кібербезпеки.

Список літератури:

1. Dhanarani A., Evans R., Loumi H., Lowenthal R., Lopes P., Mesaros M., Schaeumer B., Wahl P., Williams A., Zaidi N. Oracle Database Security a technical primer. Fifth edition. 2023. 160 p.
2. Global Data Protection Index 2022 Key Findings. October 2022. URL: https://www.delltechnologies.com/asset/en-nz/products/data-protection/industry-market/global-data-protection-index-key-findings.pdf.
3. General Data Protection Regulation GDPR. URL: https://gdpr-info.eu/.
4. Заплатинський В. М. Логіко-детермінантні підходи до розуміння поняття «Безпека» // Вісник Кам'янець-Подільського нац. ун-ту ім. Івана Огієнка. Фізичне виховання, спорт і здоров'я людини. Кам'янець-Подільський : Кам'янець-Подільський нац. ун-т ім. Івана Огієнка, 2012. Вип. 5. С. 90–98.
5. Dictionary. URL: https://www.merriam-webster.com/dictionary/security.
6. Whitman M. E., Mattord H. J. Principles of Information Security. 6th ed. Cengage Learning, 2017. 656 p.
7. Stoneburner G. NIST Special Publication 800-33. Underlying Technical Models for Information Technology Security. URL: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-33.pdf.
8. NIST Special Publication 800-66 Revision 1. An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. October 2008. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-66r1.pdf.
9. NISTIR 8074 Volume 2. Supplemental Information for the Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity. December 2015. URL: http://dx.doi.org/10.6028/NIST.IR.8074v2.
10. ISO/IEC 27000:2018 Information technology. Security techniques. Information security management systems. Overview and vocabulary. URL: https://www.iso.org/standard/73906.html.
11. NIST Special Publication NIST SP 800-66r2 ipd. Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide. July 2022. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-66r2.ipd.pdf.
12. ISO/IEC 15408-1:2022 Information security, cybersecurity and privacy protection – Evaluation criteria for IT security. Part 1: Introduction and general model. URL: https://www.iso.org/obp/ui/ru/#iso:std:iso-iec:15408:1:ed-4:v1:en
13. Tanenbaum A. S., Van Steen M. Distributed systems principles and paradigms. Prentice Hall, 2002. 803 p.
14. Van Steen M., Tanenbaum A. S. Distributed systems. Third edition. Pearson Education, Inc. 2017. 596 p.
15. Avizienis A., Laprie J. C., Randell B. Fundamental concepts of dependability. Department of Computing Science Technical Report Series. University of Newcastle upon Tyne. 2001. 21 p.
16. Laprie J. C. Dependability – Its Attributes, Impairments and Means // Randell B., Laprie J.C., Kopetz H., Littlewood B. (eds) Predictably Dependable Computing Systems. ESPRIT Basic Research Series. Springer, Berlin, Heidelberg. 1995. P. 3-24. https://doi.org/10.1007/978-3-642-79789-7_1
17. Chapple M., Stewart J. M., Gibson D. CISSP Certified Information Systems Security Professional Official Study Guide, 8th ed. Sybex, John Wiley & Sons, Inc.: Indianapolis, Indiana, 2018. 1050 p.
18. Chapple M., Stewart J. M., Gibson D. CISSP: certified information systems security professional official study guide. 9th Edition. Sybex, John Wiley & Sons, Inc.: Indianapolis, Indiana, 2021. 1248 p.
19. Pfleeger C. P., Pfleeger S. L. Security in Computing. 3rd edition. Upper Saddle River, NJ, USA: Prentice Hall, 2002. 746 p.
20. Pfleeger C. P., Pfleeger S. L. Security in Computing. Fifth Edition. Margulies. Prentice Hall. 2015. 944 p.
21. Swanson M., Guttman B. NIST 800-14. Generally Accepted Principles and Practices for Securing Information Technology Systems. URL: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=890092.
22. Committee on National Security Systems (CNSS) Glossary. CNSSI No. 4009. 2022. URL: https://www.niap-ccevs.org/Ref/CNSSI_4009.pdf
23. Priscilla O. Top-Down Network Design. Cisco Press: Indianapolis, IN, USA. 2010. 447 p.
24. NIST Special publication 1800-10. Protecting Information and System Integrity in Industrial Control System Environments: Cybersecurity for the Manufacturing Sector. 2022. https://doi.org/10.6028/NIST.SP.1800-10.
25. FIPS PUB 200. Federal information processing standards publication. Minimum Security Requirements for Federal. Information and Information Systems. 2006. URL: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf.
26. Harini N., Padmanabhan T. R. 2CAuth: A new two factor authentication scheme using QR-code. International Journal of Engineering and Technology. 2013. 5(2). P. 1087–1094.
27. Velásquez I., Caro A., Rodríguez A. Authentication schemes and methods: A systematic literature review // Information and Software Technology. 2018. Vol. 94. P. 30–37. https://doi.org/10.1016/j.infsof.2017.09.012
28. O'Gorman L. Comparing passwords, tokens, and biometrics for user authentication. In Proceedings of the IEEE. 2003. 91(12). P. 2021–2040. https://doi.org/10.1109/JPROC.2003.819611
29. Ometov A., Bezzateev S., Mäkitalo N., Andreev S., Mikkonen T., Koucheryavy Y. Multi-Factor Authentication: A Survey. Cryptography 2018. 2(1). 1. https://doi.org/10.3390/cryptography2010001
30. Auditing Database Activity. URL: https://docs.oracle.com/en/database/oracle/oracle-database/12.2/tdpsg/auditing-database-activity.html#GUID-BF747771-01D1-4BFB-8489-08988E1181F6
31. Gollmann D. Computer Security. 3rd ed. Hoboken, NJ, USA: Wiley, 2011. 436 p.

32. Methods and systems for transparent data encryption and decryption. Richard James McCarty, Austin, TX (US); International Business Machines Corporation, Armonk, NY (US) – N 10/422,667. US Patent 7426,745 B2, 16 September 2008.
33. Stallings W., Brown L. Computer security principles and practice. Fourth Edition. 2018. 778 p.
34. Security management definition. URL: https://www.lawinsider.com/dictionary/security-management.
35. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture. Special Publication NIST SP 800-207. 2020. https://doi.org/10.6028/NIST.SP.800-207.
36. Gartner. URL: https://www.gartner.com/en/about.
37. Gartner. Gartner Predicts 10% of Large Enterprises Will Have a Mature and Measurable Zero-Trust Program in Place by 2026. URL: https://www.gartner.com/en/newsroom/press-releases/2023-01-23-gartner-predicts-10-percent-of-large-enterprises-will-have-a-mature-and-measurable-zero-trust-program-in-place-by-2026.
38. Gartner Research. Market Share Analysis: Enterprise Network Equipment, Worldwide, 2022. URL: https://www.gartner.com/en/documents/4412099.
39. Bishop M. Computer Security: Art and Science. Second ed. Addison-Wesley, Reading, MA., 2019. 1383 p.
40. Bouch A. 3-D Secure: A critical review of 3-D Secure and its effectiveness in preventing card not present fraud. University of London. 2011. URL: https://www.58bits.com/thesis/3-D_Secure.pdf.
41. NIST Special Publication 1800-21. Mobile Device Security: Corporate-Owned Personally-Enabled (COPE). URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-21.pdf.
42. Google Cloud documentation. Encryption in transit. URL:https://cloud.google.com/docs/security/encryption-in-transit.
43. Sommerhalder M. Hardware Security Module. In: Mulder V., Mermoud A., Lenders V., Tellenbach B. (eds) Trends in Data Protection and Encryption Technologies. Springer, Cham. 2023. P. 83–87.
44. Google Cloud. Default encryption at rest. URL: https://cloud.google.com/docs/security/encryption/default-encryption
45. Єсін В. І., Вілігура В. В. Основні категорії NewSQL баз даних та їх особливості // Радіотехніка. 2022. № 211. С. 37–66. https://doi.org/10.30837/rt.2022.4.211.03.
46. Sarbanes-Oxley Act of 2002. Public Law 107–204, Approved July 30, 2002, 116 Stat. 745. URL: https://www.govinfo.gov/content/pkg/COMPS-1883/pdf/COMPS-1883.pdf
47. Scholl M., Stine K., Hash J., Bowen P., Johnson A., et al. NIST Special Publication 800-66 Revision 1. An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. 2008. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-66r1.pdf
48. Payment Card Industry (PCI) Data Security Standard. Requirements and Testing Procedures Version 4.0. 2022. URL: https://www.pcisecuritystandards.org/documents/PCI-DSS-v4_0.pdf
49. Nanda A., Feuerstein S. Oracle PL/SQL for DBAs: Security, Scheduling, Performance & More. O'Reilly Media, Inc., 2005. 454 p.
50. Advanced Security Guide. Introduction to Transparent Data Encryption. URL: https://docs.oracle.com/en/database/oracle/oracle-database/23/asoag/introduction-to-transparent-data-encryption.html#GUID-62AA9447-FDCD-4A4C-B563-32DE04D55952
51. Barker E., Kelsey J. NIST Special Publication 800-90A Revision 1. Recommendation for Random Number Generation Using Deterministic Random Bit Generators. 2015. http://dx.doi.org/10.6028/NIST.SP.800-90Ar1.
52. Needham R. M., Schroeder M. D. Using encryption for authentication in large networks of computers. Communications of the ACM. 1978. 21(12). P. 993–999. https://doi.org/10.1145/359657.359659
53. FIPS 186-5. Federal information processing standards publication (Supersedes FIPS 186-4). Digital Signature Standard (DSS). Category: computer security. Subcategory: cryptography. 2023. https://doi.org/10.6028/NIST.FIPS.186-5
54. Barker E., Chen L., Roginsky A., Vassilev A., Davis R., Simon S. NIST Special Publication 800-56B Revision 2. Recommendation for Pair-Wise Key Establishment Using Integer Factorization Cryptography. 2019. https://doi.org/10.6028/NIST.SP.800-56Br2
55. Cruz-Cunha M. M., Oliveira E. F., Tavares A. J., Ferreira, L. G. Handbook of research on social dimensions of semantic technologies and web services. Hershey, PA: IGI Global, 2009. 1180 p.
56. Lampson B. W. Protection. ACM SIGOPS Operating Systems Review. 1974. 8(1). P. 18–24.
57. Lampson B. W. Dynamic protection structures. Proceedings of the November 18-20, 1969, fall joint computer conference. 1969. P. 27–38.
58. Graham G. S., Denning P. J. Protection: principles and practice. Proceedings of the May 16-18, 1972, spring joint computer conference. 1971. P. 417–429.
59. Harrison M. A., Ruzzo W. L., Ullman J. D. Protection in Operating Systems // Communications of the ACM, 1976. 19(8). P. 461–471.
60. Weissman C. Security controls in the ADEPT-50 time-sharing system // Proceedings of the November 18-20, 1969, fall joint computer conference. 1969. P. 119–133.
61. Hartson H. R., Hsiao D. K. A Semantic Model for Database Protection Languages // Proceedings of the second international conference on Systems for Large Data Bases. 1976. P. 27–42.
62. Lipton R. J., Snyder L. A linear time algorithm for deciding subject security // Journal of the ACM (JACM). 1977. 24(3). P. 455–464.

63. Hoffman L.J. Modern Methods for Computer Security and Privacy. Englewood Cliffs, NJ, USA: Prentice-Hall. Inc., 1977. 268 p.
64. Білігура В. В. Аналіз формальних моделей управління доступом і особливості їх застосовності для баз даних // Радіотехніка. 2021. Вип. 205. С. 53–70. https://doi.org/10.30837/rt.2021.2.205.05.
65. Білігура В. В., Горбенко Ю. І., Єсін В. І., Рассомахін С. Г. Використання формальних моделей безпеки в захищених базах даних // Фізико-математичне моделювання та інформаційні технології. 2021. № 32. С. 70–74. https://doi.org/10.15407/fmmit2021.32.070
66. Bell D. E., LaPadula L. J. Secure Computer Systems: Unified Exposition and Multics Interpretation (MTR-2997 Rev. 1). Bedford, Mass.: MITRE Corp., 1976. 129 p.
67. Sandhu R.S., Coyne E. J., Feinstein H. L., Youman C. E. Role-based access control models // IEEE Computer. 1996. № 2. P. 38–47.
68. NIST. Attribute Based Access Control. URL: https://csrc.nist.gov/Projects/Attribute-Based-Access-Control.
69. Hu V. C., Ferraiolo D., Kuhn R. Guide to Attribute Based Access Control (ABAC) Definition and Considerations. NIST Special Publication 800-162. 2014. URL: https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.sp.800-162.pdf.
70. Hu V. C., Kuhn D. R., Ferraiolo D. F., Voas J. Attribute-Based Access Control // Computer. 2015. Vol. 48. No. 2. P. 85–88. https://doi.org/10.1109/MC.2015.33.
71. Servos D., Osborn S.L. HGABAC: Towards a Formal Model of Hierarchical Attribute-Based Access Control // Cuppens, F., Garcia-Alfaro, J., Zincir Heywood, N., Fong, P. (eds) Foundations and Practice of Security. FPS 2014. Lecture Notes in Computer Science. Springer, Cham. 2015. Vol. 8930. P. 187–204.
72. Biswas P., Sandhu R., Krishnan R. Label-based access control: An ABAC model with enumerated authorization policy // Proceedings of the 2016 ACM International Workshop on Attribute Based Access Control (ABAC '16). Association for Computing Machinery, New York, NY, USA. 2016. P. 1–12. https://doi.org/10.1145/2875491.2875498.
73. Servos D., Osborn S. L. Current research and open problems in attribute-based access control // ACM Computing Surveys (CSUR). 2017. 49(4). P. 1–45. https://doi.org/10.1145/3007204.
74. OASIS eXtensible Access Control Markup Language (XACML) TC. URL: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml
75. International Committee for Information Technology Standards, Information technology – Next Generation Access Control – Functional Architecture (NGAC–FA), ANSI/INCITS 499-2018, American National Standards Institute, New York, January 30, 2018. 57 p.
76. INCITS 565-2020. Information technology – Next Generation Access Control (NGAC). American National Standard for Information Technology. April, 2020.
77. Ferraiolo D., Chandramouli R., Hu V., Kuhn R. A Comparison of Attribute Based Access Control (ABAC) Standards for Data Service Applications. NIST Special Publication 800-178. 2016. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-178.pdf. http://dx.doi.org/10.6028/NIST.SP.800-178.
78. Hu V. C., Ferraiolo D. F, Chandramouli R., D. Kuhn D. R. Attribute-Based Access Control. Artech House. 2017. 280 p.
79. Shirey R. Internet Security Glossary. Version 2. 2007. №. rfc4949. URL: https://datatracker.ietf.org/doc/html/rfc4949.
80. Stouffer K., Pease M., Tang C.Y., Zimmerman T., Pillitteri V., Lightman S., Hahn A., Saravia S., Sherule A., Thompson M. NIST Special Publication NIST SP 800-82r3. Guide to Operational Technology (OT) Security. 2023. https://doi.org/10.6028/NIST.SP.800-82r3.
81. Scarfone K., Hoffman P. Special Publication 800-41 Revision 1. Guidelines on Firewalls and Firewall Policy. 2009. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf.
82. Cheswick W. R. Bellovin S. M., Rubin A. D. Firewalls And Internet Security: Repelling The Wily Hacker. 2nd ed. Addison-Wesley Professional. 2003. 464 p.
83. Mukkamala P. P., Rajendran S. A survey on the different firewall technologies // International Journal of Engineering Applied Sciences and Technology. 2020. 5(1). P. 363–365.
84. Goralski W. The illustrated network: how TCP/IP works in a modern network. Morgan Kaufmann. 2017. 899 p.
85. Next-generation Firewalls (NGFWs). URL: https://www.gartner.com/en/information-technology/glossary/next-generation-firewalls-ngfws.
86. Malecki F. Next-generation firewalls: Security with performance // Network Security. 2012. Vol. 2012. Issue 12. P. 19–20.
87. What is a next-generation firewall (NGFW)? URL: https://www.cloudflare.com/learning/security/what-is-next-generation-firewall-ngfw/.
88. What are Network Firewalls? URL: https://www.gartner.com/reviews/market/network-firewalls.
89. A Leader Positioned Highest in Ability to Execute. URL: https://www.fortinet.com/solutions/gartner-network-firewalls.
90. What is a cloud firewall? URL: https://www.cloudflare.com/learning/cloud/what-is-a-cloud-firewall/.
91. Wool A. Trends in firewall configuration errors: Measuring the holes in Swiss cheese // IEEE Internet Computing. 2010. 14(4). P. 58–65. https://doi.org/10.1109/MIC.2010.2910.1109/MIC.2010.29.

Надійшла до редколегії 05.09.2023

Відомості про авторів:

Есін Віталій Іванович – д-р техн. наук, Харківський національний університет імені В.Н. Каразіна, професор кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук; Україна; e-mail: v.i.yesin@karazin.ua; ORCID: https://orcid.org/0000-0003-1977-7269

Вілігура Владислав Вікторович – Харківський національний університет імені В.Н. Каразіна, аспірант кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук; Україна; e-mail: viligura93@gmail.com; ORCID: https://orcid.org/0000-0002-1137-2382

Сватовський Ігор Іванович – канд. техн. наук, Харківський національний університет імені В. Н. Каразіна, старший науковий співробітник, доцент кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук; Україна; e-mail: i.svatowsky@karazin.ua; ORCID: https://orcid.org/0000-0002-1836-5599

УДК 621.391:519.2 **DOI:10.30837/rt.2023.3.214.05**

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

МЕТОД НАПРАВЛЕНОГО ШИФРУВАННЯ В КРИПТОСИСТЕМІ MST3 НА ОСНОВІ ГРУПИ АВТОМОРФІЗМІВ ФУНКЦІОНАЛЬНОГО ПОЛЯ СУЗУКІ

Вступ

Розвиток комерційних квантових комп'ютерів вносить значні виклики у сферу безпеки багатьох криптосистем з відкритим ключем. Квантовий алгоритм, розроблений Шором, призначений для розв'язання задач цілочисельної факторизації та обчислення дискретних логарифмів, ставить під загрозу безпеку криптосистем, таких як RSA та ECC. Один з перспективних напрямків створення криптосистем, стійких до квантових атак, полягає у використанні задач, що мають високу складність вирішення в певних групах [1 – 11]. Побудова криптосистем на основі нерозв’язних задач була сформульована Шпільрайном та Ушаковим на початку 2000-х років у [3]. З початку 2000-х років запропоновано декілька десятків криптосистем у групових структурах [5 – 11].

Використовуючи групи перестановок, Вагнер і Магьярик [5] запропонували нерозв'язну схему, засновану на проблемі слова, для створення квантово-стійких криптосистем. Квантова безпека таких систем залежить від їх конкретної реалізації, і, на попередньому етапі, можливе використання квантового алгоритму Гровера для криптоаналізу. Ідея нерозв'язної проблеми слова вперше була реалізована в криптосистемі з логарифмічними підписами [6]. Логарифмічний підпис є особливим типом факторизації і застосовується до кінцевих груп. Покращення оригінальної версії були внесені в [7, 8].

Побудова криптосистем на основі неабелевих груп з використанням нерозв’язаних задач залишається перспективним напрямом досліджень [12 – 17]. Сімейство криптосистем MST реалізує практичні результати даних досліджень. Остання версія реалізації відома як MST3 [8] і базується на групі Сузукі. Було розглянуто різні стратегії для покращення MST3 [9 – 19], зокрема, за допомогою багатопараметричних груп великого порядку та оптимізації обчислювальних процесів на малому кінцевому полі.

Одним з ключових нововведень було використання автоморфізмів груп над функціональними полями Сузукі, Ерміта, Рі великого порядку. Автори [18 – 28] першими запропонували напрями посилення секретності та покращення параметрів реалізації даної криптосистеми для створення кандидата квантово-стійкої криптосистеми на основі неабелевих груп Сузукі, Ерміта, Рі. Однак первинні реалізації криптосистем на основі групи автоморфізмів над функціональним полем Ерміта мали недоліки, такі як слабке зв'язування ключів логарифмічних підписів, що підвищувало ризик послідовних атак на відновлення ключа.

У статті представлена новітня безпечна схема шифрування, заснована на групі автоморфізму функціонального поля Сузукі.

Група автоморфізмів функціонального поля Сузукі

Визначення та властивості криптосистеми MST3, визначення групи, її розмір, порядок, детально описано в роботі [13 – 18]. Тому, розглянемо та визначимо властивості автоморфізмів функціонального поля Сузукі.

Нехай F_q – скінченне поле, а F/F_q – поле алгебраїчної функції над повним сталим полем F_q роду g. Функціональне поле Сузукі – це оптимальне функціональне поле, визначене над кінцевим полем з парною характеристикою p. Нехай $p=2$, $q=2^n$ з $n=2s+1$, де $s\in N\setminus\{0\}$, і $q_0=2^s$. Нехай K – кінцеве поле F_q. Функціональне поле Сузукі над K визначається як $S=K(x,y)$ де $y^q+y=x^{2q_0}(x^q+x)$.

$S/K(x)$ є розширенням Галуа ступеня q, а полюс x повністю розгалужений у розширенні $S/K(x)$. Позначимо P_∞ єдине раціональне місце, що S лежить над полюсом x. Рід дорівнює S, $g(S)=q_0(q-1)$, а кількість раціональних розрядів S дорівнює q^2+1.

Група автоморфізмів S позначається $A=Aut(S/K)$ ізоморфною групі Сузукі, $Sz(q)$, яка має порядок $ordA=\left(q^2+1\right)q^2\left(q-1\right)$.

Група розкладання P_∞, яку позначають як $A\left(P_\infty\right)$, складається з автоморфізмів $S\left|F_q\right.$, що діють на ній як

$$\begin{cases}\sigma(x)=ax+b\\ \sigma(y)=a^{2q_0+1}y+ab^{2q_0}x+c,\end{cases}$$

де $a\in F_q^*:=F_q\setminus\{0\}$, $b,c\in F_q$[10]. Інволюцію $\psi\in A$ задають

$$\begin{cases}\psi(x)=y/h\\ \psi(y)=y/h\end{cases},$$

де $h=xy+x^{2q_0+2}+y^{2q_0}$.

Група автоморфізмів S породжується $A\left(P_\infty\right)$ і ψ, тобто $Sz(q)\cong\left\langle A\left(P_\infty\right),\psi\right\rangle$.

Знову ж, автоморфізм у групі розкладання $A\left(P_\infty\right)$ можна ототожнити з трійкою [a, b, c]. Точніше, $A\left(P_\infty\right)=\left[a,b,c\right]$, $a,b,c\in K$, і $a=0$.

Структура групи має вигляд $\left[a_1,b_1,c_1\right]\cdot\left[a_2,b_2,c_2\right]=\left[a_1a_2,a_2b_1+b_2,a_2^{2q_0+1}c_1+a_2b_2^{2q_0}b_1+c_2\right]$.

Тотожність є трійкою $\left[1,0,0\right]$ та оберненою $\left[a,b,c\right]$,

$$\left[a,b,c\right]^{-1}=\left[a^{-1},-a^{-1}b,\left(a^{-1}b\right)^{2q_0+1}-a^{-(2q_0+1)}c\right].$$

Порядок групи дорівнює $ordA\left(P_\infty\right)=q^2\left(q-1\right)$.

З а у в а ж е н н я . Порядкова група $A\left(P_\infty\right)$ більша за групу Сузукі. Групи Сузукі ізоморфні проєктивній лінійній групі $PGL\left(3,F_q\right)$, де $q=2q_0^2$, $q_0=2^n$ і мають порядок q^2 і включені в криптосистеми MST3. Більший груповий порядок дає перевагу секретності криптосистеми.

Запропонований метод на основі групи автоморфізмів функціонального поля Сузукі

Наша пропозиція полягає в тому, щоб використовувати логарифмічний підпис для шифрування не тільки в центрі групи $A\left(P_\infty\right)$, як у відомій реалізації MST3 для груп Сузукі, але також для інших координат поза центром групи. Раніше такий підхід ми розглядали для групи Ерміта [23].

Із з а у в а ж е н н я випливає, що для побудови криптосистеми MST3 перевага надається групі $A\left(P_\infty\right)$ на основі автоморфізму $\sigma(x),\sigma(y)$. Кожен елемент $A\left(P_\infty\right)$ може бути виражений унікально: $A\left(P_\infty\right)=\left\{S(a,b,c)\left|a\in F_q\setminus\{0\},b,c\in F_q\right.\right\}$ де $S(a,b,c)=\left[a,b,c\right]$, і групова операція визначається як $\left[a_1,b_1,c_1\right]\cdot\left[a_2,b_2,c_2\right]=\left[a_1a_2,a_2b_1+b_2,a_2^{2q_0+1}c_1+a_2b_2^{2q_0}b_1+c_2\right]$. Обернення до $S\left(a,b,c\right)$ дорівнює $S\left(a,b,c\right)^{-1}=S\left(a^{-1},-a^{-1}b,\left(a^{-1}b\right)^{2q_0+1}-a^{-(2q_0+1)}c\right)$.

Це легко показати прямими розрахунками. Тотожність – це трійка $S\left(1,0,0\right)$.

З цього випливає, що $\left|A\left(P_\infty\right)\right| = q^2\left(q-1\right)$. Центр $Z\left(A\left(P_\infty\right)\right) = \left\{S(1,0,c)\middle| c \in F_q\right\}$ і $\left|Z\left(A\left(P_\infty\right)\right)\right| = q$.

Основні етапи нашої схеми шифрування наступні. Згенеруємо ключі.

Згенеруємо перший простий логарифмічний підпис
$\beta_{(1)} = \left[B_{1(1)},...,B_{s(1)}\right] = \left(b_{ij}\right)_{(1)} = S\left(1, b_{ij(1)}, 0\right)$ типу $\left(r_{1(1)},...,r_{s(1)}\right)$, $i = \overline{1,s(1)}$, $j = \overline{1,r_{i(1)}}$, $b_{ij(1)} \in F_q$.

Згенеруємо другий простий логарифмічний підпис
$\beta_{(2)} = \left[B_{1(2)},...,B_{s(2)}\right] = \left(b_{ij}\right)_{(2)} = S\left(1,0,b_{ij(2)}\right)$ типу $\left(r_{1(2)},...,r_{s(2)}\right)$, $i = \overline{1,s(2)}$, $j = \overline{1,r_{i(2)}}$, $b_{ij(2)} \in F_q$.

Згенеруємо перше випадкове накриття $\alpha_{(1)} = \left[A_{1(1)},...,A_{s(1)}\right] = \left(a_{ij}\right)_{(1)} = S\left(a_{ij(1)_1}, a_{ij(1)_2}, a_{ij(1)_3}\right)$ того самого типу, що й $\beta_{(1)}$, де $a_{ij} \in A\left(P_\infty\right)$, $a_{ij(1)_1}, a_{ij(1)_2}, a_{ij(1)_3} \in F_q \setminus \{0\}$.

Згенеруємо друге випадкове накриття $\alpha_{(2)} = \left[A_{1(2)},...,A_{s(2)}\right] = \left(a_{ij}\right)_{(2)} = S\left(a_{ij(2)_1}, a_{ij(2)_2}, a_{ij(2)_3}\right)$ того самого типу, що й $\beta_{(2)}$, де $a_{ij(2)_1}, a_{ij(2)_2}, a_{ij(2)_3} \in F_q \setminus \{0\}$.

Згенеруємо $t_{0(k)}, t_{1(k)},..., t_{s(k)} \in A(P_\infty) \setminus Z$, де $t_{i(k)} = S\left(t_{i(k)_1}, t_{i(k)_2}, t_{i(k)_3}\right)$, $t_{i(\mathrm{k})_j} \in F^\times$, $i = \overline{0,s(\mathrm{k})}$, $j = \overline{1,2}$, $k = \overline{1,2}$. Домовимося, що $t_{s(1)} = t_{0(2)}$.

Побудуємо гомоморфізм f_1, визначений за $f_1\left(S\left(a_1,a_2,a_3\right)\right) = S\left(1,a_1,a_2\right)$.

Проведемо обчислення: $\gamma_{(1)} = \left[h_{1(1)},...,h_{s(1)}\right] = \left(h_{ij}\right)_{(1)} = t_{(i-1)(1)}^{-1} f_1\left(\left(a_{ij}\right)_{(1)}\right)\left(b_{ij}\right)_{(1)} t_{i(1)}$,

де $i = \overline{1,s(1)}$, $j = \overline{1,r_{i(1)}}$, $f_1\left(\left(a_{ij}\right)_{(1)}\right)\left(b_{ij}\right)_{(1)} = S\left(1, a_{ij(1)_1} + b_{ij(1)}, a_{ij(1)_2} + a_{ij(1)_1} b_{ij(1)}^{q_0}\right)$ та визначимо гомоморфізм $f_2\left(S\left(1,a_2,a_3\right)\right) = S\left(1,0,a_2\right)$.

Обчислимо $\gamma_{(2)} = \left[h_{1(2)},...,h_{s(2)}\right] = \left(h_{ij}\right)_{(2)} = t_{(i-1)(2)}^{-1} f_2\left(\left(a_{ij}\right)_{(2)}\right)\left(b_{ij}\right)_{(2)} t_{i(2)}$,

де $i = \overline{1,s(2)}$, $j = \overline{1,r_{i(2)}}$ та $f_2\left(\left(a_{ij}\right)_{(2)}\right)\left(b_{ij}\right)_{(2)} = S\left(1,0,a_{ij(2)_2} + b_{ij(2)}\right)$.

Отримали відкритий $\left[f_1, f_2, (\alpha_k, \gamma_k)\right]$ та закритий $\left[\beta_{(k)}, \left(t_{0(k)},...,t_{s(k)}\right)\right]$, $k = \overline{1,2}$ ключі.

Для шифрування використаємо повідомлення $m \in A\left(P_\infty\right)$, $m = S\left(m_1,m_2,m_3\right)$, $m_1 \in F_q \setminus \{0\}$, $m_2, m_3 \in F_q$ та відкритий ключ $\left[f_1, f_2, (\alpha_k, \gamma_k)\right]$, $k = \overline{1,2}$, в результаті отримаємо зашифрований текст $\left(y_1, y_2, y_3, y_4\right)$ повідомлення m.

Згенеруємо випадковий $R = (R_1, R_2)$, $R_1, R_2 \in Z_{|F_q|}$. Обчислимо:

$$y_1 = \alpha'(R) \cdot m = \alpha_1'(R_1) \cdot \alpha_2'(R_2) \cdot m = S\left(a_{(1)_1}(R_1) a_{(2)_1}(R_2), a_{(2)_1}(R_2) a_{(1)_2}(R_1) + a_{(2)_2}(R_2),\right.$$
$$a_{(2)_1}(R_2)^{2q_0+1} a_{(1)_3}(R_1) + a_{(2)_1}(R_2) a_{(2)_2}(R_2)^{2q_0} a_{(1)_2}(R_1) + a_{(2)_3}(R_2)\ \left.\right) \cdot m =$$
$$S\left(\ a_{(1)_1}(R_1) a_{(2)_1}(R_2) m_1, a_{(2)_1}(R_2) a_{(1)_2}(R_1) m_1 + a_{(2)_2}(R_2) m_1 + m_2, m_3 + *\ \right).$$

Тут $(*)$ компоненти визначаються перехресними обчисленнями в груповій операції добутку $a_{(i)_j}(R_i)$. Обчислимо:

$$y_2 = \gamma'(R) = \gamma_1'(R_1) \cdot \gamma_2'(R_2) = S\left(*, a_{(1)_1}(R_1) + \beta_{(1)}(R_1) + *, a_{(2)_2}(R_2) + \beta_{(2)}(R_2) + *\right).$$

Тут $(*)$ компоненти визначаються перехресними обчисленнями в груповій операції добутку $t_{0(k)},...,t_{s(k)}$, а для третьої координати додається добуток $a_{(1)_1}(R_1) + \beta_{(1)}(R_1)$.

Обчислимо

$y_3 = f_1\left(\alpha_1'(R_1)\right) = S\left(1, a_{(1)_1}(R_1), a_{(1)_1}(R_1) + a_{(1)_2}(R_1) + *\right)$; $y_4 = f_2\left(\alpha_2'(R_2)\right) = S\left(1, 0, a_{(2)_2}(R_2)\right)$.

Тут $(*)$ компоненти визначаються перехресними обчисленнями в груповій операції добутку $a_{(1)_1}(R_1)$. Маємо зашифроване повідомлення (y_1, y_2, y_3, y_4).

Для дешифрування беремо зашифрований текст (y_1, y_2, y_3, y_4) та закритий ключ $\left[\beta_{(k)}, \left(t_{0(k)}, ..., t_{s(k)}\right)\right]$, $k = \overline{1,2}$. В результаті маємо отримати повідомлення $m \in A(P_\infty)$, що відповідає зашифрованому тексту (y_1, y_2, y_3, y_4).

Щоб розшифрувати повідомлення m, нам потрібно відновити випадкові числа $R = (R_1, R_2)$. Параметр $a_{(1)_1}(R_1)$ відомий з y_3 і він включений у другий компонент y_2.

Обчислимо $D^{(1)}(R_1, R_2) = t_{0(1)} \cdot y_2 t_{s(2)}^{-1} = S\left(1, a_{(1)_1}(R_1) + \beta_{(1)}(R_1), a_{(2)_2}(R_2) + \beta_{(2)}(R_2) + *\right)$

та $D^*(R) = y_3^{-1} D^{(1)}(R_1, R_2) = S\left(1, \beta_{(1)}(R_1), a_{(2)_2}(R_2) + \beta_{(2)}(R_2) + *\right)$.

Відновимо R_1 з $\beta_{(1)}(R_1)$ за допомогою $\beta_{(1)}(R_1)^{-1}$, оскільки β – просте.

Для подальшого розрахунку необхідно видалити компонент масиву $\gamma_1'(R_1)$ з y_2.

Обчислимо $y_2^{(1)} = \gamma_1'(R_1)^{-1} y_2 = \gamma_2'(R_2) = S\left(*, *, a_{(2)_2}(R_2) + \beta_{(2)}(R_2) + *\right)$.

Повторимо обчислення для R_1 відновлення $y_2^{(1)}$:

$D^{(2)}(R_2) = t_{0(2)} \cdot y_2^{(1)} t_{s(2)}^{-1} = S\left(1, 0, a_{(2)_2}(R_2) + \beta_{(2)}(R_2)\right)$ та $D^*(R) = y_4^{-1} D^{(2)}(R_2) = S\left(1, 0, \beta_{(2)}(R_2)\right)$.

Відновимо R_2 з $\beta_{(2)}(R_2)$ за допомогою $\beta_{(2)}(R_2)^{-1}$. Таким чином, відновлюємо $R = (R_1, R_2)$ та повідомлення m від y_1: $m = \alpha'(R_1, R_2)^{-1} \cdot y_1$.

Практична реалізація

Перевіримо правильність отриманих результатів практичними розрахунками. Зафіксуємо групу $A(P_\infty) = \left\{S(a,b,c) \middle| a \in F_q \setminus \{0\}, b, c \in F_q\right\}$ на основі автоморфізму $\sigma(x), \sigma(y)$ над F_q, $q = 2q_0^2$, $q_0 = 2^3$, $g(\mathrm{x}) = x^7 + x^3 + 1$. Групова операція визначається як добуток двох матриць:

$$S(a_1, b_1, c_1) S(a_2, b_2, c_2) = S(a_1 a_2, a_2 b_1 + b_2, a_2^{2q_0+1} c_1 + a_2 b_2^{2q_0} b_1 + c_2)$$

Обернений елемент визначається як $S(a,b,c)^{-1} = S\left(a^{-1}, -a^{-1}b, \left(a^{-1}b\right)^{2q_0+1} - a^{-(2q_0+1)}c\right)$.

Побудуємо прості логарифмічні підписи $\beta_{(1)} = \left[B_{1(1)}, ..., B_{s(1)}\right] = \left(b_{ij}\right)_{(1)} = S\left(1, b_{ij(1)}, 0\right)$ типу $\left(r_{1(1)}, ..., r_{s(1)}\right)$, $i = \overline{1, s(1)}$, $j = \overline{1, r_{i(1)}}$, $b_{ij(1)} \in F_q$ для координати b та $\beta_{(2)} = \left[B_{1(2)}, ..., B_{s(2)}\right] = \left(b_{ij}\right)_{(2)} = S\left(1, 0, b_{ij(2)}\right)$ типу $\left(r_{1(2)}, ..., r_{s(2)}\right)$, $i = \overline{1, s(2)}$, $j = \overline{1, r_{i(2)}}$, $b_{ij(2)} \in F_q$ для координати c.

Логарифмічні підписи β_1 та β_2 в групі визначають координати $b_{ij(1)}$ та $b_{ij(2)}$. Типи $\left(r_{1(k)}, ..., r_{s(k)}\right)$ і логарифмічні підписи β_1 і β_2 вибираються самостійно. Для практичних розрахунків беремо логарифмічні підписи β_1 та β_2 з типами $\left(r_{1(1)}, r_{2(1)}, r_{3(1)}\right) = \left(2^2, 2^3, 2^2\right)$, $\left(r_{1(2)}, r_{2(2)}, r_{3(2)}\right) = \left(2^2, 2^2, 2^3\right)$, а масиви $b_{ij(1)}$ та $b_{ij(2)}$ складаються з трьох підмасивів з кількістю рядків, що дорівнює r_i. Можемо вибрати будь-яку фрагментацію масивів за умови $\prod_{i=1}^{s} r_i = q$. У нашому випадку маємо $\prod_{i=1}^{s} r_i = 2^7$. Кожен рядок b_{ij} є елементом поля F_q.

Побудова масивів логарифмічних підписів представлена в [12].

Перший етап полягає в генерації простого логарифмічного підпису з розмірністю відповідного вибраного типу $\left(r_{1(k)},...,r_{s(k)}\right)$ та кінцевим полем F_q. Для підвищення безпеки масивів β_k можна використовувати різні криптографічні перетворення. Наприклад, такі прості, як додавання векторів шуму, перестановки рядків у підмасивах B_i, злиття масивів B_i, їх перестановка, перетворення матриці. У цьому прикладі використовуємо шум масиву. Це дозволяє побудувати два різні логарифмічні підписи β_1 та β_2.

У рядку та представленні поля β_1, β_2 мають наступний вигляд:

β_1=	$b_{ij(1)}$			$S\left(0,b_{ij(1)},0\right)$	β_2=	$b_{ij(2)}$			$S\left(0,0,b_{ij(2)}\right)$
$B_{1(1)}$	00	000	00	0,0,0	$B_{1(2)}$	00	00	000	0,0,0
	10	000	00	0,α^{0},0		10	00	000	0,0,α^{0}
	01	000	00	0,α^{1},0		01	00	000	0,0,α^{1}
	11	000	00	0,α^{31},0		11	00	000	0,0,α^{31}
$B_{2(1)}$	00	000	00	0,0,0	$B_{2(2)}$	01	00	000	0,0,α^{1}
	01	100	00	0,α^{32},0		00	10	000	0,0,α^{2}
	10	010	00	0,α^{7},0		11	01	000	0,0,α^{15}
	11	110	00	0,α^{93},0		11	11	000	0,0,α^{93}
	11	001	00	0,α^{121},0	$B_{3(2)}$	10	11	000	0,0,α^{84}
	01	101	00	0,α^{16},0		10	11	100	0,0,α^{46}
	10	011	00	0,α^{11},0		00	10	010	0,0,α^{9}
	11	111	00	0,α^{51},0		00	00	110	0,0,α^{35}
$B_{3(1)}$	00	101	00	0,α^{64},0		10	11	001	0,0,α^{120}
	11	011	10	0,α^{89},0		11	10	101	0,0,α^{76}
	00	11	01	0,α^{117},0		01	10	011	0,0,α^{29}
	11	000	11	0,α^{113},0		00	10	111	0,0,α^{48}

Масиви логарифмічних підписів β_1 та β_2 в груповому представленні визначають координати $b_{ij(1)}$ і $b_{ij(2)}$ відповідно:

$$\beta_{(1)}=\left[B_{1(1)},...,B_{s(1)}\right]=\left(b_{ij}\right)_{(1)}=S\left(0,b_{ij(1)},0\right),\ \beta_{(2)}=\left[B_{1(2)},...,B_{s(2)}\right]=\left(b_{ij}\right)_{(2)}=S\left(0,0,b_{ij(2)}\right).$$

Побудуємо випадкові накриття α_k для одного типу, як β_1 і β_2:

$$\alpha_{(\mathrm{k})}=\left[A_{1(\mathrm{k})},...,A_{\mathrm{s}(\mathrm{k})}\right]=\left(a_{ij}\right)_{(\mathrm{k})}=S\left(a_{ij(\mathrm{k})_1},a_{ij(\mathrm{k})_2},a_{ij(\mathrm{k})_3}\right),$$

де $a_{ij(k)_1},a_{ij(k)_2},a_{ij(k)_3}\in F_q\setminus\{0\}$, $i=\overline{1,s}$, $j=\overline{1,r_{i(k)}}$, $k=\overline{1,2}$. Кожне накриття α_k визначається трьома масивами $\left(a_{ij(k)_1},a_{ij(k)_2},a_{ij(k)_3}\right)$ з ненульовими записами. У полі представлення $\alpha_k=S\left(a_{ij(k)_1},a_{ij(k)_2},a_{ij(k)_3}\right)$ має вигляд:

$\alpha_1=\left[A_{1(1)},A_{2(1)},A_{3(1)}\right]$			$\alpha_2=\left[A_{1(2)},A_{2(2)},A_{3(2)}\right]$		
$A_{1(1)}$	$A_{2(1)}$	$A_{3(1)}$	$A_{1(2)}$	$A_{2(2)}$	$A_{3(2)}$
α^{97}, α^{107}, α^{71}	α^{110}, α^{100}, α^{44}	α^{35}, α^{28}, α^{15}	α^{106}, α^{78}, α^{81}	α^{43}, α^{16}, α^{90}	α^{99}, α^{93}, α^{87}
α^{107}, α^{82}, α^{55}	α^{67},α^{2},α^{87}	α^{105}, α^{19}, α^{68}	α^{92}, α^{33}, α^{41}	α^{114}, α^{85}, α^{82}	α^{65}, α^{88}, α^{23}
α^{118}, α^{86}, α^{6}	α^{43}, α^{86}, α^{87}	α^{45}, α^{8}, α^{29}	α^{124}, α^{80}, α^{125}	α^{21}, α^{77}, α^{114}	α^{17}, α^{68}, α^{73}
α^{69}, α^{17}, α^{54}	α^{70}, α^{95}, α^{125}	α^{23}, α^{42}, α^{82}	α^{48}, α^{63}, α^{47}	α^{92}, α^{71}, α^{119}	α^{116}, α^{98}, α^{116}
	α^{101}, α^{45}, α^{115}				α^{0},α^{53},α^{4}
	α^{40}, α^{82}, α^{25}				α^{108}, α^{79}, α^{81}
	α^{19}, α^{60}, α^{84}				α^{85}, α^{62}, α^{23}
	α^{29}, α^{55}, α^{112}				α^{81}, α^{29}, α^{49}

Згенеруємо випадкові $t_{0(k)}, t_{1(k)}, ..., t_{s(k)} \in A(P_\infty) \setminus Z$, $s = 3$, $k = \overline{1,2}$ та $t_{3(1)} = t_{0(2)}$.

Для логарифмічних підписів β_1, β_2 отримаємо представлення:

$t_{0(1)}, t_{1(1)}, ..., t_{s(1)}$	$t_{0(2)}, t_{1(2)}, ..., t_{s(2)}$
$t_{0(1)=(}\ \alpha^{122}, \alpha^{115}, \alpha^{0})$ $t_{1(1)}=(\ \alpha^{23}, \alpha^{93}, \alpha^{107})$ $t_{2(1)}=(\ \alpha^{30}, \alpha^{105}, \alpha^{23})$ $t_{3(1)}=(\ \alpha^{122}, \alpha^{117}, \alpha^{49})$	$t_{0(2)}=(\ \alpha^{122}, \alpha^{117}, \alpha^{49})$ $t_{1(2)}=(\ \alpha^{98}, \alpha^{9}, \alpha^{109})$ $t_{2(2)}=(\ \alpha^{58}, \alpha^{44}, \alpha^{110})$ $t_{3(2)}=(\ \alpha^{32}, \alpha^{120}, \alpha^{53})$
$t_{-10(1)}=(\ \alpha^{122}, \alpha^{95}, \alpha^{100})$ $t_{-11(1)}=(\ \alpha^{23}, \alpha^{102}, \alpha^{68})$ $t_{-12(1)}=(\ \alpha^{30}, \alpha^{34}, \alpha^{89})$ $t_{-10(1)}=(\ \alpha^{122}, \alpha^{100}, \alpha^{27})$	$t_{-10(2)}=(\ \alpha^{122}, \alpha^{100}, \alpha^{27})$ $t_{-11(2)}=(\ \alpha^{98}, \alpha^{23}, \alpha^{10})$ $t_{-12(2)}=(\ \alpha^{58}, \alpha^{117}, \alpha^{50})$ $t_{-13(2)}=(\ \alpha^{32}, \alpha^{69}, \alpha^{38})$

Наступним кроком є обчислення масивів γ_1 і γ_2.

За початковими умовами прикладу отримуємо:

$$\gamma_1 = \left[h_{1(1)}, ..., h_{3(1)} \right] = \left(h_{ij} \right)_1 = t_{(i-1)(1)}^{-1} f_1 \left(\left(a_{ij} \right)_1 \right) \left(b_{ij} \right)_1 t_{i(1)};$$

$$\gamma_2 = \left[h_{1(2)}, ..., h_{3(2)} \right] = \left(h_{ij} \right)_2 = t_{(i-1)(2)}^{-1} f_2 \left(\left(a_{ij} \right)_2 \right) \left(b_{ij} \right)_2 t_{i(2)}.$$

Побудуємо гомоморфізм f_1, визначений за $f_1\left(S\left(a_1, a_2, a_3\right)\right) = S\left(1, a_1, a_2\right)$, та визначимо гомоморфізм f_2: $f_2\left(S\left(1, a_2, a_3\right)\right) = S\left(1, 0, a_2\right)$.

У полі представлення $\gamma_k = S(h_{ij(k)_1}, h_{ij(k)_2}, h_{ij(k)_3})$, $k = \overline{1,2}$ має вигляд:

$\gamma_1 = S(h_{ij(1)_1}, h_{ij(1)_2}, h_{ij(1)_3})$			$\gamma_2 = S(h_{ij(2)_1}, h_{ij(2)_2}, h_{ij(2)_3})$		
$h_{1(1)}$	$h_{2(1)}$	$h_{3(1)}$	$h_{1(2)}$	$h_{2(2)}$	$h_{3(2)}$
$\alpha^{28}, \alpha^{81}, \alpha^{39}$	$\alpha^{7}, \alpha^{93}, \alpha^{65}$	$\alpha^{92}, \alpha^{16}, \alpha^{80}$	$\alpha^{103}, \alpha^{42}, \alpha^{93}$	$\alpha^{87}, \alpha^{27}, \alpha^{14}$	$\alpha^{101}, \alpha^{79}, \alpha^{29}$
$\alpha^{28}, \alpha^{52}, \alpha^{39}$	$\alpha^{7}, \alpha^{115}, \alpha^{17}$	$\alpha^{92}, \alpha^{53}, \alpha^{102}$	$\alpha^{103}, \alpha^{42}, \alpha^{99}$	$\alpha^{87}, \alpha^{27}, \alpha^{120}$	$\alpha^{101}, \alpha^{79}, \alpha^{51}$
$\alpha^{28}, \alpha^{32}, \alpha^{49}$	$\alpha^{7}, \alpha^{56}, \alpha^{42}$	$\alpha^{92}, \alpha^{51}, \alpha^{117}$	$\alpha^{103}, \alpha^{42}, \alpha^{80}$	$\alpha^{87}, \alpha^{27}, \alpha^{16}$	$\alpha^{101}, \alpha^{79}, \alpha^{55}$
$\alpha^{28}, \alpha^{42}, \alpha^{92}$	$\alpha^{7}, \alpha^{66}, \alpha^{105}$	$\alpha^{92}, \alpha^{57}, \alpha^{114}$	$\alpha^{103}, \alpha^{42}, \alpha^{22}$	$\alpha^{87}, \alpha^{27}, \alpha^{1}$	$\alpha^{101}, \alpha^{79}, \alpha^{38}$
	$\alpha^{7}, \alpha^{44}, \alpha^{106}$				$\alpha^{101}, \alpha^{79}, \alpha^{20}$
	$\alpha^{7}, \alpha^{17}, \alpha^{88}$				$\alpha^{101}, \alpha^{79}, \alpha^{120}$
	$\alpha^{7}, \alpha^{109}, \alpha^{50}$				$\alpha^{101}, \alpha^{79}, \alpha^{53}$
	$\alpha^{7}, \alpha^{26}, \alpha^{7}$				$\alpha^{101}, \alpha^{79}, \alpha^{63}$

Для прикладу беремо $R_1 = 77$. Отримаємо наступну базову факторизацію для заданого типу $\left(r_{1(1)}, r_{2(1)}, r_{3(1)}\right) = \left(2^2, 2^3, 2^2\right)$ у формі $R_1 = \left(R_{1(1)}, R_{2(1)}, R_{3(1)}\right) = (1, 3, 2)$, де $R_1 + R_2 2^2 + R_3 2^5 = 77$ та обчислюємо γ_1:

$$\gamma_1(77) = h_{1(1)}(1) h_{2(1)}(3) h_{3(1)}(2) = S(\alpha^{28}, \alpha^{52}, \alpha^{39}) S(\alpha^{7}, \alpha^{66}, \alpha^{105}) S(\alpha^{92}, \alpha^{51}, \alpha^{117}) = S\left(\alpha^{0}, \alpha^{83}, \alpha^{56}\right).$$

Для прикладу беремо $R_2 = 53$. Отримуємо $R_2 = \left(R_{1(2)}, R_{2(2)}, R_{3(2)}\right) = (1, 1, 3) = 53$ для заданого типу $\left(r_{1(2)}, r_{2(2)}, r_{3(2)}\right) = \left(2^2, 2^2, 2^3\right)$ та отримуємо γ_2:

$$\gamma_2(53) = h_{1(2)}(1) h_{2(2)}(1) h_{3(2)}(3) = S\left(\alpha^{103}, \alpha^{42}, \alpha^{99}\right) S\left(\alpha^{87}, \alpha^{27}, \alpha^{120}\right) S\left(\alpha^{101}, \alpha^{79}, \alpha^{38}\right) = S\left(\alpha^{37}, \alpha^{4}, \alpha^{52}\right).$$

Практичні розрахунки кроку шифрування виконуємо наступним чином.

Нехай $m = \left(\alpha^0, \alpha^1, \alpha^2\right) = S\left(\alpha^0, \alpha^1, \alpha^2\right)$. Згенеруємо випадковий $R = (R_1, R_2)$, $R_1, R_2, \in \square_{|F_q|}$.

Нехай $R_1 = 77$ і $R_2 = 53$. Обчислимо

$$y_1 = \alpha'(R)\cdot m = \alpha_1'(77)\cdot\alpha_2'(53)\cdot m = \alpha_{1(1)}(1)\cdot\alpha_{2(1)}(3)\cdot\alpha_{3(1)}(2)\cdot\alpha_{1(2)}(1)\cdot\alpha_{2(2)}(1)\cdot\alpha_{3(2)}(3)\cdot m = S(\alpha^{107},\alpha^{82},\alpha^{55})$$

$$S(\alpha^{70},\alpha^{95},\alpha^{125})S(\alpha^{45},\alpha^{8},\alpha^{29})S(\alpha^{92},\alpha^{33},\alpha^{41})S(\alpha^{114},\alpha^{85},\alpha^{82})S(\alpha^{116},\alpha^{98},\alpha^{116})$$

$$S\left(\alpha^0,\alpha^1,\alpha^2\right) = S\left(\alpha^{36},\alpha^{86},\alpha^4\right),$$

$$y_2 = \gamma'(R) = \gamma_1'(77)\cdot\gamma_2'(53) = S\left(\alpha^0,\alpha^{83},\alpha^{56}\right)S\left(\alpha^{37},\alpha^4,\alpha^{52}\right) = S\left(\alpha^{37},\alpha^{27},\alpha^{83}\right),$$

$y_3 = f_1\left(\alpha_1'(R_1)\right) = S\left(\alpha^0,\alpha^{36},\alpha^{16}\right)$ та $y_4 = f_2\left(\alpha_2'(R_2)\right) = S\left(\alpha^0,0,\alpha^{21}\right)$.

Тоді зашифроване повідомлення має вигляд

$y_1 = \left(\alpha^{36},\alpha^{86},\alpha^4\right)$, $y_2 = \left(\alpha^{37},\alpha^{27},\alpha^{83}\right)$, $y_3 = \left(\alpha^0,\alpha^{36},\alpha^{16}\right)$, $y_4 = \left(\alpha^0,0,\alpha^{21}\right)$. Щоб розшифрувати повідомлення m, нам потрібно відновити випадкові числа $R = (R_1, R_2)$. Обчислимо

$$D^{(1)}(R_1,R_2) = t_{0(1)}y_2t_{s(2)}^{-1} = S\left(\alpha^{122},\alpha^{115},\alpha^0\right)S\left(\alpha^{36},\alpha^{86},\alpha^4\right)S\left(\alpha^{32},\alpha^{120},\alpha^{53}\right)^{-1} =$$

$$S\left(\alpha^{122},\alpha^{115},\alpha^0\right)S\left(\alpha^{36},\alpha^{86},\alpha^4\right)S\left(\alpha^{32},\alpha^{69},\alpha^{38}\right) = S\left(\alpha^0,\alpha^{12},\alpha^{114}\right)$$

$$D^*(R) = y_3^{-1}D^{(1)}(R_1,R_2) = S\left(\alpha^0,\alpha^{36},\alpha^{16}\right)^{-1}S\left(\alpha^0,\alpha^{12},\alpha^{114}\right) = S\left(\alpha^0,\alpha^{36},\alpha^{34}\right)S\left(\alpha^0,\alpha^{12},\alpha^{114}\right) = S\left(\alpha^0,\alpha^{68},\alpha^{35}\right).$$

Отримаємо $\beta_1(R_1) = \alpha^{68} = (0100101)$.

Відновлення R_1 від $\beta_1(R_1)$

01|001|01	R_1=(*,*,2)
00|111|01	ряд від β(1)
01|110|00	R_1= (*,3,2)
11|110|00	рядок від β(1)
10|000|00	R_1=(1,3,2)

Для подальших обчислень необхідно вилучити $\alpha_1'(R_1)$ з шифротексту компоненти масивів (y_1, y_2) і $\gamma_1'(R_1)$. Обчислимо:

$$y_2^{(1)} = \gamma_1'(R_1)^{-1}y_2 = S\left(\alpha^0,\alpha^{83},\alpha^{56}\right)^{-1}S\left(\alpha^{37},\alpha^{27},\alpha^{83}\right) = S\left(\alpha^0,\alpha^{83},\alpha^{94}\right)^{-1}S\left(\alpha^{37},\alpha^{27},\alpha^{83}\right) = S\left(\alpha^{37},\alpha^4,\alpha^{52}\right).$$

Повторимо обчислення

$$D^{(2)}(R_2) = t_{0(2)}y_2^{(1)}t_{s(2)}^{-1} = S\left(\alpha^{122},\alpha^{117},\alpha^{49}\right)S\left(\alpha^{37},\alpha^4,\alpha^{52}\right)S\left(\alpha^{32},\alpha^{120},\alpha^{53}\right)^{-1} = S\left(\alpha^0,0,\alpha^{18}\right)$$

та

$$D^*(R) = D^{(2)}(R_2)y_4^{-1} = D^{(2)}(R_2)S\left(0,0,a_{(2)_2}(R_2)\right)^{-1} = S\left(\alpha^0,0,\alpha^{18}\right)S\left(\alpha^0,0,\alpha^{21}\right)^{-1} = S\left(\alpha^0,0,\alpha^{25}\right).$$

Відновимо R_2 з $\beta_2(R_2) = \alpha^{25} = (1010110)$.

Виконаємо обернені обчислення $\beta_2(R_2)^{-1}$. Виберемо групи бітів у векторі $\beta(R)$ відповідно до типу $\left(r_{1(2)},...,r_{s(2)}\right) = \left(3,3^2,3^2\right)$. Використовуємо ті ж обчислення, що й у прикладі для $\beta_1(R_1)^{-1}$, та отримаємо:

10|10|110	R_2=(*,*,3)
00|00|110	рядок від β(2)
10|10|000	R_2= (*,1,3)
00|10|000	рядок від β(2)
10|00|000	R_2=(1,1,3)

$$\beta_2(R')^{-1} = 2|02|01 = \left(R_{1(2)},R_{2(2)},R_{3(2)}\right) = (1,1,3),$$

$$R_2 = \left(R_{1(2)},R_{2(2)},R_{3(2)}\right) = (1,1,3) = 53.$$

Дешифруємо повідомлення:

$$m = \alpha'(R)^{-1} y_1 = \alpha_2'(R_2)^{-1} \cdot \alpha_1'(R_1)^{-1} \cdot y_1 = S\left(\alpha^{36}, \alpha^{39}, \alpha^{99}\right)^{-1} S\left(\alpha^{36}, \alpha^{86}, \alpha^{4}\right) =$$

$$S\left(\alpha^{91}, \alpha^{3}, \alpha^{19}\right) S\left(\alpha^{36}, \alpha^{86}, \alpha^{4}\right) = S\left(\alpha^{0}, \alpha^{1}, \alpha^{2}\right).$$

Отримуємо повідомлення $m = \left(a^0, a^1, a^2\right)$.

Аналіз безпеки запропонованого методу

Мета криптоаналітика – знайти невідомий закритий ключ $\left[\beta_{(1)}, \beta_{(2)}, \left(t_{0(1)}, ..., t_{s(1)}\right), \left(t_{0(2)}, ..., t_{s(2)}\right)\right]$. Основні вирази, які визначають параметри відкритого та закритого ключів, такі:

$S(a_1, b_1, c_1) S(a_2, b_2, c_2) = S(a_1 a_2, a_2 b_1 + b_2, a_2^{2q_0+1} c_1 + a_2 b_2^{2q_0} b_1 + c_2)$;

$\beta_{(1)} = \left(b_{ij}\right)_{(1)} = S\left(1, b_{ij(1)}, 0\right)$, $\beta_{(2)} = \left(b_{ij}\right)_{(2)} = S\left(1, 0, b_{ij(2)}\right)$ типів $\left(r_{1(\mathrm{k})}, ..., r_{s(\mathrm{k})}\right)$;

$t_{i(k)} = S\left(t_{i(k)_a}, t_{i(k)_b}, t_{i(k)_c}\right)$;

$\left(a_{ij}\right)_{(\mathrm{k})} = S\left(a_{ij(\mathrm{k})_a}, a_{ij(\mathrm{k})_b}, a_{ij(\mathrm{k})_c}\right)$;

$\gamma_{(\mathrm{k})} = \left(h_{ij}\right)_{(\mathrm{k})} = t_{(i-1)(\mathrm{k})}^{-1} f_k\left(\left(a_{ij}\right)_{(\mathrm{k})}\right)\left(b_{ij}\right)_{(\mathrm{k})} t_{i(\mathrm{k})} = S\left(h_{ij(\mathrm{k})_a}, h_{ij(\mathrm{k})_b}, h_{ij(\mathrm{k})_c}\right)$.

Масив $\gamma_{(\mathrm{k})}$ векторів складається з підмасивів $\gamma_{(1)}$ і $\gamma_{(2)}$, які, в свою чергу, складаються з $s(1)$ і $s(2)$ блоків відповідно.

Розглянемо можливості криптоаналітика на основі $\gamma_{(1)}$ аналізу. Вираз $\gamma_{(1)}$ має вигляд

$$\gamma_{(1)} = \left(h_{ij}\right)_{(1)} = t_{(i-1)(1)}^{-1} f_1\left(\left(a_{ij}\right)_{(1)}\right)\left(b_{ij}\right)_{(1)} t_{i(1)} = S\left(h_{ij(1)_a}, h_{ij(1)_b}, h_{ij(1)_c}\right)$$

Беремо $h_{ij(1)_a}, h_{ij(1)_b}, h_{ij(1)_c}$, наприклад, для першого блоку $\gamma_{(1)}$ масиву:

$h_{1j(1)_a} = t_{0(1)_a}^{*} t_{1(1)_a}$

$h_{1j(1)_b} = t_{0(1)_b}^{*} t_{1(1)_a} + a_{1j(1)_a} t_{1(1)_a} + b_{1j(1)} t_{1(1)_a} + t_{1(1)_b}$

$h_{1j(1)_c} = t_{1(1)_a}^{2q_0+1} t_{0(1)_c}^{*} + t_{1(1)_a}^{2q_0+1} t_{0(1)_b}^{*} a_{1j(1)_a}^{2q_0} + t_{1(1)_a}^{2q_0+1} t_{0(1)_b}^{*} b_{1j(1)}^{2q_0} + t_{1(1)_a}^{2q_0+1} a_{1j(1)_b} +$

$t_{1(1)_a}^{2q_0+1} a_{1j(1)_a} b_{1j(1)}^{q_0} + t_{1(1)_a} t_{1(1)_b}^{2q_0} t_{0(1)_b}^{*} + t_{1(1)_a} t_{1(1)_b}^{2q_0} a_{1j(1)_a} + t_{1(1)_a} t_{1(1)_b}^{2q_0} b_{1j(1)} + t_{1(1)_c}$

Значення $h_{1j(1)_a} = t_{0(1)_a}^{*} t_{1(1)_a}$ однакове для будь-якого j. Якщо додамо елементи з першого зразкового блоку для різних j, то отримаємо

$$\sum_{j \in J} h_{1j(1)_b} = |J| t_{0(1)_b}^{*} t_{1(1)_a} + t_{1(1)_a} \sum_{j \in J} a_{1j(1)_a} + t_{1(1)_a} \sum_{j \in J} b_{1j(1)}$$

$|J|$ – кількість елементів у J наборі. Для парного значення $|J|$ отримуємо рівняння $\sum_{j \in J} h_{1j(1)_b} = t_{1(1)_a} \sum_{j \in J} a_{1j(1)_a} + t_{1(1)_a} \sum_{j \in J} b_{1j(1)}$ з двома невідомими $t_{1(1)_a}$ і $\sum_{j \in J} b_{1j(1)}$. Існує кілька $q-1$ можливих $t_{1(1)_a}$ варіантів. Зафіксуємо значення $\hat{t}_{1(1)_a}$ і нехай $|J| = 2$. Складемо всі вибірки з пар значень. У нас є $r_{1(1)}(r_{1(1)} - 1)/2$ рівняння для невідомих $b_{1j(1)}$:

$$\hat{t}_{1(1)_a}^{-1} \sum_{j \in J} h_{1j(1)_b} + \sum_{j \in J} a_{1j(1)_a} + \sum_{j \in J} b_{1j(1)} = 0.$$

Розв'язок цих рівнянь визначає логарифмічний підпис для першого блоку відносно вибраного $\hat{t}_{1(1)_a}$. Оскільки є $q-1$ можливі варіанти $t_{1(1)_a}$, отримуємо $q-1$ можливі варіанти логарифмічних підписів. Оскільки для побудови логарифмічного підпису використовується

рандомізація на основі шуму, злиття та матричні перетворення підблоків, питання про те, як можна встановити, що $\hat{t}_{1(1)_a}$ – істинне, не має відповіді. Припустимо, що рівняння матриці перетворення для логарифмічних сигнатур мають поліноміальну оцінку складності розділь-ної здатності, тоді нижню межу можна взяти для оцінки складності атаки $b_{1j(1)}$ на $\mathrm{O}(q)$. Для $\hat{t}_{1(1)_a}$ можна обчислити , $\hat{t}^*_{0(1)_a} = \hat{t}^{-1}_{1(1)_a} h_{1j(1)_a}$, а щоб визначити $t^*_{0(1)_b}$, $t_{1(1)_b}$ потрібно розв'язати рів-няння $h_{1j(1)_b} = t^*_{0(1)_b} t_{1(1)_a} + a_{1j(1)_a} t_{1(1)_a} + b_{1j(1)} t_{1(1)_a} + t_{1(1)_b}$.

Існують $q-1$ можливі варіанти $t^*_{0(1)_b}$, $t_{1(1)_b}$. Тоді отримуємо оцінку складності атаки за $t_{i(1)_a}, t_{i(1)_b}$ параметрами $t_{i(1)}$ вектора, що дорівнює $\mathrm{O}(q^2)$. Це те саме для визначення $t^*_{0(1)_c}$, $t_{1(1)_c}$, де можна розв'язати рівняння для $h_{1j(1)_c}$ в межах вибору $q-1$ можливих значень $t^*_{0(1)_c}$, $t_{1(1)_c}$. Результуюча атака на $t_{i(1)} = S\left(t_{i(1)_a}, t_{i(1)_b}, t_{i(1)_c}\right)$ за складністю буде меншою ніж $\mathrm{O}(q^3)$.

Для $s(1)$ підблоків логарифмічного підпису $\gamma_{(1)}$ маємо застосувати $s(1)$ час для пошуку $t_{i(1)} = S\left(t_{i(1)_a}, t_{i(1)_b}, t_{i(1)_c}\right)$, і підсумкова складність атаки буде оцінена в $\mathrm{O}(q^{3s(1)})$.

Поширимо цю атаку на всі підблоки логарифмічного підпису. Отримаємо вираз $\sum_{i=1,\, j=j_i}^{s(1)} h_{ij(1)_b} = t^*_{0(1)_b} t_{s(1)_a} + t_{s(1)_a} \sum_{i=1,\, j=j_i}^{s(1)} a_{ij(1)_a} + t_{s(1)_a} \sum_{i=1,\, j=j_i}^{s(1)} b_{ij(1)} + t_{s(1)_b}$, де $(j_1, ..., j_{s(1)})$ – номери обраних записів у відповідних підблоках. Зробимо парну вибірку за записами підблоків, отримаємо рівняння

$$\sum_{i=1,\, j\in J_i}^{s(1)} h_{ij(1)_b} = t_{s(1)_a} \sum_{i=1,\, j\in J_i}^{s(1)} a_{ij(1)_a} + t_{s(1)_a} \sum_{i=1,\, j\in J_i}^{s(1)} b_{ij(1)},$$

що однаково для атаки на один підблок. Аналогічний вираз отримуємо для $h_{ij(1)c}$. Можна з високою впевненістю припустити, що складність атаки в цьому випадку не буде меншою $\mathrm{O}(q^3)$.

Розглянемо атаку відновлення $t_{1(1)_a}$ зі значення $b_{1j(1)}$. У рівнянні для $\sum_{j\in J} h_{1j(1)_b}$ будемо вибирати $b_{1j(1)}$ таким чином, що $\sum_{j\in J} b_{1j(1)} = 0$. Значення $\hat{t}_{1(1)_a}$ можуть бути в межах рівняння $\hat{t}^{-1}_{1(1)_a} \sum_{j\in J} h_{1j(1)_b} + \sum_{j\in J} a_{1j(1)_a} = 0$.

Нам відомі $h_{1j(1)_b}$ та $a_{1j(1)_a}$. Атака на логарифмічний підпис була запропонована в [16]. Залишається відкритим питання, як ідентифікувати один раз $\sum_{j\in J} b_{1j(1)} = 0$ для рандомізованого логарифмічного підпису. Якщо побудувати аперіодичний логарифмічний підпис без наявно-сті таких блоків $\sum_{j\in J} b_{1j(1)} = 0$, то така атака стає неможливою [16].

Тепер розглянемо криптоаналіз для масиву $\gamma_{(2)}$. Основні вирази для першого блоку масиву $\gamma_{(2)}$:

$$\gamma_{(2)} = \left(h_{ij}\right)_{(2)} = t^{-1}_{(0)(2)} f_2\left(\left(a_{ij}\right)_{(2)}\right)\left(b_{1j}\right)_{(2)} t_{1(2)} = S\left(t^*_{0(2)_a}, t^*_{0(2)_b}, t^*_{0(2)_c}\right)$$
$$S\left(1, 0, a_{ij(1)_c} + b_{ij(2)}\right) S\left(t_{s(2)_a}, t_{s(2)_b}, t_{s(2)_c}\right) = S\left(h_{ij(2)_a}, h_{ij(2)_b}, h_{ij(2)_c}\right)$$

Узагальнимо цю атаку на всі підблоки логарифмічного підпису. Отримаємо вирази:

$$\sum_{i=1,\,j=j_i}^{s(2)} h_{ij(2)_a} = t^*_{0(2)_a} t_{s(2)_a}, \qquad \sum_{i=1,\,j=j_i}^{s(2)} h_{ij(2)_b} = t^*_{0(2)_b} t_{1(2)_a} + t_{1(2)_b},$$

$$\sum_{i=1,\,j=j_i}^{s(2)} h_{ij(2)_c} = t^{2q_0+1}_{s(2)_a} t^*_{0(2)_c} + t^{2q_0+1}_{s(2)_a} \sum_{i=1,\,j=j_i}^{s(2)} a_{ij(2)_c} + t^{2q_0+1}_{s(2)_a} \sum_{i=1,\,j=j_i}^{s(2)} b_{1j(2)} + t_{s(2)_a} t^{2q_0}_{s(2)_b} t^*_{0(2)_b} + t_{s(2)_c},$$

де $(j_1,..., j_{s(2)})$ – номери виділених записів у відповідних підблоках. Зробимо парну вибірку за записами підблоків, маємо таке рівняння:

$$\sum_{i=1,\,j\in J_i}^{s(2)} h_{ij(2)_c} = t^{2q_0+1}_{s(2)_a} \sum_{i=1,\,j\in J_i}^{s(2)} a_{ij(2)_c} + t^{2q_0+1}_{s(2)_a} \sum_{i=1,\,j\in J_i}^{s(2)} b_{1j(2)}.$$

Рівняння має два невідомих $t_{s(2)_a}$ і $\sum_{j\in J} b_{ij(2)}$. Існують $q-1$ можливі варіанти $t_{s(2)_a}$. Як і у випадку з масивом $\gamma_{(1)}$, у нас є те саме відкрите питання про те, як з'ясувати, де $t_{s(2)_a}$ – істинне значення рандомізованого логарифмічного підпису. Можна з високою впевненістю припустити, що складність атаки на $t_{s(2)_a}$ буде меншою, ніж $O(q)$ в такому випадку, а складність атаки на всі компоненти $t_{0(2)} = S\left(t_{0(2)_a}, t_{0(2)_b}, t_{0(2)_c}\right)$і $t_{s(2)} = S\left(t_{s(2)_a}, t_{s(2)_b}, t_{s(2)_c}\right)$ буде меншою, ніж $O(q^3)$.

Підводячи підсумки щодо атаки з закритим ключем, можна зробити висновок, що складність буде не меншою $O(q^3)$.

Розглянемо основні атаки на зашифрований текст. Успіх атаки зашифрованого тексту визначається знаходженням ключа $R=(R_1,R_2)$. Мають місце наступні види атак.

Атака грубою силою на зашифрований текст. Обираємо $R=(R_1,R_2)$ та спробуємо розшифрувати текст $y_1 = \alpha'(R)\cdot m = \alpha_1'(R_1)\cdot\alpha_2'(R_2)\cdot m$. Успіх атаки визначається попередньою інформацією про повідомлення. Складність атаки визначається умовою повного пошуку ключів R_1, R_2 і його рівністю $O(q^2)$.

Атака грубою силою на $R=(R_1,R_2)$. Обираємо $R=(R_1,R_2)$ відповідно $y_2 = \gamma'(R) = \gamma_1'(R_1)\cdot\gamma_2'(R_2)$. Складність такої атаки $O(q^2)$. Можлива послідовна атака відновлення R_1, R_2. Обираємо R_1 відповідно до значення $a_{(1)_1}(R_1)$ у векторі y_1 та обираємо R_2 відповідно значенню $a_{(2)_2}(R_2)$ у векторі y_2. Атака має складність $O(q)$. Для захисту від атаки послідовного відновлення слід розглянути механізми зв'язування ключів.

Атака на алгоритм. Параметри вилучення $a_{(1)_1}(R_1)$, $a_{(2)_2}(R_2)$з y_3, y_4 не дозволяють обчислити $\alpha_1'(R_1)\cdot\alpha_2'(R_2)$в $y_1 = \alpha_1'(R_1)\cdot\alpha_2'(R_2)\cdot m$. Простий пошук параметрів R_1, R_2 призводить до атаки грубої сили зі складністю q^2. Оскільки група автоморфізму $A(P_\infty)$ функціонального поля Сузукі визначена над великим полем F_q, атака обчислювально неможлива.

Висновки

У роботі обґрунтовано наступні переваги пропозиції: висока секретність схеми шифрування на основі групи автоморфізмів поля $A(P_\infty)$ функції Сузукі над F_q, що дорівнює q^2; довжина зашифрованого тексту призначена $3\log q$ для обчислення в скінченному полі над F_q; обчислення в кінцевому полі простіші в порівнянні з криптосистемою в групі Сузукі. Крім того, шифрування виконується на кінцевому полі втричі меншого розміру порівняно з

криптосистемою на основі груп Сузукі, а довжина логарифмічного масиву підпису визначається кінцевим полем понад F_q і є значно меншою порівняно з криптосистемою MST3.

Реалізація криптосистеми на групі автоморфізмів $A(P_\infty)$ функціонального поля Сузукі вимагає побудови логарифмічного підпису β на векторах 2^h, де h визначається розміром типу $r_i = 2^h$. Підкреслимо, що всі блоки B_i є підгрупами $U(q) = \left\{ S(1,b,c) \middle| b,c \in F_q \right\}$. Розмір масивів β і α визначається типом $(r_1,...,r_s)_b$ і $(r_1,...,r_s)_c$ координатою b,c для підгруп $U(q)$. Для 128-бітної криптографії, яка еквівалентна обчисленням над полем $q = 2^{64}$, якщо r_i тип $r_i = 2^2$, $s = 32$, для криптографії в групі потрібні лише 256 записів по 64 біти. У порівнянні з MST3 у Сузукі 2-групи матиме 256 записів по 128 біт для $r_i = 2^2$, $s = 64$ і 512 записів – для $r_i = 4^2$, $s = 32$. Однак це все ще є недоліком пропозиції з великим розміром ключових даних і необхідністю обчислення оберненого елемента в кінцевому полі.

Список літератури:

1. K.H. Ko, S.J. Lee, J.H .Cheon, J.W. Han, J. Kang, and C. Park. New public-key cryptosystem using braid groups // Advances in cryptology–CRYPTO 2000, vol.1880of Lecture Notes in Computer Science, pp. 166–183, Springer, Berlin, Germany, 2000.
2. B. Eick and D. Kahrobaei. Polycyclic groups: a new platform for cryptology // http://arxiv.org/abs/math/0411077.
3. V. Shpilrain and A. Ushakov. Thompsons group and public key cryptography // Applied Cryptography and Network Security, vol. 3531 of Lecture Notes in Computer Science, pp. 151–164, 2005.
4. D. Kahrobaei, C. Koupparis, and V. Shpilrain. Public key exchange using matrices over group rings // Groups, Complexity, and Cryptology ,vol.5,no.1, pp.97–115, 2013.
5. N.R. Wagner and M.R. Magyarik. A public-key cryptosystem based on the word problem // Proc. Advances in Cryptology–CRYPTO 1984, LNCS 196, Springer-Verlag (1985), pp. 19–36.
6. S.S. Magliveras. A cryptosystem from logarithmic signatures of finite groups // Proceedings of the 29th Midwest Symposium on Circuits and Systems , pp. 972–975, Elsevier Publishing, Amsterdam, The Netherlands, 1986.
7. W. Lempken, S.S. Magliveras, Tran van Trung and W. Wei. A public key cryptosystem based on non-abelian finite groups // Journal of Cryptology, 22 (2009), 62–74.
8. H.Hong, J.Li, L.Wang, Y. Yang, X.Niu. A Digital Signature Scheme Based on MST3 Cryptosystems // Hindawi Publishing Corporation, Mathematical Problems in Engineering, vol 2014, 11 p., http://dx.doi.org/10.1155/2014/630421
9. Y. Cong, H. Hong, J. Shao, S. Han, J. Lin and S. Zhao. A New Secure Encryption Scheme Based on Group Factorization Problem // IEEExplore, November 20, 2019 Digital Object Identifier 10.1109/ACCESS.2019.2954672 https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8907845
10. P. Svaba and T. van Trung. Public key cryptosystem MST3 cryptanalysis and realization // Journal of Mathematical Cryptology,vol.4,no.3,pp.271–315,2010
11. T. van Trung. Construction of strongly aperiodic logarithmic signatures // Journal Math. Cryptol., vol. 12, no. 1, pp. 23–35, 2018.
12. Kotukh Y., Severinov E., Vlasov O., Tenytska A., Zarudna E. Some results of development of cryptographic transformations schemes using non-abelian groups // Радіотехніка. 2021. Вип. 204. С. 66–72.
13. Котух Є., Сєвєрінов О., Власов А. та ін. Методи побудови та властивості логарифмічних підписів // Радіотехніка. 2021. Вип. 205. С. 94–99. https://doi.org/10.30837/rt.2021.2.205.09
14. Kotukh Y., Khalimov G. Hard Problems for Non-abelian Group Cryptography, 2021 // Fifth International Scientific and Technical Conference "Computer and Information systems and technologies". https://doi.org/10.30837/csitic52021232176
15. Халімов Г., Котух Є., Сергійчук Ю., Марухненко О. Аналіз складності реалізацій криптосистеми на групі Сузукі // Радіотехніка. 2018. Вип. 193. С. 75–81.
16. Котух Є., Охріменко Т., Дяченко О., Ротаньова Н., Козіна Л., Зеленський Д. Криптоаналіз систем на основі проблеми слова з використанням логарифмічних підписів // Радіотехніка. 2021. Вип. 206. С. 106–114. https://doi.org/10.30837/rt.2021.3.206.09
17. 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.
18. 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.

19.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

20.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.

21.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

22.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.

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

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

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

26.Kotukh Y., Khalimov G., Korobchinsky M. Construction of a three-parameter encryption scheme on Hermitian groups in the MST3 cryptosystem // Radiotekhnika. 2023. 213. P. 49–55. https://doi.org/10.30837/rt.2023.2.213.05

27.Kotukh Y., Khalimov G., Korobcninskiy M. Method of Security Improvement for MST2 Cryptosystem Based on Automorphism Group of Ree Function Field// 2023 Theoretical and applied cybersecurity, vol.5, no. 2, pp. 31–39. https://doi.org/10.20535/tacs.2664-29132023.2.290414

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

Надійшла до редколегії 20.08.2023

Відомості про авторів:

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

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

Коробчинський Максим Володимирович, д-р техн. наук, професор, начальник 2-ї кафедри технічних видів розвідки та інформаційних технологій 2-го навчального інституту Воєнної академії імені Євгенія Березняка Міністерства оборони України, м. Київ, Україна; mars_kor@ukr.net; ORCID:https://orcid.org/0000-0001-8049-4730,

УДК 621.396.671 **DOI:10.30837/rt.2023.3.214.06**

Р.І. ЦЕХМІСТРО, канд. фіз.-мат. наук, С.В. ШАПОВАЛОВ, канд. техн. наук

ОСОБЛИВОСТІ ФОРМУВАННЯ ОПТИМАЛЬНОГО РОЗПОДІЛУ АКУСТИЧНОГО ПОЛЯ КІЛЬЦЕВОЇ ЕКВІДИСТАНТНОЇ ТА НЕЕКВІДИСТАНТНОЇ ДВОСЕКЦІЙНОЇ МІКРОФОННОЇ РЕШІТКИ З ЕЛЕКТРОННИМ КЕРУВАННЯМ

Вступ

Фазовані мікрофонні решітки знайшли широке застосування пристроїв обробки акустичних сигналів з метою збільшення співвідношення сигнал/шум в заданому напрямку. Наприклад, у стільниковому телефоні найпростіші мікрофонні решітки складається всього з двох мікрофонів і служить для збільшення співвідношення сигнал/шум говорить [1 – 3].

Більш складні фазовані мікрофонні ґрати зазвичай складаються з чотирьох і більше мікрофонів. Їхня кількість може досягати 64 і навіть 512 штук. Головне призначення фазованих мікрофонних ґрат – створити потрібну діаграму спрямованості в заданому напрямку, оперативно змінювати цей напрям у просторі і тим самим збільшити співвідношення сигнал/шум від обраного акустичного джерела, на який спрямована фазована антенна решітка [4 – 7]. Велика кількість мікрофонів значно впливає на вартість решітки.

Особливості аналізу акустичних решіток

У роботі описано аналіз просторового розподілу амплітуди акустичного поля кільцевої мікрофонної решітки (рис. 1). Кожен мікрофон був представлений моделлю – випромінювачем сферичної хвилі (ізотропний випромінювач). Проведено аналіз впливу числа випромінювачів, радіуса ґрат на концентрацію акустичного поля в центрі ґрат і на довільній відстані. Складено алгоритм, що дозволяє враховувати довільне парне та непарне число випромінювачів, розташоване по довжині дуги при рівномірному та нерівномірному розташуванні [4, 7].

Рис. 1. Мікрофонна решітка BSWA-TECH SPS-980 [3]

Сигнал з мікрофона решітки (рис. 1) надходить на підсилювач, далі йде на аналоговий коректор фази, який побудований на операційному підсилювачі, що зсуває фазу RC ланцюжком. Причому використовується не звичайний резистор, а керований I2C. Далі сигнал йде на аналого-цифровий перетворювач АЦП, де оцифровується і надходить у програмовану логічну інтегральну схему – ПЛІС по паралельній шині або, у кращому випадку, послідовному периферійному інтерфейсу ППІ. У першому випадку потрібно щонайменше 17 ліній зв'язку, у другому – 5. На практиці широко використовуються мікрофонні решітки з великим масивом випромінювачем, що потребує використання дорогого електронного обладнання,

вартість якого пропорційна кількості мікрофонів [1, 5, 6]. У зв'язку з цим актуальним стає питання зниження кількості використовуваних мікрофонів в решітки при збереженні їх електричних характеристик, що призводить до зниження вартості відповідного електронного обладнання.

Метою статті є пошук шляхів вирішення зазначеної задачі на основі виявлення фізичних особливостей акустичних грат.

Особливості ближньої та проміжної зони проявляються насамперед у тому [4, 7], що просторовий розподіл амплітуд та потужності звукового поля не має характеру сформованої діаграми спрямованості з головними та бічними пелюстками. В області напрямів нулів діаграми спрямованості грат амплітуда поля досить висока. Однак поза напрямом максимуму діаграми спрямованості в області проміжної зони, де потенційно може бути джерело звуку, можуть виникати ситуації, коли менше випромінювачів при певній конфігурації забезпечує більш високе значення потужності поля в певних локальних областях [4, 7, 8].

Основна частина

У [7] розглянуто розподіл комплексної потужності акустичного поля лінійних ґрат випромінювачів у припущенні, що кожен мікрофон (випромінювач) транслює акустичне поле у вигляді сферичної хвилі. Відповідно до класичних положень (лема Лоренца, теорема "Взаємності") вважаємо, що форма діаграми спрямованості як сформованої немає, тобто розподіл поля випромінювача в режимі прийому та передачі акустичного сигналу ідентичний.

Через малі відстані між мікрофонами решітки і точками спостереження останні можуть перебувати як у ближній (проміжній), так і в дальній зоні безпосередньо кожного випромінювача.

У нашій поточній задачі точки спостереження знаходяться також у проміжній зоні решітки випромінювачів. Таким чином, необхідно враховувати обидва прояви особливостей проміжного поля одиночного випромінювача, і решітки, зокрема, розробки алгоритмів розрахунків розподілу поля і потужності.

Обмежимося розглядом задачі, яка полягає в аналізі фізичних закономірностей формування розподілу амплітуди поблизу грат випромінювачів. Це дозволяє врахувати особливості ближньої та проміжної зони як решітки випромінювачів, а й кожного випромінювача окремо. Візьмемо рішення для ізотропного випромінювача як сферичної хвилі:

$$U_n = \sum_{n=-N/2}^{N/2} U_0 \frac{\cos(\omega t - kR_n)}{R_n}; \quad (1)$$

де R – відстань від центру випромінювача до точки спостереження; N – число випромінювачів, симетрично розташованих від центру решітки.

Розглянемо далі лінійні ґрати з N+Nm мікрофонів, розташованих за великим і малим радіусом. Введемо декартову систему координат, як показано на рис. 2. Для знаходження амплітуди поля поблизу ґрат мікрофонів розташуємо їх уздовж осі OX, і відстань Rn до точки спостереження будемо визначати в декартових координатах. Спочатку представимо результат аналізу просторового розподілу амплітуди поля решітки на малих та середніх відстанях за відсутності взаємодії між елементами решітки (теорія елементарного випромінювача). Сумарні компоненти полів у кожній точці спостереження знаходимо згідно з принципом суперпозиції:

$$U = \sum_{n=-(N+Nm)/2}^{(N+Nm)/2} U_n \quad (2)$$

для парного числа мікрофонів,

$$U = U_o + \sum_{n=(-N-Nm+2)/2}^{(N+Nm-2)/2} U_n \qquad (3)$$

для непарного числа випромінювачів (мікрофонів), де n – номер випромінювача (мікрофона), N, Nm – число випромінювачів, розташованих уздовж півосі OX по великому та малому радіусах відповідно.

Для конкретності розглядатимемо близьку до практики систему [4, 7, 8], коли випромінювачі розташовуються еквідистантно на колі радіуса R і Rm (рис. 2). Для аналізу досліджуваних фізичних закономірностей необхідно враховувати, що область фокусування акустичного поля знаходиться у ближній зоні як джерела звуку, так і масиву. Сумарні амплітуди полів мікрофонів у кожній точці простору знаходимо згідно з принципом суперпозиції.

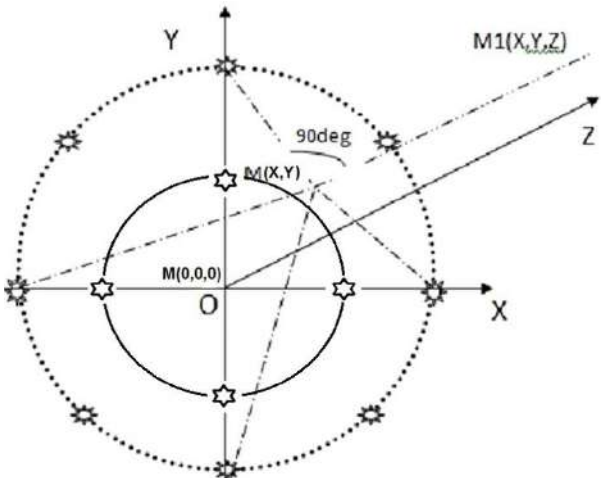


Рис. 2. Схема розташування мікрофонів у кільцевій двосекційній решітці

При цьому відстані Rn від *n*-го випромінювача до точки спостереження M (X, Y, Z), що визначають фази складових полів кожного мікрофона в точці спостереження (рис. 2), знаходимо аналогічно викладеному вище алгоритму для лінійних решіток. Формула для розрахунку відстаней Rn залежить від взаємного розташування точки випромінювання та точки спостереження. У загальному випадку

$$R_n = \sqrt{Z^2 + (Y_n \pm Y)^2 + (X_n \pm X)^2}\,; \qquad (4)$$

де Xn,Yn – координати *n*-го випромінювача; X,Y – координати точки спостереження в декартових координатах, пов'язаних з ґратами; Z – відстань від плоскості решітки, як показано на рис. 2.

Знак “+” у виразі (4) береться у разі, якщо точка спостереження M (X, Y) перебуває у першому квадранті, знак " – " береться у разі, якщо вона у третьому квадранті, знаки “+,-” чергуються, якщо точка спостереження та джерело знаходяться у другому та четвертому квадрантах.

На практиці в решітках, що розглядаються, зручно розташовувати мікрофони на однакових відстанях один від одного, вибираючи відповідним чином радіус решітки R. Тоді вираз для Rn може бути записаний через радіус решітки та кут α між променями, спрямованими з початку координат на два сусідні джерела.

Для точки спостереження всередині кільця радіуса R на відстані Z:

$$R_n = \sqrt{Z^2 + (X - R\sin(n\alpha))^2 + (Y - R(\cos(\pi - n\alpha)))^2}\,, \qquad (5)$$

n=0,±1,±2,...N/2 для непарного N,

$$R_n = \sqrt{Z^2 + (X - R\sin((2n-1)\alpha/2))^2 + (Y - R(\cos(\pi - (2n-1)\alpha/2)))^2}\,, \qquad (6)$$

n=±1,±2,...N/2 для парного N.

Для мікрофонів, розташованих по малому радіусу,

$$Rm_n = \sqrt{Z^2 + (X - Rm\sin(nm\alpha))^2 + (Y - Rm(\cos(\pi - nm\alpha)))^2}\,, \qquad (7)$$

nm=0,±1,±2,...Nm/2 – для непарного Nm,

$$Rm_n = \sqrt{Z^2 + (X - Rm\sin((2nm-1)\alpha/2))^2 + (Y - Rm(\cos(\pi - (2nm-1)\alpha/2)))^2}, \quad (8)$$

n=±1,±2,...N/2 – для парного N.

У разі нееквідистантного розташування мікрофонів у ґратах формули (5) – (6) трохи перетворюються так:

$$Rd_n = \sqrt{Z^2 + (X - R\sin(n(\alpha \pm \Delta\alpha))^2 + (Y - R(\cos(\pi - n(\alpha \pm \Delta\alpha))))^2}, \quad (9)$$

n=0,±1,±2,...N/2 – для непарного N;

$$Rd_n = \sqrt{Z^2 + (X - R\sin((2n-1)(\alpha \pm \Delta\alpha)/2))^2 + (Y - R(\cos(\pi - (2n-1)(\alpha \pm \Delta\alpha)/2)))^2}, \quad (10)$$

n=±1,±2,...N/2 – для парного N.

У цих співвідношеннях $\Delta\alpha = 2\arcsin(d/2R)$, де d – найкоротша відстань між мікрофонами (довжина хорди), R – радіус дуги розміщення мікрофонів.

Кут меж мікрофонами $\alpha = 2\pi/N$, де N – кількість мікрофонів.

Таким чином, задаючи радіус кільця – R, кут – α, який визначає відстань між джерелами звуку та їх число, будемо аналізувати вплив цих параметрів на просторовий розподіл поля всередині та поза ґратами, а також і вздовж якоїсь осі. З'являється можливість отримати просторове розподілення поля на відстані Z від площини розташування мікрофонів.

З використанням виразів (5) – (8) були розроблені алгоритм та програма комп'ютерного аналізу, що дозволяє досліджувати просторовий розподіл потужності поля всередині решітки з урахуванням та без урахування особливостей полів ближньої та проміжної зони елемента решітки.

Аналіз розрахунків параметрів решітки з односекційним розмішуванням мікрофонів

Результати розрахунків можуть бути представлені як ліній рівного рівня амплітуд полів або потужності, так і у вигляді відповідних залежностей уздовж будь-якої координати. У розроблених алгоритмах і програмах жодних обмежень на розміри решітки, кількість випромінювачів та їх становище у ґратах не накладається.

Розрахунки проводилися для двох варіантів: у першому задавалася відстань по дузі кола між випромінювачам у довжинах хвиль, що виключало симетрію решітки, а також для цілих значень кута α наприклад – 15,30,45,60 град. Другий варіант дозволяв розташувати випромінювачі (мікрофони) симетрично не тільки щодо осі OY, але і щодо осі OX, а також по дузі меншого радіусу.

На рис. 3 представлено просторовий розподіл сумарної амплітуди поля випромінювання кільцевої решітки 12 мікрофонів. з радіусом рівним 1,5λ (три випромінювачі по дузі з радіусом R=0,7λ). Розрахункові значення нормовані на максимальне значення. Видно чіткі концентрації акустичного поля в центрі решітки, і на відстанях від центру, рівних λ. Виразно спостерігається концентрація поля у точках розташування випромінювачів. Чітко видно інтерференційні максимуми між мікрофонами.

На відстані рівних приблизно чверть довжини хвилі простежується інтерференційний сплеск амплітуди акустичного поля поблизу кожного випромінювача.

Розрахункові значення унормовані на максимальне значення. Цей результат відповідає фізичному уявленню та свідчить про правильність створеного алгоритму. Подальші розрахунки встановили чіткі концентрації акустичного поля у центрі решітки, з відносним значенням поля більшого розміру, ніж решітки з радіусом рівним 2λ. Виразно спостерігається концентрація поля у точках розташування випромінювачів. Другий варіант дозволяв розташувати випромінювачі (мікрофони) симетрично щодо осі OY, але і щодо осі OX.

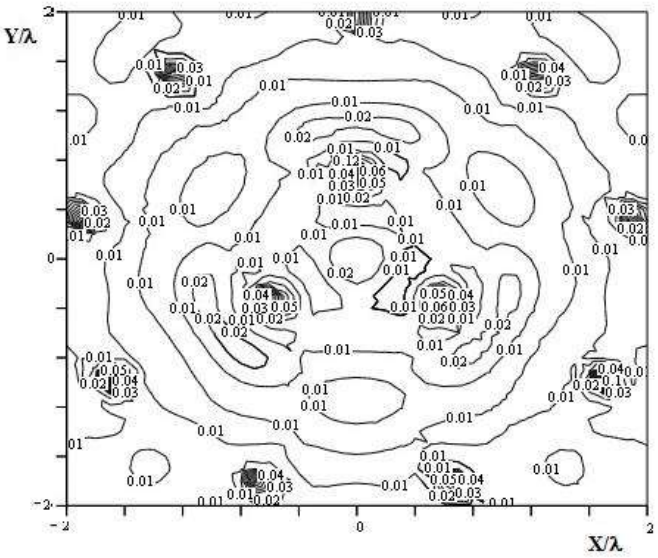


Рис. 3. Розподіл сумарного поля двосекційної акустичної решітки N=12 мікрофонів (3 мікрофони на малій дузі Rm=0,7λ) Z=0, R=2λ

На відстані, рівній приблизно чверті довжини хвилі, простежується інтерференційний сплеск амплітуди акустичного поля поблизу кожного випромінювача.

Цей результат відповідає фізичному уявленню та свідчить про правильність створеного алгоритму. Подальші розрахунки встановили чіткі концентрації акустичного поля у центрі решітки з відносним значенням поля більшого розміру, ніж решітки з радіусом рівним 2λ.

Збільшення радіуса решітки призводить до більшої кількості інтерференційних максимумів, ніж видно на рис. 3. Аналіз наступних розрахунків показав, що збільшення числа мікрофонів при фіксованому радіусі призводить до більш рівномірного розподілу звукового випромінювання в центрі решітки на відстані, що дорівнює довжині хвилі.

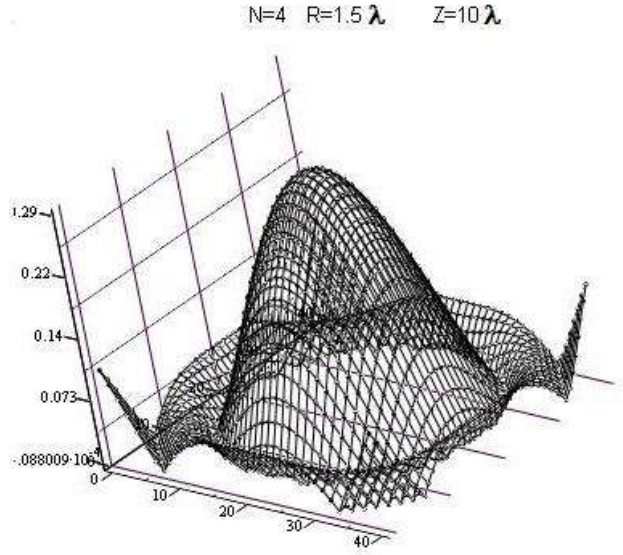


Рис. 4. Розподіл поля акустичної еквідістантної решітки мікрофонів рівня N=4 (по великій дузі), Z=10λ, R=1,5λ

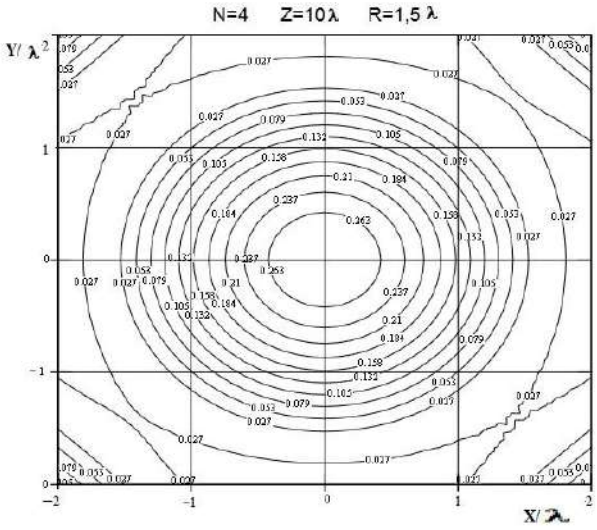


Рис. 5. Розподіл поля еквідістантної решітки з N=4, Z=10λ, R=1,5λ у вигляді контурів рівного значення

На рис. 4 представлено просторовий розподіл сумарної амплітуди поля випромінювання кільцевої решітки 4 акустичних випромінювачів. з радіусом рівним 1.5λ при рівномірному розміщенні по великому радіусу.

На рис. 5 видно розподіл акустичного поля для грат з чотирьох випромінювачів у вигляді поверхневих ліній, з виразним максимумом в центрі решітки на відстані в 10 довжин хвиль. Довжина хвилі у разі є параметром рівним 1.

На рівновіддаленій відстані від центру решітки, більшому, чи рівному радіусу решітки, відмінності за абсолютним значенням менш значні, але відрізняються формою. Форма розподілу поля у напряму, перпендикулярному центру решітки, має конусоподібну форму, представлену на рис. 5, для чотирьох мікрофонів на відстані 10 довжин хвиль.

Графіки, представлені на рис. 6, показують, що у відстанях рівних близьких до 1,8λ і 2,4λ вздовж лінії рівновіддаленої від координатних осей абсолютні значення сумарної амплітуди полів практично збігаються.

Графіки, представлені на рис. 7, показують більше значення абсолютної амплітуди поля для двох випромінювачів, розташованих на осі X на відстані між 1,4λ – 2λ. Показано також, що розподіл поля вздовж осі Y при Z=10λ и радіусі решітки R=1,5λ для решіток з двох та чотирьох мікрофонів має практично рівні значення сумарної амплітуди акустичного поля на відстанях, відповідних 1,6λ – 1,7λ, які рівновіддалені від центру решітки вздовж осі Y.

Далі розглянемо еквідистантне розташування випромінювачів по двох радіусах (двох кільцях) аналогічно рис. 1 в моделі, запропонованій на рис. 2. Рис. 3 наочно демонструє правильність роботи запропонованого алгоритму (5) – (8), видно розташування кожного мікрофона (дворадіусне розташування) по дузі з малим радіусом 0,7 довжини хвилі та зовнішнім радіусом – рівним двом довжинам хвилі R=2λ.

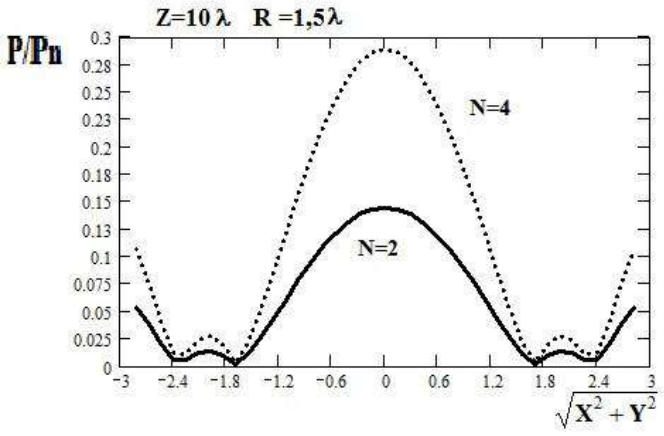


Рис. 6. Розподіл поля решітки з двох та чотирьох мікрофонів уздовж діагоналі (див рис. 5) Z=10λ, R=1,5λ

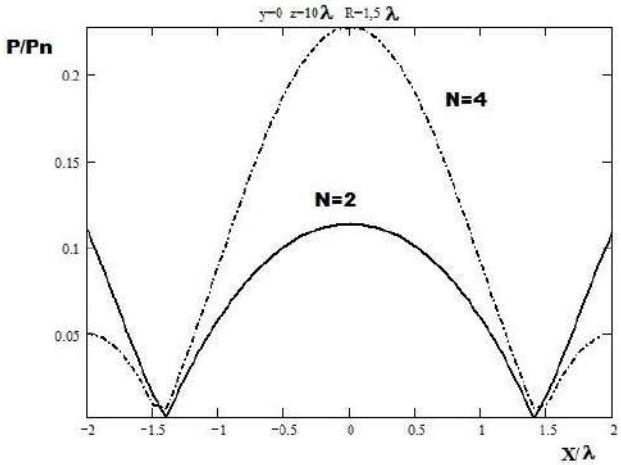


Рис. 7. Розподіл поля решітки з двох та чотирьох мікрофонів (на зовнішній дузі) вздовж осі X, Z=10λ, R=1,5λ

Аналіз розрахунків параметрів решітки з двосекційним розмішуванням мікрофонів

На рис. 8 представлено розподіл поля в двокільцевих еквідистантних гратах, змодельований за алгоритмом (1) – (8) складається з трьох мікрофонів ($R_{зовн.}$) на великій дузі та трьох на внутрішній (Rm – малої дуги). Вздовж лінії рівновіддаленої від координатних осей абсолютні значення сумарної амплітуди полів практично збігаються.

Аналіз інформації, наведеної на рис. 9 – 11, показує ефективність використання переваги розміщення мікрофонів у двосекційній решітці.

Рис. 9 і 11 аналогічні за розташуваннями мікрофонів на рис. 8 і 10, точка спостереження знаходиться на відстані Z = 11 довжин хвиль (у центрі), яка відповідає проміжній зоні (Френеля).

З порівняння рис. 8 і 9 видно, що в центрі решітки нормоване значення поля (потужності) буде великим (або рівним) при застосуванні всього 6 мікрофонів у порівнянні з 9 мікрофонами у точці головного максимуму на відстані 11λ . Графіки на рис. 10 і 11 також підкреслюють висновки з графіків на рис. 8 і 9, у всіх випадках абсолютне значення амплітуд поля нормоване на максимальне значення поля трьох випромінювачів, розташованих еквідістантно по радіусу, що дорівнює двом довжинам хвиль, по абсолютному значенню буде більше при меншій кількості мікрофонів, тобто на рис. 8 і 10.

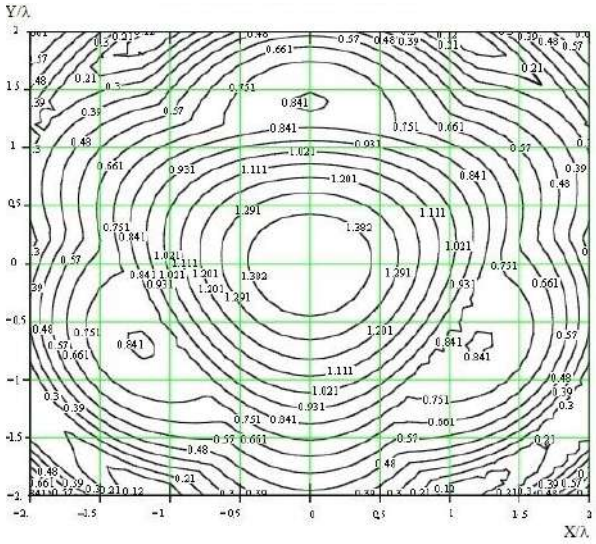


Рис. 8. Розподіл поля двосекційної акустичної решітки мікрофонів у вигляді контурів рівного значення N=6 мікрофонів (3 по малій дузі), Z=11λ, $R_{зовн.}$=2λ, $R_{малий}$=0,7λ

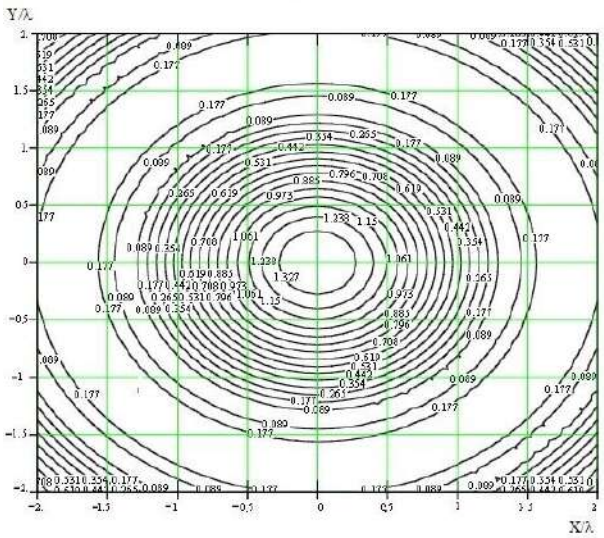


Рис. 9. Розподіл сумарного поля еквідистантної акустичної решітки N=9 мікрофонів, Z=11λ, $R_{зовн.}$ =2λ у виглядів контурів рівного значення

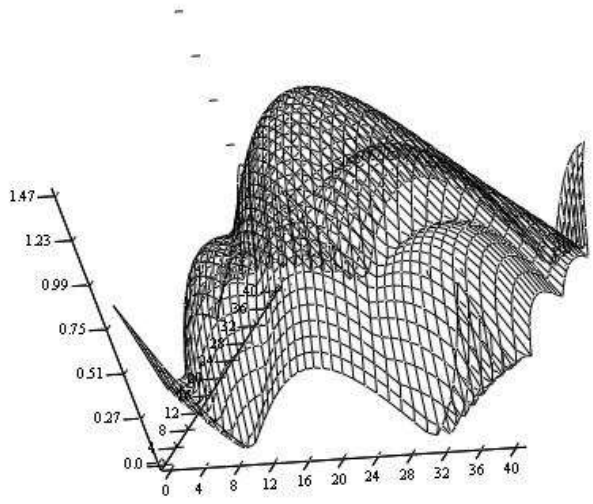


Рис. 10. Структура поля у вигляді поверхневого розподілу сумарного поля двосекційної акустичної решітки N=6 (3 по малій дузі), Z=11λ,$R_{зовн.}$=2λ; $R_{малий}$=0,7λ

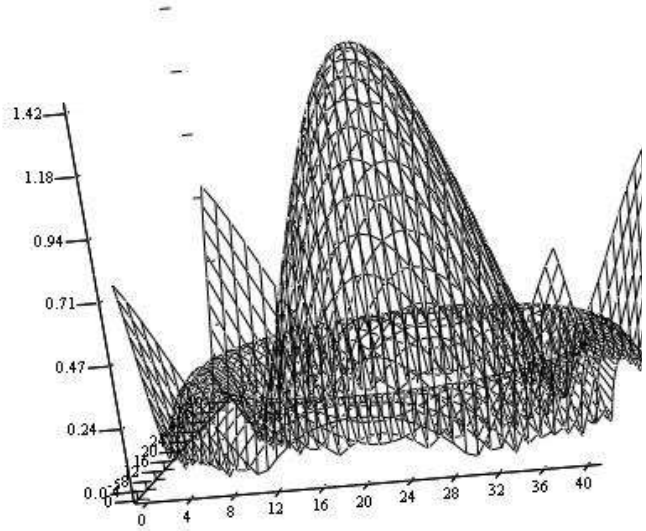


Рис. 11. Структура поля акустичних ґрат у вигляді поверхневого розподілу сумарного поля еквідистантної акустичної решітки N=9 мікрофонів , Z=11λ, $R_{зовн.}$=2λ

Висновки

Досліджено хвильові процеси випромінювання лінійних решіток акустичних випромінювачів на малих та проміжних відстанях.

Показано, що облік особливостей полів на відстанях, менших за довжину хвилі, та інтерференція акустичного поля, кількість випромінювачів, відстань між ними призводить до різного характеру рівномірності розподілу амплітуди акустичного поля. Продемонстровано, що збільшення числа випромінювачів призводить до більш рівномірного характеру зміни амплітуди поля в центрі решітки при фіксованому радіусі. Збільшення радіусу решітки при фіксованому числі призводить до появи інтерференційних максимумів поля. Показано

можливості керування концентрацією амплітуди акустичного поля всередині ґрат зміною її параметрів.

Показано, що на відстанях між межами проміжної та дальньої зони ($D^2/\lambda<Z<2D^2/\lambda$, D-зовнішній діаметр решітки) можливі появи локальних областей, у яких меншою кількістю мікрофонів можна забезпечити таке ж акустичне поле або навіть більше, ніж за більшої кількості мікрофонів. Цього можна досягти за умови використання внутрішньої дуги розташування мікрофонів, тоді можливе досягнення еквівалентного поля по осі решітки. Меншим числом мікрофонів, розташованих еквідистантно по зовнішньому радіусу, можна досягти еквівалентного поля. Варіація діаметру внутрішнього кільця, де розташовані мікрофони, також може сприяти максимальному розподілу потужності у центрі решітки при зменшеній загальній кількості мікрофонів при розміщенні у проміжній зоні джерел звуку.

Проведені дослідження можуть бути корисними також у рішенні задачі визначення розпізнавання конкретного джерела звуку конкретним мікрофоном решітки.

Список літератури:

1. Bolotina I.O., Kroening H.M., Kvasnikov K.G., Sednev D.A., Sumtsova O.V. Acoustic Field Simulation of an Antenna Array at Scanning by the SPA Method for Modern Ultrasonic Testing Technologies // J. Advanced Materials Research. 2014. Vol. 1040. P. 959–964.

2. Kartashov V.M., Kulia D.M., Kushnir M.V. and Tolstyh E.G. Selection of the Model for Varying Speed of Sound for the Optimal Linear Filter of Atmosphere Radio Acoustic Sounding Systems // Telecommunications and Radioengineering. 2014. Vol. 73, no. 91. P. 803–812.

3. BSWA Technology: product Catalogue – China, BSWA Technology Co., Ltd, 2008. Available http://www.bswa-tech.com.

4. Gorobets N.N., Gorobets Yu.N. and Tsekhmistro R.I. Near-Field Effects in the Electromagnetic Power Distribution in the Vicinity of Lattice of Hertzian Dipoles // Telecommunications and Radioengineering. 1999. Vol. 53, № 3. P. 24–29.

5. Lamonaca F., Carrozzini A., Grimaldi D. and Olivito R.S. Acoustic emission monitoring of damage concrete structures by multi-triggered acquisition system // Proceedings of IEEE International Instrumentation and Measurement Technology Conference (I2MTC), 13 – 16 May, 2012. P. 1630–1634.

6. Carnì D.L., Scuro C., Lamonaca F., Olivito R.S., & Grimaldi D. Damage analysis of concrete structures by means of b-value technique // International Journal of Computing. 2017. vol. 16(2). P. 82–88.

7. Omarov M., Tsekhmistro R., Shapovalov S. Analysis of Acoustic Field Distribution of Circular Microphone Array in Free Space // Proceedings – 16th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering.TCSET 2022. P. 134–138.

8. Цехмистро Р.И. Особенности излучения телекоммуникационных импедансных проволочных антенн // Радиотехника. 2004. № 139. С. 28–32.

Надійшла до редколегії 15.09.2023

Відомості про авторів:

Цехмістро Роман Іванович – канд. фіз.-мат. наук, Харківський національний університет радіоелектроніки, доцент кафедри медіаінженерії та інформаційних радіоелектронних систем; Україна; e-mail: roman.tsekhmistro@nure.ua; ORCID:https://orcid.org/0000-0003-3628-3658

Шаповалов Сергій Вікторович – канд. техн., наук, Харківський національний університет радіоелектроніки, доцент кафедри медіаінженерії та інформаційних радіоелектронних систем; Україна; e-mail: serhii.shapovalov@nure.ua; ORCID: https://orcid.org/ 0000-0003-0066-5291https://orcid.org/0000-0003-0066-5291

УДК 629.7.022 **DOI:10.30837/rt.2023.3.214.07**

В.М. КАРТАШОВ, д-р техн. наук, М.В. РИБНИКОВ

МЕТОДИ КОГЕРЕНТНОЇ ОБРОБКИ АКУСТИЧНИХ СИГНАЛІВ ДЛЯ ПЕЛЕНГУВАННЯ БПЛА

Вступ

Поточні події показують, наскільки серйозною загрозою є безпілотні літальні апарати (БПЛА), особливо дрони-камікадзе, які здатні вражати інфраструктурні об'єкти на досить великій відстані [1, 2]. Наявні засоби виявлення БПЛА є недостатньо ефективними, оскільки не дозволяють вчасно виявляти безпілотні літальні апарати, які мають малі розміри і виконують політ на малих висотах [3]. Актуальним науково-прикладним завданням є розробка нових і удосконалення існуючих методів і засобів виявлення та пеленгування БПЛА. Малі висоти польотів БПЛА змушують збільшувати кількість просторово розподілених каналів систем виявлення і пеленгування, відповідно до цього одна з вимог, що пред'являються до таких систем, це відносна дешевизна системи. Акустичний метод локації БПЛА здатен забезпечити достатню ефективність функціонування і є економічно доцільним рішенням; він може функціонувати як самостійно, так і доповнювати інші методи виявлення [4 – 6].

Енергія акустичних сигналів БПЛА розподілена в широкому діапазоні частот [7], тому при застосуванні акустичних решіток (АР) в станціях виявлення БПЛА потрібно використовувати широкосмугову обробку сигналів [5, 8]. В літературі описано два підходи до обробки широкосмугових сигналів при пеленгуванні об’єктів з використанням акустичних решіток, перший підхід – застосування вузькосмугової обробки для знаходження кута приходу сигналу на кожній з гармонік вхідного сигналу, після чого отримані результати підсумовуються. Такий підхід прийнято називати некогерентною обробкою [9], він розглянутий у [10]. Його перевагою є простота реалізації, а у якості одного з головних недоліків відзначається зниження ефективності визначення когерентних джерел сигналу і низька ефективність при малому відношенні сигнал шум (ВСШ) вхідного сигналу. Сигнали різних БПЛА можуть бути корельовані, коли у просторі знаходяться однакові типи БПЛА, а в разі, коли має місце недостатня роздільна здатність по частоті, сигнали і зовсім можуть бути когерентними. Тому при пеленгуванні великої кількості однотипних дронів ускладнюється їх поодиноке виявлення, що може становити велику загрозу, адже зараз ведуться активні розробки малих БПЛА, які працюють в групах (роях) [11].

Для підвищення ефективності визначення когерентних джерел випромінювання при некогерентній обробці можна застосувати методи прямого/зворотного просторового згладжування [12]. Однак такі алгоритми мають істотний недолік – результуюча кореляційна матриця буде меншою за вихідну, що, в свою чергу, зменшує кількість розрізнень поодиноких цілей [13]. Для обробки корельованих сигналів доцільно застосовувати інший підхід, при якому використовується когерентна обробка [14]. Перший когерентний алгоритм представлений в [15], він має назву алгоритму сигнального когерентного підпростору (CSSM). Суть цього алгоритму полягає в трансформуванні кореляційних матриць вхідного сигналу в універсальну кореляційну матрицю певної частоти, в результаті чого вже до універсальної кореляційної матриці можна застосувати один з вузькосмугових алгоритмів пеленгування, таких як MUSIC або Root MUSIC [16, 17].

В статті проаналізовано переваги і недоліки застосування когерентних алгоритмів обробки акустичних сигналів для пеленгації БПЛА з метою покращення роздільної кутової здатності по відношенню до однотипних БПЛА. Отримання якісних показників аналізованих

алгоритмів здійснювалося методом статистичного комп'ютерного моделювання в середовище Matlab.

Використання методів когерентної обробки акустичних сигналів для пеленгування БПЛА

В методах когерентної обробки з перетворенням кореляційних матриць вхідних сигналів в універсальну кореляційну матрицю певної частоти застосовується матриця трансформації, яка має діагональний вид

$$T_i = \begin{bmatrix} \frac{a(f_0,\theta_0)}{a_1(f_i,\theta_0)} & 0 & \dots & 0 \\ 0 & \frac{a(f_0,\theta_0)}{a_2(f_i,\theta_0)} & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & \frac{a(f_0,\theta_0)}{a_M(f_i,\theta_0)} \end{bmatrix}, \quad (1)$$

де f_i – частота в діапазоні $f_1 \dots f_L$; $a_m(f,\theta_0)$ – вектори керування у діапазоні $a_1(f,\theta_0) \dots a_M(f,\theta_0)$; M – загальна кількість елементів в акустичній решітці; θ_0 – передбачуваний кут приходу сигналу, який знаходять при попередній оцінці напрямку сигналу.

Вектори управління АР містять інформацію про кути приходу сигналу та мають вигляд

$$a(f,\theta_0) = \exp(-j2\pi f(n-1)d\sin\theta_0 / v), \quad (2)$$

де n – елемент акустичної решітки від 1 до M; d – відстань між елементами акустичної решітки; v – швидкість поширення сигналу.

Універсальну кореляційну матрицю сигналу $V_{f_0}(f_i)$ можна знайти? застосувавши матрицю трансформації до кореляційної матриці вхідного сигналу з наступним усередненням:

$$V_{f_0} = \sum_{i=1}^{L} T(f_i) V_{xx}(f_i) T^T(f_i), \quad (3)$$

де $()^T$ – операція транспонування; $V_{xx}(f_i)$ – кореляційна матриця вхідного сигналу, яка має вигляд

$$V_{xx}(f_i) = E[x_m(f_i) x_m(f_i)^T] = A(f_i) P_{ss}(f_i) A(f_i)^T + \sigma^2 I, \quad (4)$$

де $x_m(f_i)$ – сигнал частоти f_i на вході m-го елемента АР; $A(f_i)$ – вектор амплітудно-фазового розподілу сигналу; $P_{ss}(f_i)$ – кореляційна матриця сигналу на частоті f_i, σ^2 – дисперсія шуму; I – одинична матриця.

За допомогою універсальної кореляційної матриці когерентного сигнального простору $V_{f_0}(f_i)$ можна визначити справжній напрямок приходу широкосмугового сигналу, застосувавши вузькосмуговий метод високої роздільної здатності.

Алгоритм CSSM вимагає попередньої оцінки напряму надходження сигналу θ_0. Причому чим точніше буде попередня оцінка реального напряму, тим точніше буде результуюча оцінка кута приходу сигналу.

Як початкову оцінку зазвичай використовують оцінку класичних алгоритмів, таких як CAPONE, або алгоритмів, які не потребують попереднього використання пошукових алгоритмів, наприклад Root-MUSIC. Застосування безпошукових алгоритмів при формуванні

початкової оцінки і при знаходженні результуючої оцінки дозволяє отримати виграш за часом обробки в порівнянні з пошуковими алгоритмами високої роздільної здатності. Для зменшення часу обробки слід обмежити смугу частот при формуванні початкової оцінки, а у разі застосування алгоритму для пеленгації БПЛА слід використовувати частоти, які є основними тонами акустичного сигналу цього об'єкту.

Для порівняння точності визначення напрямку БПЛА різними методами будемо розраховувати середньоквадратичне відхилення (СКВ) знайденого кута джерела сигналу від істинного напряму, яке розраховується за формулою [18]

$$RMSE = \sqrt{E\left[\frac{1}{K}\sum_{j=1}^{J}\sum_{l=1}^{K}[(\hat{\theta}_j - \varphi_j)^2]\right]}, \quad (5)$$

де $j = (1...J)$ – кількість джерел випромінювання; $l = (1...K)$ – кількість випробувань при моделюванні; E – модуль числа.

На рис. 1 наведено просторові спектри, отримані з використанням алгоритму CSSM для двох сигналів БПЛА, що надходять з напрямів 25 і 28 град. Кількість елементів МР – 30, смуга пропускання 3000 – 4000 Гц, початкова оцінка напряму знаходилася за допомогою алгоритму MUSIC, в першому випадку відхилення початкової оцінки становить 1 град, у другому випадку – 3 град.

На рис. 2 представлений графік залежності СКВ від похибки кута початкової оцінки для алгоритму CSSM, кількість випробувань при моделюванні методом Монте-Карло складає К=500.

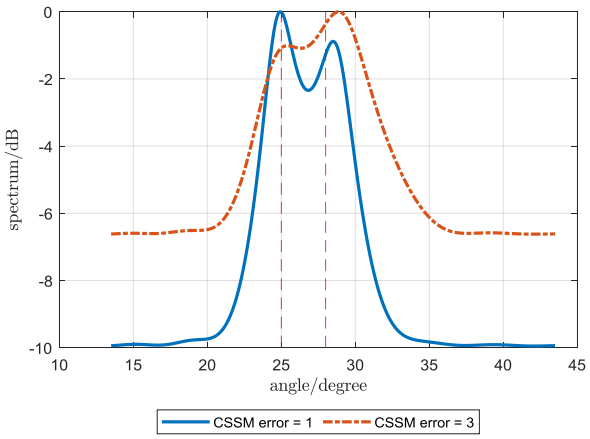


Рис. 1. Порівняння просторових спектрів, отриманих за допомогою алгоритму CSSM при похибках первинної оцінки 1 і 3 град

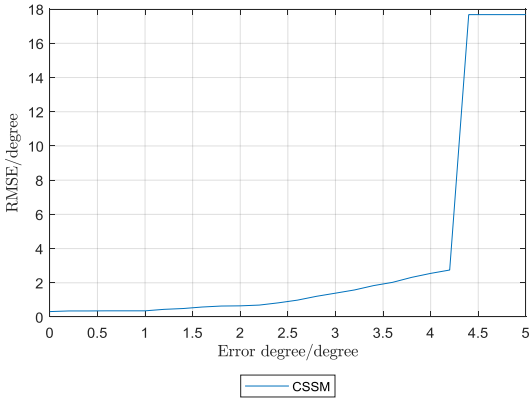


Рис. 2. Залежності СКВ оцінок алгоритму CSSM від похибки кута первинної оцінки

Зі спектрів, наведених на рис. 1, можна бачити, що спектр, отриманий при початковій похибці в 1 град, має більш глибокий провал між напрямами цілей і ця різниця становить приблизно 2 дБ. З рис 2. видно, що зі значення початкової похибки більше 4 град СКВ різко зростає, оскільки джерела сигналів в цьому випадку вже не розрізняються.

Оскільки похибка при початковій оцінці сильно впливає на підсумкову оцінку, то кореляційну обробку слід проводити за декілька ітерацій, де як початкова оцінка для другої ітерації обробки використовується результат попередньої обробки, такий підхід дозволяє поліпшити підсумкові результати кореляційної обробки.

На рис. 3 наведено просторові спектри, отримані з використанням алгоритму CSSM, для двох сигналів БПЛА, що надходять з напрямів 25 і 28 град, кількість елементів МР – 30, смуга пропускання 3000 – 4000 Гц, початкова оцінка напрямку знаходилася з використанням

алгоритму MUSIC. В першому випадку обробка проводиться один раз, в другому – два і в третьому – три рази. Похибка початкової оцінки дорівнює трьом градусам.

На рис. 4 представлений графік залежності СКВ від ВСШ для випадків, коли виконується одна, дві і три послідовні обробки одного сигналу БПЛА за допомогою алгоритму CSSM, кількість випробувань при моделюванні методом Монте-Карло складає К=500.

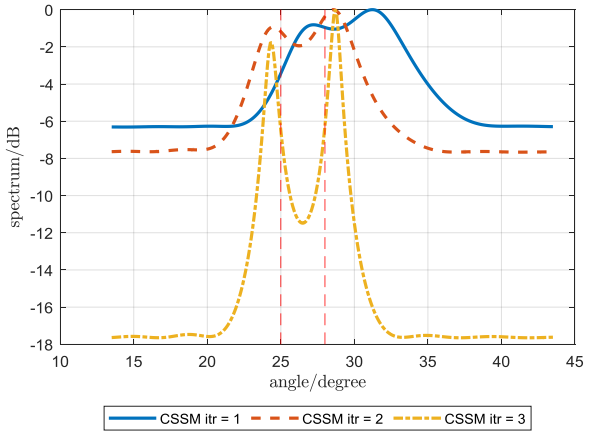


Рис. 3. Порівняння просторових спектрів сигналів БПЛА для одного, двух та трьох ітерацій послідовної обробки з використанням алгоритму CSSM

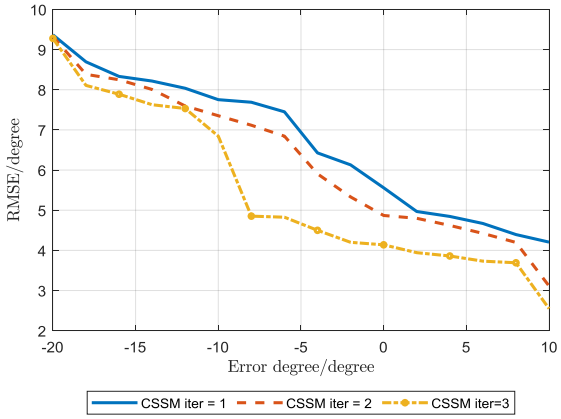


Рис. 4. Графики залежностей СКВ оцінок алгоритму CSSM від ВСШ для кількісті ітераций 1, 2 и 3

З рис. 3 можна бачити, що в першому випадку підсумкова оцінка має великі похибки у визначенні кутів, у другому – оцінки ближче до істинних значень напрямів, у третьому – провал між напрямами приходу сигналів значне більше, а точність їх визначення вище.

З рис. 4 випливає, що у третьому випадку спостерігається найменше відхилення оцінки від істинного значення кута у всьому діапазоні ВСШ.

На рис. 5 представлений графік залежності СКВ від ВСШ: у першому випадку для формування початкової оцінки використовується алгоритм IMUSIC, у другому – алгоритм IMUSIC-NAM, який є модифікованим IMUSIC і показує кращі результати при обробці всієї смуги частот [16], у третьому випадку використовується класичний алгоритм CAPONE і в останньому випадку використовується безпошуковий алгоритм ROOT-MUSIC. Кількість випробувань при моделюванні методом Монте-Карло – К=500.

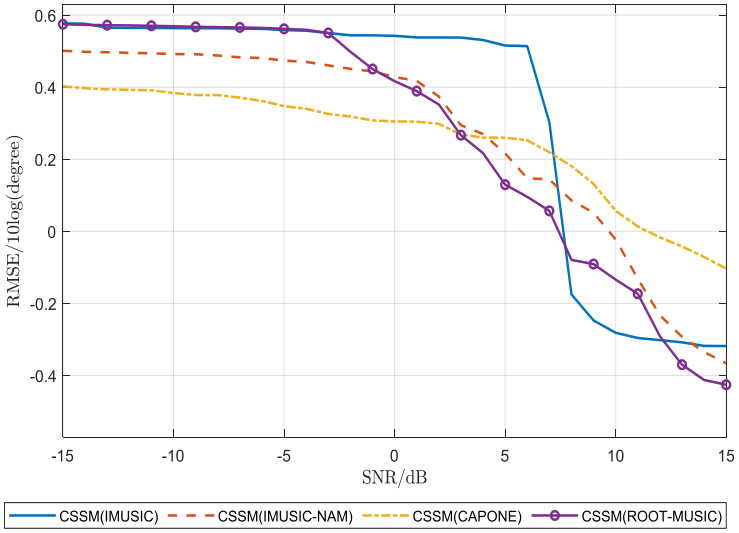


Рис. 5. Графики залежностей СКВ оцінок алгоритму CSSM від ВСШ при первинній обробці сигналу з використанням алгоритмів IMUSIC, IMUSIC-NAM, CAPONE, ROOT-MUSIC

Графіки рис. 5 показують, що в першому випадку підсумкова оцінка при формуванні початкової оцінки з використанням алгоритму IMUSIC має велику похибку в області низьких ВСШ, але значення похибки помітно покращується в області високого ВСШ. У третьому випадку для формування попередньої оцінки використовується класичний алгоритм CAPONE, в цьому випадку алгоритм CSSM показує меншу похибку при низькому відношенні сигнал-шум, проте він програє алгоритмам, які використовують розкладання за власними значеннями, в області високого ВСШ. При використанні алгоритму ROOT-MUSIC для формування початкової оцінки алгоритм CSSM показує найкращий результат в області середніх та високих значень ВСШ, крім цього алгоритм ROOT-MUSIC є безпошуковим, що дозволяє зменшити час обробки.

Алгоритм CSSM просторово перетворює як сигнали, так і шуми. Для отримання асимптотично ефективних оцінок можна використовувати власні вектори простору сигналу. Такий підхід застосовується в алгоритмі середньоквадратичного простору сигналу (WAVES). Алгоритм заснований на методі підбору зваженого простору [18]; так само як і алгоритм CSSM він використовує матриці трансформації, проте застосовуються вони до зважених векторів власних значень, що охоплюють сигнальний простір. Напрямки джерела сигналу за алгоритмом WAVES можна знайти, вирішивши задачу мінімізації виду:

$$\hat{\theta}_k = \arg\min \left\{ \sum_{i=1}^{L} \left| A(f_i,\theta) Y(f_i) - E_s(f_i) G(f_i) \right|^2 \right\}, \tag{6}$$

де $Y(f_i)$ – сигнал на виході елементів акустичної решітки на частоті f_i; $E_s(f_i)$ – матриця власних векторів, що охоплює сигнальний простір, $G(f_i)$ – вагова діагональна матриця, яка знаходиться за виразом

$$G(f_i) = \frac{e_k(f_i) - \sigma^2}{\sqrt{e_k(f_i)\sigma^2}}, \tag{7}$$

де $e_k(f_i)$ – власні значення, що охоплюють сигнальний простір, σ^2- дисперсія шумів, яка може бути знайдена як власні значення, що охоплюють шумовий простір e_n.

Алгоритм WAVES використовує нову матрицю $F(f_i)$ з рангом D, в якій матриця перетворення $T(f_i)$ застосовується до виваженої матриці власних значень і має вигляд

$$F(f_i) = [T(f_1)E_s(f_1)G(f_1),\ T(f_2)E_s(f_1)G(f_2)\ \ldots\ T(f_L)E_s(f_L)G(f_L)]. \tag{8}$$

Через шум ранг матриці буде повним, і після застосування алгоритму SVD – сингулярного розкладання до цієї матриці можуть бути отримані універсальні власні значення, що охоплюють простори сигналу і шуму:

$$SVD\{F(f_i)\} = [E_s\ E_n] = \begin{bmatrix} e_s & 0 \\ 0 & e_n \end{bmatrix}. \tag{9}$$

Матриця власних векторів шуму з формули (9) може бути використана вузькосмуговим надроздільним методом для знаходження кутів приходу сигналу. На рис. 5 зображено просторові спектри, отримані з використанням алгоритмів CSSM і WAVES для двох сигналів БПЛА, що надходять з напрямків 25 і 28 град. Кількість елементів МР – 30, смуга пропускання 3000 – 4000 Гц, відношення сигнал-шум 0 дБ.

На рис. 6 надано залежності СКВ оцінок алгоритмів IMUSIC, CSSM, WAVES від ВСШ в діапазоні від -20 до 10 дБ, для сигналів БПЛА з напрямків 25 і 28 град, кількість елементів МР – 36 , смуга пропускання 3000 – 4000Гц, кількість випробувань при моделюванні К=500.

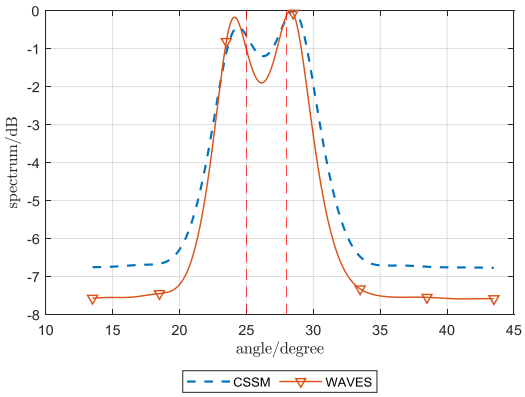


Рис. 5. Порівняння просторових спектрів, отриманих з використанням алгоритмів CSSM і WAVES для сигналів БПЛА з напрямів 25 і 28 град

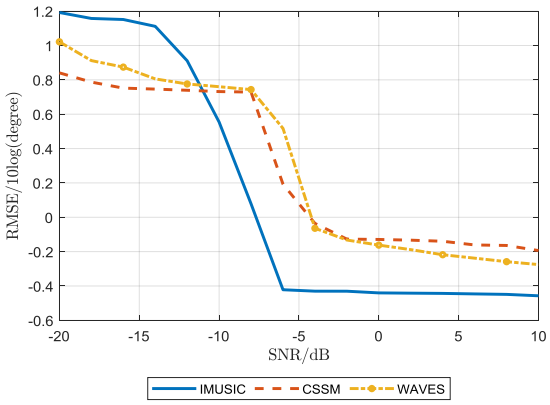


Рис. 6. Графики залежностей СКВ оцінок алгоритмів IMUSIC, CSSM, WAVES від ВСШ

З рис. 5 видно, що при оцінці напрямів надходження сигналів за допомогою алгоритму WAVES має місце суттєва можливість розрізнення сигналів від різних джерел випромінювання за рахунок глибшого провалу між напрямами сигналів. Це досягається за рахунок використання векторів власних значень сигналу замість кореляційних матриці.

На рис. 6 можна бачити, що в області високих ВСШ некогерентний алгоритм IMUSIC має менші значення СКВ порівняно з когерентними, в той час як при низьких ВСШ когерентні алгоритми CSSM та WAVES показують себе краще. В області високих ВСШ алгоритм WAVES показує кращі результати в порівнянні з CSSM, в той час як в області низьких ВСШ алгоритм CSSM краще WAVES.

Роздільна обробка сигналів БПЛА при значної їх кількості на вході системи пеленгування

Обробка значної кількості когерентних сигналів, що надходять від БПЛА, є досить складним завданням, причому зі збільшенням числа джерел сигналів якість оцінок визначення напрямів на БПЛА знижується. З метою збільшення ефективності визначення напрямів близько розташованих джерел сигналів може застосовуватися алгоритм CLEAN [19], суть якого полягає в послідовному видаленні найбільш сильних сигналів із даних, що спостерігаються.

Так сигнал, відфільтрований з деякого напряму, описується виразом

$$S(f_i,\theta_n)=[A(f_i,\theta_n)^T A(f_i,\theta_n)]^{-1}A(f_i,\theta_n)Y(f_i), \quad (10)$$

де $Y(f_i)$ – вектор вхідного сигналу.

Розділені за напрямами сигнали можна знайти наступним чином:

$$y_{i,n}=Y(f_i)-A(f_i,\theta_n)S(f_i,\theta_n). \quad (11)$$

Тоді кореляційна матриця розділеного векторного вхідного сигналу матиме вигляд

$$V(f_i,\theta_n)=E[y_{i,n}y_{i,n}{}^T], \quad (12)$$

а універсальна кореляційна матриця CSSM CLEAN набуде вигляду

$$V_{f_0} = \sum_{n=1}^{L}\sum_{i=1}^{N} T(f_i,\theta_n)V(f_i,\theta_n)T^T(f_i,\theta_n). \quad (13)$$

У разі поділу джерел випромінювання для алгоритму WAVES він набуває вигляду

$$F(\theta_n) = [T(f_1,\theta_n)E_s(f_1,\theta_n)G(f_1,\theta_n),\ T(f_2,\theta_n)E_s(f_1,\theta_n)G(f_2,\theta_n) \\ \dots\ T(f_L,\theta_N)E_s(f_L,\theta_N)G(f_L,\theta_N)] \quad (14)$$

Універсальні власні значення охоплюють простори сигналу і шуму для кожного джерела випромінювання і в порядку зростання їх можна знайти за виразом

$$U(\theta_n) = SVD\{F(\theta_n)\}. \quad (15)$$

Тоді власні значення, які охоплюють простір шуму, будуть відповідати найменшим власним значенням:

$$U_n(\theta_n) = (U_D(\theta_n),...,U_M(\theta_n)), \quad (16)$$

де D – кількість джерел сигналу.

Універсальна кореляційна матриця власних значень шуму матиме вигляд

$$R_{f0} = \sum_{n=1}^{L} U_u(\theta_n)U_u(\theta_n)^T. \quad (17)$$

На рис. 7 зображено просторові спектри, отримані за допомогою алгоритмів CSSM-CLEAN та WAVES-CLEAN для двох сигналів БПЛА, що надходять з напрямків 25 і 28 град, при відношенні сигнал шум 0 дБ. Кількість елементів АР – 30, смуга пропускання 3000 – 4000 Гц, початкову оцінку отримано з використанням некогерентного алгоритму IMUSIC.

На рис. 8 подано залежності СКВ оцінок напрямів алгоритмів CSSM-CLEAN, WAVES-CLEAN від ВСШ в діапазоні ВСШ від -20 до 10 дБ при впливі сигналів БПЛА з напрямів 25 і 28 град, при кількості елементів МР – 36, смузі пропускання 3000 – 4000 Гц, кількості випробувань при моделюванні К=500.

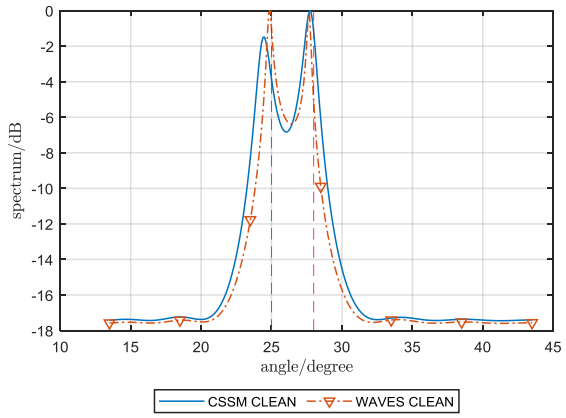


Рис. 7. Порівняння просторових спектрів, отриманих з використанням алгоритмів CSSM-CLEAN и WAVES-CLEAN, для сигналів БПЛА з напрямів 25 и 28 град

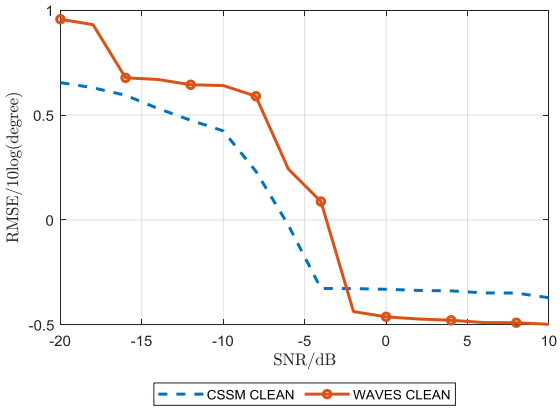


Рис. 8. Графики залежностей СКВ оцінок алгоритмів CSSM-CLEAN, WAVES-CLEAN від ВСШ

Відповідно до рис. 7 алгоритм WAVES-CLEAN дає більш точні оцінки напрямів джерел випромінювання у порівнянні з алгоритмом CSSM-CLEAN.

Як бачимо з рис. 8, в області високих ВСШ алгоритм WAVES-CLEAN має менші значення СКВ, в той час як при низьких ВСШ алгоритм CSSM-CLEAN показують кращі результати.

Висновки

Ефективне виявлення, спостереження і пеленгування великих груп малих БПЛА за акустичним сигналом потребує високої роздільної здатності по кутовим координатам від алгоритмів обробки сигналів, що використовуються. Надроздільні алгоритми забезпечують високу роздільну здатність для некорельованих сигналів, але втрачають свою ефективність при пеленгуванні однотипних БПЛА, сигнали яких мають певну ступінь кореляції. В когерентних алгоритмах застосовується фокусування і перетворення кореляційних матриць вхідного сигналу для отримання єдиної універсальної матриці коваріації, яка відповідає широкосмуговому вхідному сигналу. Це дозволяє не тільки розрізняти джерела випромінювання когерентних сигналів, але і більш ефективно працювати при низькому відношенні сигнал-шум.

Проте алгоритми когерентної обробки сигналів мають деякі недоліки, один з основних – це необхідність формування попередніх оцінок напрямів надходження сигналів, від точності яких значною мірою залежатиме точність результуючої оцінки. Для збільшення точності результуючої оцінки когерентну обробку слід виконувати кілька разів, причому результат попередньої обробки використовується як попередня оцінка для наступної обробки, і чим ближче початкова оцінка до істинної, тим менше буде потрібна кількість ітерацій для точного визначення напрямку джерел сигналу. Недоліком когерентних алгоритмів є також висока чутливість до помилок, наприклад, наявність помилок визначення напрямку на окремих частотах може сильно позначатися на результаті підсумкової оцінки. Тому в процесі обробки потрібно відокремлювати частотні компоненти, що мають низьке відношення сигнал-шум. Ще однією проблемою є зниження ефективності алгоритмів при збільшенні числа джерел сигналу. В статті показано, що поділ джерел сигналів і обробка їх окремо збільшує точність визначення напрямів, проте це також збільшує обчислювальну складність алгоритму.

За результатами моделювання показано, що когерентні алгоритми ефективніше працюють в області низького ВСШ, тоді як деякі алгоритми краще показують себе в області високого ВСШ. Застосування безпошукових методів для формування попередньої та результуючої оцінок напрямку сигналу, дозволяють отримати виграш за часом обробки порівняно з некогерентними надроздільними алгоритмами. WAVES показує кращі результати в області високого відношення сигнал-шум, проте в області низького відношення сигнал-шум програє методу CSSM. Метод WAVES більш обчислювально витратний порівняно з методом CSSM, оскільки використовує матрицю власних векторів замість кореляційної матриці сигналу.

Таким чином, застосування алгоритмів когерентної обробки сигналів може покращити результати виявлення та пеленгації великої кількості однотипних БПЛА. Подальші зусилля щодо вдосконалення когерентних алгоритмів слід спрямувати на розробку безпошукового алгоритму обробки та на зменшення впливу помилок попередніх оцінок на результуючу оцінку напрямів джерел випромінювання акустичних сигналів.

Список літератури:

1. Królikowski, Hubert. (2022). The Use of Unmanned Aerial Vehicles in Contemporary Armed Conflicts – Selected Issues. Politeja. 19. 10.12797/Politeja.19.2022.79.02.

2. Adam Lowther, Mahbube K.S. Combat Drones in Ukraine // Air & Space Operations Review 2022 / Vol. 1, No. 4, WINTER 2022

3. Карташов В. М., Олейников В. Н., Шейко С. А., Бабкин С. И., Корытцев И. В., Зубков О. В. Особенности обнаружения и распознавания малых беспилотных летательных аппаратов // Радиотехника. 2018. Вып. 195. С. 235–243.

4. Олейников В.Н., Зубков О.В, Карташов В.М., Корытцев И.В., Бабкин С.И., Шейко С.А, Селезнев И.С. Экспериментальная оценка эффективности аглоритмов пеленгования беспилотных летательных аппаратов по акустическому излучению // Радиотехника. 2019. Вып. 199. С. 29–37.

5. Карташов В.М., Корытцев И.В, Олейников В.Н., Зубков О.В., Корытцев И.В., Бабкин С.И., Шейко С.А., Селезнев И.С. Алгоритмы пеленгации беспилотных летательных аппаратов по их акустическому излучению // Радиотехника. 2019. Вып. 196. С. 22–31.

6. Карташов В.М., Олейников В.Н., Воронин В.В., Рябуха В.П., Капуста А.И., Рыбников Н.В., Селезнев И.С. Методы комплексной обработки и интерпретации радиолокационных, акустических, оптических и инфракрасных сигналов беспилотных летательных аппаратов // Радиотехника. 2020. Вып. 202. С. 173–182.

7. Kartashov V., Oleynikov V., Koryttsev I., Sheiko S., Zubkov O., Babkin S. Processing of Wide Band Acoustic Signals During Detection of Unmanned Aerial Vehicles // 2020. IEEE Ukrainian Microwave Week (UkrMW). Kharkiv, Ukraine, September 21 – 25. Vol. 1 on 2020 IEEE 12th International Conference on Antenna Theory and Techniques (ICATT). P. 35–39.

8. Oleynikov V.N., Kartashov V.M., Babkin S. I., Zubkov O.V., Korytsev I.V., Sheiko S.A., Seleznov I.S. Structure and Parameter Unmanned Aerial Vehicles Sound Fields // Telecommunications and Radio Engineering. 2020. Vol. 79, №17. P.1539–1550.

9. Kartashov V.M., Oleynikov V.N, Zubkov O.V., Korytsev I.V., Babkin S. I., Sheiko S.A. Kolendovskaya M.M. Spatial-temporal Processing of acoustic Signals of Unmanned Aerial Vehicles // Telecommunications and Radio Engineering. 2020. Vol. 79, №9. P. 769–780.

10. T. Engin Tuncer, Benjamin Friedlander / Classical and Modern Direction-of-Arrival Estimation, 2009.

11. Mitch Campion, Prakash Ranganathan, and Saleh Faruque. 2018. UAV swarm communication and control architectures: a review // Journal of Unmanned Vehicle Systems. 7(2): 93–106. https://doi.org/10.1139/juvs-2018-0009

12. Карташов В.М. Рибников М.В., Карташов О.В., Посошенко В.О. Аналіз методів акустичної пеленгації безпілотних літальних апаратів // Радіотехніка. 2022. Вип. 210. С. 104–112.

13. Pillai S. U. and Kwon B. H. Forward/backward spatial smoothing techniques for coherent signal identification // IEEE Transactions on Acoustics, Speech, and Signal Processing. 1989. Vol. 37, no. 1. P. 8–15, Jan., doi: 10.1109/29.17496.

14. Wang H., Kaveh M. Coherent signal-subspace processing for the detection and estimation of angles of arrival of multiple wide-band sources // IEEE Trans. Acoust., Speech, Signal Process. 1985. Vol. 33, No. 4. P. 823–831.

15. Schmidt R. Multiple emitter location and signal parameter estimation // IEEE Trans. Antennas Propag. 1986. Vol. 34, No. 3. P. 276–280,

16. Wong K. T. and Zoltowski M. D. Uni-vector-sensor ESPRIT for multisource azimuth, elevation, and polarization estimation // IEEE Transactions on Antennas and Propagation. 1997. Vol. 45, No. 10. P. 1467–1474, Oct., doi: 10.1109/8.633852.

17. Wang Ben, Wang Wei, Gu Yujie, Lei Shujie. Underdetermined DOA Estimation of Quasi-Stationary Signals Using a Partly-Calibrated Array // Sensors. 2017, 17, 702.

18. E. D. di Claudio, R. Parisi. WAVES: Weighted average of signal subspaces for robust wideband direction finding // IEEE Trans. Signal Process. 2001. Vol. 49, No. 10. P.2179–2191.

19. Clark B. G. An efficient implementation of the algorithm 'CLEAN // Astronomy and Astrophysics. 1980. 89: 377.

Надійшла до редколегії 25.09.2023

Відомості про авторів:

Карташов Володимир Михайлович – д-р техн. наук, професор, Харківський національний університет радіоелектроніки, завідувач кафедри медіаінженерії та інформаційних радіоелектронних систем, Україна; email: volodymyr.kartashov@nure.ua; ORCID: https://orcid.org/0000-0001-8335-5373

Рибников Микола Володимирович – Харківський національний університет радіоелектроніки, аспірант кафедри медіаінженерії та інформаційних радіоелектронних систем, Україна; email: mykola.rybnykov@nure.ua; ORCID: https://orcid.org/0000-0003-1340-8788

APPLICATION OF RADIO TECHNOLOGY METHODS
ЗАСТОСУВАННЯ МЕТОДІВ РАДІОТЕХНІКИ

УДК 615.472.03 **DOI:10.30837/rt.2023.3.214.08**

В.В. СЕМЕНЕЦЬ, д-р техн. наук, В.І. ЛЕОНІДОВ, канд. техн. наук

ВИКОРИСТАННЯ МІКРОКОНТРОЛЕРА STM32F407VG ДЛЯ ДОСЛІДЖЕННЯ АМПЛІТУДНО-ЧАСТОТНИХ ХАРАКТЕРИСТИК БІОЛОГІЧНИХ ТКАНИН

Вступ

Фізичні методи діагностики [1 – 6] функціонального стану біологічних тканин (електротермометрія, колірна та інфрачервона термографія, капілярна фотометрія, а також ультразвукові методи та лазерна доплерівська флуометрія) у разі термічних, механічних та вогнепальних пошкоджень або в результаті здавлювання малоефективні, через різний ступінь ураження тканини не дають можливості визначити стан кожного м'яза окремо.

Тому до теперішнього часу жоден із перелічених вище методів не знайшов широкого застосування у практиці оперативної оцінки життєздатності (здатності біологічної тканини до самовідновлення) ушкоджених областей м'яких тканин. У той же час добре відомо, що при лікуванні уражень або при трансплантації тканин однією з найважливіших умов успішного проведення операції є якомога раніше визначення меж некротичних уражень. Проте надійних, широкодоступних і оперативних інструментальних методів оцінки ступеня життєздатності тканин нині досі не розроблено.

Розвиток методів імпедансометрії є важливою складовою досліджень при вирішенні задачі формалізації діагностики ступеня життєздатності уражених ділянок біотканин. Використання як критерій оцінки стану біотканини фізичної величини – імпедансу замість описів, що містять, як правило, деяку частку довільності, дозволяє підвищити достовірність діагнозу і, отже, підвищити ймовірність правильного вибору тактики лікувальних дій щодо відновлення області ураження біотканини [7 – 10].

Значимість імпедансометрії в області діагностики стану біотканин випливає з відомого положення, сформульованого в [7], згідно з яким модуль $|Z_{БТ}|$ імпедансу нежиттєздатної тканини відносно малий і не залежить від частоти $f_{изм}$ струму, що використовується для вимірювання імпедансу ураженої ділянки біотканини. Для повністю життєздатної (неураженої) біотканини модуль імпедансу помітно залежить від частоти $|Z_{БТ}| = F(f_{изм})$ і у області відносно низьких частот значно перевищує ті самі значення, отримані для нежиттєздатних тканин. Приклад такої залежності, наведений у [8], показано на рис. 1.

Рис.1. Залежність імпедансу біотканини від частоти

Розвитком цього положення є, згідно з [7], запровадження коефіцієнта життєздатності:

$$k_j = \frac{|Z_{f2}|}{|Z_{f1}|},\ при\ f_2 >> f_1, \quad (1)$$

при цьому біотканина вважається життєздатною, якщо виконується нерівність $k_j > 1$, і нежиттєздатною – якщо виконується альтернативна нерівність $k_j \le 1$.

У виразі (1) значення частот суворо не визначено, і, отже, критерій (1) не може гарантувати сувору визначеність рішення.

Очевидно, що критерій (1) дає невизначеність рішення про стан біотканини в області зі значеннями $K_f = 1 \pm \xi$, де ξ – мала величина, величина значення якої також є невизначеним. У загальному випадку область може бути великою і, отже, виникає необхідність опису відмінностей у стані біотканини при різних значеннях критерія у цій області, де імовірно можливе формування декількох підобластей, які відповідають відомому чи виявленому у процесі експериментальних досліджень набору детермінованих станів біотканини.

Область рішень також може включати суттєві відмінності у стані біотканини.

Крім того, невизначеність в інтерпретацію величини вносять значні флуктуації величини імпедансу при повторенні дослідів навіть для схожих або однотипних тканин і випадків ураження.

Тканини в залежності від умов ураження та часу, що минув з моменту ураження, можуть містити різний об'єм рідкої фракції (електроліту), що суттєво впливає на абсолютне значення імпедансу досліджуваної області біотканини. Ці обставини призводять до труднощів однозначного визначення граничних значень абсолютної величини імпедансу для уражених і неуражених ділянок біотканини (як для біотканин різного типу, так для різного типу та ступеня ураження).

Отже, використання лише одного параметра, саме величини абсолютного значення імпедансу, не є оптимальним підходом для забезпечення надійної діагностики стану ураженої біотканини. Для розвитку діагностичних можливостей методів імпедансометрії необхідно розширити область параметрів, що вимірюються, для чого необхідно дослідити розподіли імпедансу в частотній і часовій областях з метою виявлення оптимального підходу до підвищення діагностичних можливостей методу імпедансометрії.

Наведені вище положення нині не формалізовані. Це означає, що немає правил, що дозволяють визначити ступінь ураження на підставі вимірювання та аналізу функції $|Z_{БТ}| = F(f_{изм})$. Також відсутні стандартизовані критерії використання величин f_1 і f_2. У свою чергу, у ряді робіт [7, 9, 10] визнаються високі діагностичні можливості методів імпедансометрії, включаючи аналіз як уражених ділянок тканини, так і неуражених. Слід також зазначити, що інформація у вигляді функції $|Z_{БТ}| = F(f_{изм})$ дозволяє створити і вдосконалити власне систему класифікації ступеня ураження тканини щодо величини k_j.

З викладеного випливає, що побудова систем, що дозволяють вимірювати та аналізувати частотні залежності імпедансу біотканин в реальному часі, є актуальним завданням.

Мета роботи – аналіз одного з підходів до побудови системи вимірювання коефіцієнта життєздатності з використанням мікропроцесорних систем на базі мікроконтролера STM32F407VG.

Основні положення

Для вимірювання амплітудно-частотних характеристик (АЧХ) біологічних тканин використовувалася вимірювальна схема, яка наведена на рис. 2. Методика вимірювань передбачала використання випробувальних синусоїдальних сигналів, які складають частотний ряд у діапазоні $D_{F=}[20\ Гц \ldots 2{,}0\ мГц]$.

Ефективне значення напруги, яке подавалося на зразок тканини (резистор R2) через струмообмежуючий резистор R1, становило $U_{эф} = 1{,}5B \pm 5\%$. Величина струму через зразок підтримувалася постійною під час проведення експериментів і при величині опору резистора $R1 = 20кОм$ не перевищувала значення $I_{\max} \le 0{,}7 \cdot 10^{-6} A$, помилка встановлення струму через зразок не перевищувала $\delta I = \pm 5\%$. В дослідженні було зручно використовувати аналіз залежностей модуля напруги на об'єкті. Такий метод значно спрощував процедуру вимірювань та апаратну частину експериментів.

Розміри досліджуваної області обмежені електродами голкового типу, відстань між голками $\Delta l = 10мм$, глибина занурення $\delta h = 2мм$.

В якості досліджуваних об'єктів використовувалися кілька видів рослинної біологічної тканини: яблуко, морква, буряк, картопля, пагони алое.

Завданням дослідження було визначення граничних значень області зміни розподілу напруги на біологічній тканині в залежності від частоти при відомих вихідних параметрах випробувальних сигналів. При цьому висувалась наступна робоча гіпотеза.

Модуль імпедансу біологічної тканини визначається співвідношенням обсягу живих клітин, що володіють властивістю поляризації та обсягом міжклітинної рідини, яка є розчином електроліту. Якщо вважати, що це співвідношення для непошкодженої біологічної тканини апріорі відомо, то в результаті пошкодження в міжклітинний простір додатково надходить внутрішньоклітинна рідина (теж електроліт), при цьому в процесі поляризації братиме участь вже менша кількість клітин і, отже, модуль повного електричного опору має зменшуватись.

Неважко припустити, що нижнім граничним значенням модуля імпедансу ураженої біологічної тканини буде опір тканинного електроліту в припущенні, що клітинна структура повністю зруйнована.

Також неважко припустити, що провідність тканинного електроліту різна для різних типів тканин. Тому як критерій щодо відносної оцінки ступеня ураження клітинної структури біологічної тканини слід прийняти АЧХ деякого «стандартного» електроліту. В якості такого еталону, як показника граничного ураження тканини, доцільно прийняти дисперсійну залежність імпедансу ізотонічного розчину солі $NaCl$ (фізіологічного розчину), при цьому вважатимемо, що в міру збільшення тяжкості ураження АЧХ біологічної тканини наближається до АЧХ ізотонічного розчину. Цей критерій, можливо, буде цілком справедливий у разі рослинних біологічних тканин, але ми його застосовуємо у зв'язку з тим, що кінцевою метою досліджень у цій галузі знань є створення системи інформативних ознак для класифікації стану життєздатності біологічних тканин тваринного походження.

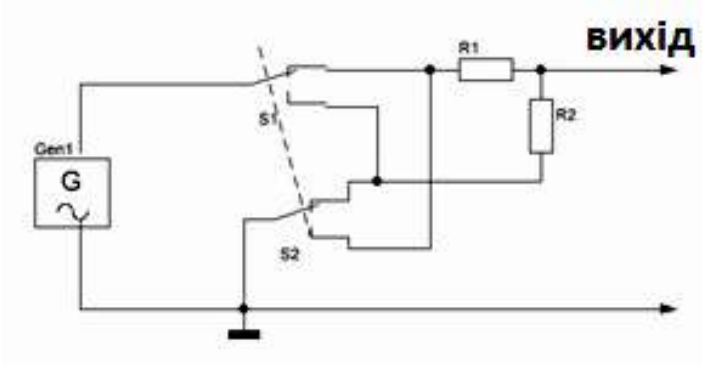


Рис. 2. Схема вимірів

Експериментальні дослідження дають необхідні вихідні дані для розробки вимірювального пристрою та алгоритму його функціонування.

У відповідність до розробленого алгоритму програмна частина пристрою працює у режимі моніторингу. Після старту програми відбувається ініціалізація портів вводу-виводу

інформації, підключення стандартних бібліотек, які забезпечують роботу ЖК індикатору та інтерфейсу USB [11 – 15]. Аналогові входи мікроконтролера підключені до схеми виміру (рис. 2). Аналогові сигнали перетворюються в цифрові за допомогою АЦП. Значення змінних виводяться на ЖК індикатор (рис. 3) і відправляються або в комп'ютер, або флешку для обробки і прийняття рішення (рис. 5).

Існує бібліотека, яка є вільним програмним забезпеченням і може вільно розповсюджуватися та змінюватись. Бібліотека доволі вдала, як на нас, і має великий спектр функцій, щоб задовольнити будь-які потреби, у відтворені інформації на дисплей типу WH1602 (WH1604) з контролером HD44780. Ця бібліотека створювалась спочатку як кросплатформа для AVR, PIC, ARM. Але на мікроконтролерах STM32F1xx і STM32F4xx працює. В мережі можна зустріти різні варіації цієї бібліотеки, але набір функцій один і той самий.

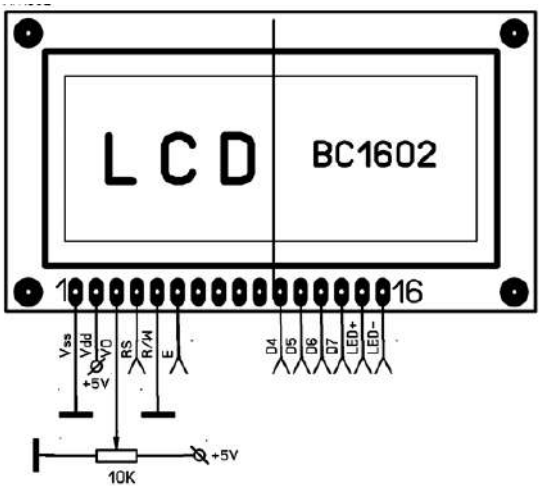


Рис. 3 Схема підключення LCDWH1602

Схема підключення дисплею представлена на рис. 3. Підключати будемо по чотирьохпровідниковій схемі з заземленим сигналом W/R. Це означає, що нам потрібно під'єднати до мікроконтролера шість дротів від дисплея, такі як D4, D5, D6, D7, E, RS. До яких саме виводів мікроконтролеру під'єднувати дисплей, це вже вирішувати вам самим. Бібліотека допускає підключення кожного виводу дисплея на різні порти і будь-які піни обраного/обраних порту/портів. Під'єднайте до дисплею живлення, це ніжка 2 – "+5 Вольт". Загальний мінус на ніжки дисплею 1 та 5. Та до ніжки дисплею під номером 3 резистивний дільник з підстроєчним резистором 10к для регулювання контрасту інформації, яка висвічується на екрані. Якщо ваш дисплей має підсвічування екрану, то можна ще подати живлення на підсвічування, це 15 і 16 ніжки дисплею. Живлення подати напряму, або через транзисторний ключ, який керується з ніжки мікроконтролеру. Тоді підсвічування можна вмикати та вимикати програмно, або навіть регулювати яскравість підсвічування, налаштувавши ніжку, яка керує ключем підсвічування, як PWM (ШИМ).

Щоб бібліотека працювала правильно, потрібно всім ніжкам, з якими буде з'єднано мікроконтролер та дисплей WH1602, дати назви (псевдоніми) за принципом:

- Enable (E) – LCD_E
- RS – LCD_RS
- D4 – LCD_D4
- D5 – LCD_D5
- D6 – LCD_D6
- D7 – LCD_D7

Обираєте зручні для вас або вільні виводи мікроконтролеру. Виставляєте їх в режим "GPIO_Output" та називаєте за принципом, як зазначено вище. Приклад на рис. 4. Червоними зонами позначено потрібне для підключення LCD:

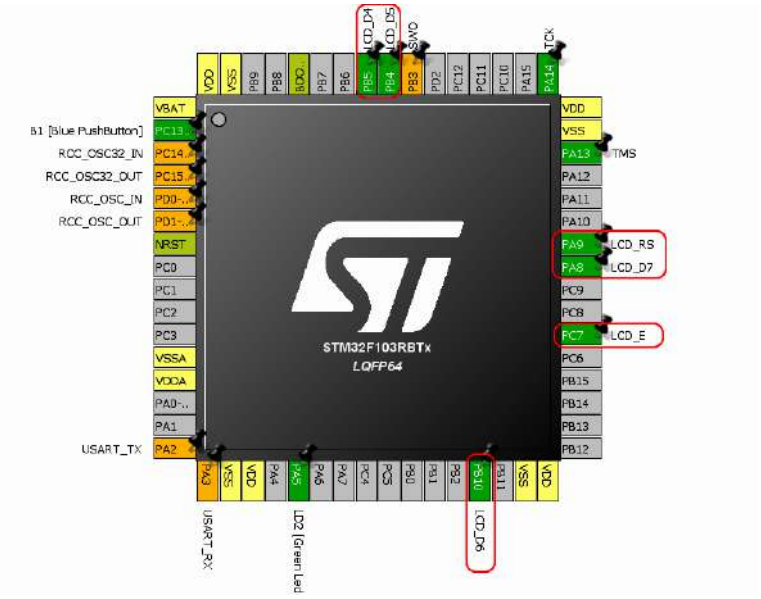


Рис. 4. Оголошення назв і режиму виводів для підключення LCD в STM32CubeIDE

Підключаємо бібліотеку до проєкту:

1. Завантажте архів бібліотеки "hd44780.zip" собі на диск. В архіві знаходиться тека "hd44780" з підтеками "inc" та "src".

2. Копіюємо файли бібліотеки до проєкту. Можна скопіювати самі файли бібліотеки до проєкту. Заголовні файли "h" у теку "inc" проєкту, а сирцеві файли "c" – до теки "src" проєкту.

Тепер, коли на рівні файлів все під'єднано як слід, треба в коді додати лиш один рядок в головний файл "main.c":

/* USER CODE BEGIN Includes */

#include "hd44780.h"

/* USER CODE END Includes */

Оце і все. Можна компілювати проєкт для перевірки. Якщо зроблено все правильно, то компілятор скомпілює проєкт без помилок.

Бібліотека для своєї роботи і зручності користувача має ряд функцій. Внутрішні функції розглядати не будемо, а розглянемо ті функції, що потрібні нам для виводу на дисплеї різноманітної інформації.

Список функцій бібліотеки:

- **lcdInit** – функція початкової ініціалізації дисплею;
- **lcdClrScr** – функція очищення дисплею, курсор в початкове положення;
- **lcdReturn** – функція повернення курсору в початкове положення;
- **lcdSetMode** – функція встановлення режимів: дисплей увімк/вимк, курсор блимає увімк/вимк, курсор увімк/вимк;
- **lcdGoto** – функція встановлює курсор в певне місце: рядок, стовпець;
- **lcdPuts** – функція виводу текстового рядка;
- **lcdPutc** – функція виводу окремого символу типу char;
- **lcdLoadChar** – функція завантаження до пам'яті дисплею користувацького символу;
- **lcdDrawChar** – функція малювання на дисплеї користувацького символу;
- **lcdBackSpace** – функція зміщення курсору на один символ ліворуч і його знищення;
- **lcdScroll** – функція зміщення всього тексту на один стовпець в потрібному напрямку (ліворуч або праворуч);
- **cursorShift** – функція зміщення курсору на позицію праворуч чи ліворуч без знищення символу, що вже зображений. Призначена для редагування/виправлення тексту;
- **lcdItos** – функція виводу на екран числа типу integer;

- **lcdFtos** – функція виводу на екран числа типу float;
- **lcdNtos** – функція виводу на екран числа типу integer з певним числом розрядів. Зайві розряди відсікаються. Розряди, яких не вистачає, заповнюються нулями;
- **lcdDrawBar** – функція малювання індикатору виконання;
- **lcdClrBar** – функція очищення індикатору виконання.

Рис. 5. Робочий макет передачі даних по USB

Результати експериментальних спостережень та їх аналіз

На рис. 6 наведено залежності частотного розподілу напруги на досліджуваній ділянці живої біологічної тканини рослинного походження. На рис. 6 прийнято такі позначення: 1 – яблуко, 2 – ізотонічний розчин, 3 – картопля, 4 – картопля молода, 5 – буряк, 6 – морква, 7 – алое.

Аналіз залежностей на рис. 6 показує, що у разі дослідження живої клітинної структури форма АЧХ зразка біологічної тканини має важливу відмінність від форми АЧХ ізотонічного розчину.

На АЧХ біологічної тканини можна виділити чотири характерні ділянки.

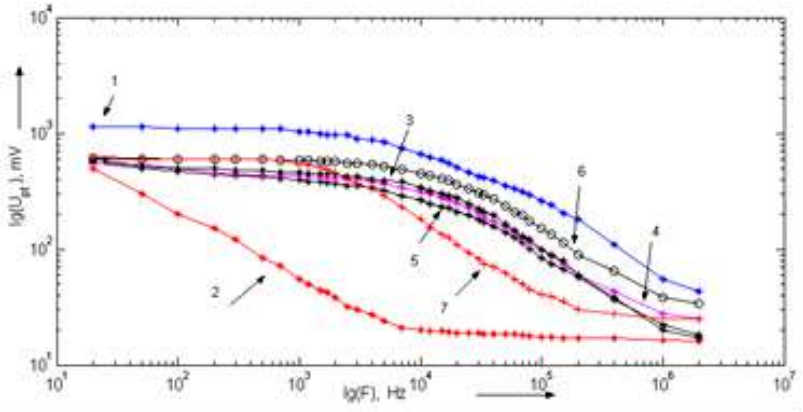


Рис. 6. АЧХ неушкодженої клітинної тканини

Перша ділянка – це відносно повільно спадаючий сигнал при позитивній кривизні в області частот $\Delta F_1 = [20; \ldots 1000]\ Гц$.

Друга ділянка в прийнятому логарифмічному масштабі наближається до лінійного виду в діапазоні частот $\Delta F_2 = [1{,}0;\ 100]\ кГц$. На третій ділянці спостерігається спад сигналу з

негативною кривизною. Ця ділянка для всіх зразків має малий діапазон частот: $\Delta F_3 = [100;\ 200]\ кГц$ для алое та $\Delta F_3 \cong 1000\ кГц$ – для інших типів досліджуваних тканин.

На четвертій ділянці сигнал майже не залежить від частоти в області частот $\Delta F_4 > 1\ мГц$

У прийнятих координатах частотна залежність для ізотонічного розчину явно відрізняється від АЧХ живої біологічної тканини. На цій залежності (крива 2 на рис. 6) спостерігаються дві ділянки, що явно розрізняються. На першій ділянці у діапазоні частот $\Delta F_{1fz} \cong [20; \ldots 7000]\ Гц$ спостерігається близьке до лінійного зменшення сигналу. На частотах $\Delta F_{2fz} > 7000\ кГц$ величина сигналу майже не залежить від частоти.

З аналізу випливає припущення про те, що при певному проміжному ступені ураження біологічної тканини АЧХ сигналу також набуватиме деяку проміжну форму між кривою 2 і, наприклад, кривою 1. Для перевірки цієї гіпотези були виміряні АЧХ біологічних тканин, які зазнали заморожування різного ступеня з наступним повільним нагріванням до кімнатної температури. Графічне зображення отриманих АЧХ наведено на рис. 7.

Аналіз залежностей рис. 7 підтверджує висунуту гіпотезу про наближення форми АЧХ до АЧХ ізотонічного розчину зі збільшенням тяжкості ураження. У цьому експерименті зразки рослинної біологічної тканини заморожувалися шляхом витримки в морозильній камері холодильника. Крива 1 є АЧХ біологічної тканини яблука, яка знаходилася в морозильній камері протягом 15 хв з наступним нагріванням в кімнатних умовах. Залежність 2 отримана на яблучній тканині після витримки в морозильній камері протягом 30 хв. Криві 3 і 5 представляють АЧХ, отримані на картоплі та яблуку після їх витримки в морозильній камері протягом 2 год. Залежність 4 є АЧХ ізотонічного розчину.

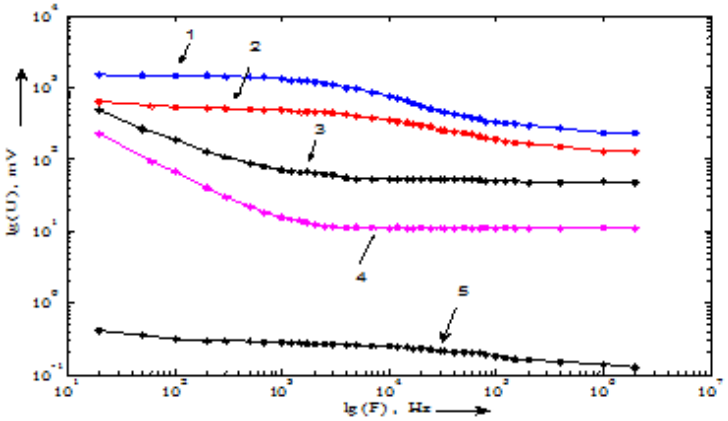


Рис. 7. АЧХ пошкодженої клітинної тканини

Отримані результати наочно демонструють явно виражене наближення форми залежності до залежності, отриманої для ізотонічного розчину.

Також видно відмінність після сильного заморожування яблучної тканини, внаслідок чого відбулося повне руйнування клітинної структури та вимірювання проводилися по суті на рідкій фракції, що представляє суміш міжклітинного та внутрішньоклітинного електролітів. Видно, що модуль імпедансу яблучного електроліту значно менший, ніж для ізотонічного розчину. Це явище можна пояснити значною відмінністю хімічного складу і, мабуть, різницею в щільності розчинів. Для біологічних тканин тваринного походження це явище спостерігатися не буде.

Отриманий результат показує, що форма АЧХ може бути інформативною ознакою об'ємного вмісту здорових клітин у досліджуваному об’ємі біологічної тканини і, отже, може бути ознакою її життєздатності.

Висновки

Основним результатом роботи є обґрунтування інформативності методу частотного аналізу імпедансу біологічних тканин для діагностики їх здатності до самовідновлення після отриманих пошкоджень.

У роботі визначено граничні значення частот сигналів, що забезпечують надійний вимір коефіцієнта життєздатності, а також граничні значення величин імпедансів на прикладі аналізу електричних властивостей клітинної структури рослинної біотканини при її неушкодженому стані. Запропоновано та розглянуто варіант реалізації автоматизованої системи збору даних імпедансометрії біотканин на базі мікроконтролера STM32F407VG.

Наступні роботи в галузі розвитку наукового напрямку імпедансометрії біотканин, будуть спрямовані на проведення досліджень з розробки та створення експериментального зразку прибору, побудованого на принципі вимірювання та аналізу сигналів перехідного процесу, що виникає в біологічній тканині при подачі на неї імпульсу мікроструму (при якому реалізується аналіз сигналів у часовій області замість аналізу частотної області).

Список літератури:

1. Bharara M., Cobb J. E., Claremont D.J. Thermography and thermometry in the assessment of diabetic neuropathic foot: a case for furthering the role of thermal techniquest // Low Extrem Wounds. 2006. № 5:4. P. 250–260.
2. Isogai N. Application of medical thermography to the diagnosis of Freys syndrome // Head Neck. 1997. №19: 2. P.143–147.
3. Sidler M., Jackowski C., Dimhofer R. et al. Use of multislice computed tomography in disaster victim identification – advantages and limitations // Forensic Sei Int. 2007. №169. P. 2–3; 118–128.
4. Dellegrottaglie S., Sanz J., Macaluso F. et al. Technology Insight: magnetic resonance angiography for the evaluation of patients with peripheral artery disease // Nat Clin Pract Cardiovasc Med. 2002. № 4: 12. P. 677–687.
5. Лежнев К.К. Сравнительная оценка методов определения жизнеспособности мягких тканей при огнестрельных повреждениях : автореф. дис. ... канд. мед. наук. 1990. 19 с.
6. Thomasset A. Bio-electrical properties of tissue impedance measurements // Lyon Med. 1962. № 207. P. 107–118.
7. Bykh A.V., Kozin Yu.I., Leonidov, V.I., Kravtsov A.V., Bobnev R.A. Development of the systems for frequency impedancemetry of biotissues using the @Arduino@ platforms // Telecommunications and Radio Engineering. 2019. 78(1). P. 71–78. DOI: 10.1615/ TelecomRadEng, v78.i1.80,
8. Кравцов О.В., Леонідов В.І., Козін Ю.І., Бобнєв Р.О. Пристрій для визначення життєздатності біологічних тканин. Патент на корисну модель №133519, номер заявки u2018 11007; подана 07.11.2018, дата 10.04.2019, дата публікації 10.04.2019. Бюл. №7.
9. Kosin U. I., Leonidov V. I., Kravtsov A. V., Bobnev R. A. Device for measurement of biological tissue characteristics // TelecomRadEng.v76.i13.50. P. 1173–1179. DOI**:** 10.1615.
10. Бойко В.В., Кравцов А.В., Леонідов В.І., Бобнєв Р.А., Ісаєв Ю.І., Козін Ю.І., Курбанов Т.А. Оцінка життєздатності обпалених тканин методом імпедансометрії // Харківська хірургічна школа. 2018. №3.
11. 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.
12. Семенець В.В., Леонідов В.І. Дослідження амплітудно-частотних характеристик біологічних тканин // Радіотехніка. 2020. Вип. 203. С. 186 В.І. 190. DOI: 10.30837/rt.2020.4.203.20
13. Семенець В.В., Леонідов В.І. Аналіз частотно-часової структури акустичних шумів малих автоматичних аеросистем // Радіотехніка. 2020. Вип. 202. С. 147–152. DOI:10.30837/rt.2020.3.202.15
14. Аврунін О.Г., Запорожець О.В., Носова Т.В., Семенець В.В. Мікропроцесори в інформаційно-вимірювальних системах : навч. посібник. Харків : ХНУРЕ, 2015. 180 с. http://openarchive.nure.ua/handle/document/5291
15. 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

Надійшла до редколегії 17.09.2023

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

Леонідов Володимир Іванович – канд. техн. наук, Харківський національний університет радіоелектроніки, с. н. с. кафедри біомедичної інженерії, Україна; e-mail: volodymyr.leonidov@nure.ua; ORCID: https://orcid.org/0000-0001-5218-3177

RADAR AND RADIONAVIGATION
РАДІОЛОКАЦІЯ І РАДІОНАВІГАЦІЯ

УДК 621.396. 967.2 **DOI:10.30837/rt.2023.3.214.09**

І.В. СВИД, канд. техн. наук, І.І. ОБОД, д-р техн. наук,
С.В. ГОЛОВАТЕНКО, С.В. ДАЦЬКО

ОЦІНКА ЯКОСТІ ВИЗНАЧЕННЯ КООРДИНАТ ПОВІТРЯНИХ ОБ'ЄКТІВ КООПЕРАТИВНИМИ РАДІОЛОКАЦІЙНИМИ СИСТЕМАМИ СПОСТЕРЕЖЕННЯ ПОВІТРЯНОГО ПРОСТОРУ

Вступ

Можна зазначити, що в інформаційному забезпеченні системи контролю повітряного простору і управлінні повітряним рухом велике місце займають кооперативні системи спостереження повітряного простору [1 – 3], до яких належать багатопозиційні радіолокаційні системи [4 – 7], запитальні системи вторинної радіолокації [8 – 12] та системи радіолокаційної ідентифікації за ознакою «свій-чужий» [13 – 17]. Головним завданням зазначених кооперативних систем спостереження повітряного простору є оцінка координат виявлених повітряних об'єктів (ПО) [18 – 20], а також отримання радіолокаційної інформації від ПО та оцінка державної приналежності виявленого ПО [21 – 23]. При цьому слід зазначити, що системи радіолокаційної ідентифікації вирішують завдання ідентифікації виявленого ПО, як на користь визначення ступеня небезпеки виявленого ПО, так і при безпосередньому застосуванні зброї [24 – 27]. Основним елементом, який суттєвим чином знижує якість інформаційного забезпечення кооперативних системам спостереження, є літаковий відповідач [28 – 31]. Ця обставина зумовлена принципом побудови останнього у вигляді відкритої одноканальної системи масового обслуговування з відмовами [32 – 34], що дозволяє зацікавленій стороні, як отримувати дані від літакового відповідача, що розглядається, так і повністю паралізувати останній постановкою навмисної корельованої завади необхідної інтенсивності [35 – 38]. Наявність просторової багатоканальності прийому сигналів запиту значно розширює структурні можливості при проведенні оптимізації обробки сигнальної інформації у літакових відповідачах, зокрема у варіантах об'єднання попередніх рішень просторових каналів обробки сигналів запиту [39 – 42]. Слід зазначити, що кооперативна обробка радіолокаційної інформації в багатопозиційних радіолокаторах дозволяє отримати потенційно більший обсяг інформації [43 – 47].

Метою запропонованої роботи є оцінка якості визначення координат повітряних об'єктів кооперативними радіолокаційними системами спостереження повітряного простору.

Класифікація систем радіолокаційного спостереження повітряного простору

Зазначимо, що всі перспективні системи радіолокаційного спостереження повітряного простору, що використовуються в даний час, позначені Комітетом з майбутніх аеронавігаційних систем терміном Surveillance System, поділяються на два основні типи:

- системи залежного спостереження;
- системи незалежного спостереження.

Слід зазначити, що радіолокаційні системи спостереження повітряного простору використовуються органами управління повітряним рухом для визначення місцезнаходження ПО. [28, 48 – 51]. Існує два типи радіолокаційних систем спостереження: кооперативні та некооперативні [52 – 56].

Кооперативні системи: в рамках цієї форми спостереження наземні системи (наприклад, вторинний радіолокатор) обмінюються даними з обладнанням (наприклад, літаковими відповідачами) на борту ПО для визначення розташування та інших характеристик ПО. Інформа-

ція про ПО, яка може включати місце розташування від супутникової системи визначення місцеположення або інших засобів, визначається на борту і потім передається до управління повітряним рухом у відповідь на запит. Інші спільні системи, такі, як ADS-B, налаштовані так, що ПО передають своє місцезнаходження та іншу інформацію без запиту із землі.

Некооперативні системи: при цій формі спостереження наземні системи (такі як первинний радіолокатор) можуть визначити місцезнаходження ПО та вимірювати його положення із землі, передаючи імпульси радіохвиль, що відбиваються від корпусу ПО.

Таким чином, основою служби радіолокаційного спостереження повітряного простору, що надається користувачам, як системи контролю повітряного простору, так і управління повітряного руху може служити сукупність трьох основних видів радіолокаційного спостереження повітряного простору (рис. 1) [56 – 59].

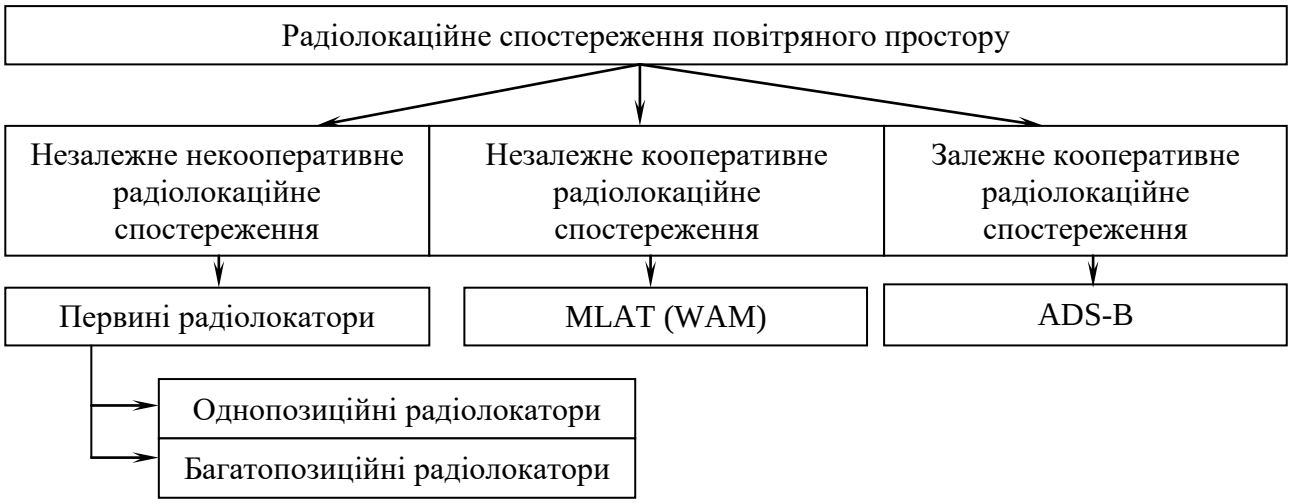


Рис. 1. Класифікація радіолокаційного спостереження повітряного простору

У незалежних некооперативних радіолокаційних спостереженнях повітряного простору розташування ПО визначається на основі інформації вимірювань без допомоги ПО, що розглядається, що можливе шляхом використання первинних радіолокаційних систем.

Первинні радіолокаційні системи є основним джерелом радіолокаційної інформації про динамічну повітряну обстановку в певній області повітряного простору. Вони призначені для виявлення ПО та визначення координат ПО. Первинні радіолокатори проводять опромінення всіх об'єктів, що потрапляють у межі їхньої зони огляду, та здійснюють прийом сигналів, відбитих цими об'єктами. Аналіз прийнятих сигналів дозволяє отримувати всю необхідну інформацію про рух ПО. Принцип функціонування первинних радіолокаторів аналогічний принципу функціонування звичайної імпульсної радіолокаційної станції, хоча і має деякі специфічні особливості, зумовлені вимогами, властивостями об'єктів, що спостерігаються, і умовами застосування.

Використання первинних радіолокаторів для спостереження повітряної обстановки не вимагає ніякого додаткового устаткування на борту ПО, тобто, така система радіолокаційного спостереження є повністю незалежною. За допомогою первинних радіолокаторів визначаються, як правило, дві координати ПО: похила дальність та азимут. На жаль, третю координату – барометричну висоту ПО – визначити за допомогою первинного радіолокатора складно. Не визначається також інша додаткова польотна інформація, така як індивідуальний номер літака, залишок палива, вектор шляхової швидкості, особливі випадки в польоті й т.п.

Основними недоліками радіолокаційних систем спостереження, що функціонують на базі первинних радіолокаторів, є:

- низька інформативність, пов'язана з відсутністю можливості отримання додаткової польотної інформації;

- велике споживання енергії;

- високий рівень завад, пов'язаний з відбиттями сигналів від місцевих предметів;

- обмеження зони огляду, що визначаються конфігурацією діаграми спрямованості антени у вертикальній площині та необхідністю виконання умови прямої видимості між радіолокатором та ПО.

У зв'язку із зазначеними вище недоліками, а також із розширенням використання сучасних систем спостереження застосування первинних радіолокаторів для огляду повітряного простору поступово скорочується.

Для незалежного кооперативного радіолокаційного спостереження розташування ПО визначається на основі інформації вимірювань, що виконуються підсистемою локального радіолокаційного спостереження з використанням повідомлень з борту ПО. Ці повідомлення можуть містити інформацію, отриману на борту ПО. Цей модуль забезпечує можливість розширення еквівалентного радіолокаційного обслуговування управління повітряного руху на основі двох технологій спостереження, які можуть використовуватись окремо або спільно MLAT [6, 7] та WAM [8, 10]. Ці технології є альтернативою класичному радіолокаційному обслуговуванню, проте для них характерні менші витрати на впровадження та технічне обслуговування, що дозволяє здійснювати радіолокаційне спостереження в тих районах, де в даний час воно не забезпечується з причин географічного або економічного характеру. Крім того, за певних умов ці технології дають змогу скоротити мінімуми ешелонування, що в перспективі розширить можливості обслуговування великих обсягів повітряного руху.

MLAT є технологією, яка забезпечує незалежне кооперативне радіолокаційне спостереження. Розгортання цієї системи сприяє використанню можливостей бортового обладнання режиму S, що забезпечує передачу автоматичних повідомлень. В цьому випадку сигнал, що передається ПО, приймається мережею приймачів, розташованих у різних місцях. Використання різниці в часі отримання сигналів різними приймачами дозволяє незалежно визначати розташування джерела сигналів. Теоретично ця технологія може бути пасивною, яка використовує інформацію, що передається ПО, або активною, що ініціює відповіді аналогічно запитам у режимі S вторинних оглядових радіолокаторів.

Спочатку системи MLAT встановлювалися у великих аеропортах для реалізації спостереження за ПО на поверхні. В даний час ця технологія використовується для ведення спостереження у великих районах (система MLAT із широкою зоною дії WAM [8, 10]). Однак слід зазначити, що у порівнянні з ADS-B для системи MLAT необхідна наявність більшої кількості наземних систем та надійної зв'язаної мережі; крім того, порівняно з ADS-B для цієї системи характерні жорсткіші вимоги до геометрії, проте використання існуючого бортового обладнання режиму A/C забезпечує можливість впровадження цієї системи.

Залежне радіолокаційне спостереження (ADS-B) є перспективною технологією спостереження повітряного простору, що забезпечує можливість радіомовної передачі бортовим електронним обладнанням розпізнавального індексу ПО, інформації про місцезнаходження, висоту, швидкість та іншу інформацію. У порівнянні зі звичайним вторинним оглядовим радіолокатором інформація, що передається в режимі радіомовлення, про місце розташування ПО є більш точною, оскільки, як правило, вона заснована на інформації, що отримується від глобальної навігаційної супутникової системи, та її передача здійснюється не менше одного разу на секунду. Характерна для GPS точність позиціонування та висока швидкість оновлення інформації дозволять постачальникам обслуговування та користувачам підвищити рівень безпеки польотів, пропускну спроможність та ефективність.

Слід зазначити, що ADS-B залежить від наявності джерела, що забезпечує необхідну точність позиціонування, яким нині є глобальна навігаційна супутникова система визначення місцеположення [60 – 63].

Використання залежного спостереження сприяє підвищенню ефективності роботи пошуково-рятувальних служб, що надаються мережею спостереження. У районах без радіолокаційного обслуговування забезпечувана ADS-B точність позиціонування та швидкість

оновлення інформації дозволяють більш ефективно відстежувати траєкторію польоту, що забезпечує можливість своєчасного визначення втрати контакту та оперативного вжиття пошуково-рятувальних служб заходів щодо точного визначення відповідного розташування [64 – 67].

При використанні залежного кооперативного радіолокаційного спостереження місцеположення визначається на борту ПО, і ця інформація передається підсистемі локального спостереження поряд із можливими додатковими даними (наприклад, розпізнавальний індекс ПО, барометрична висота тощо).

Слід зазначити, що кооперативність прийому як відбитих, так і випромінювальних радіолокаційних сигналів є у тому, що це приймальні позиції здатні приймати відбиті сигнали від ПО, опромінених будь-якою передавальною позицією. Тобто, по суті необхідно знайти таку процедуру обробки координатної інформації в мережі радіолокаційних систем спостереження, яка при реалізації кооперативної обробки дозволила б підвищити точність вимірювань дальності, при врахуванні спільної обробки всіх фізично реалізованих незалежних вимірювань похилих дальностей, сумарних дальностей та різниці відстаней [68 – 70].

Також слід звернути увагу на те, що кооперативність обробки радіолокаційної інформації в багатопозиційних радіолокаторах полягає в тому, що всі позиції системи здатні приймати відбиті сигнали від ПО у зоні відповідальності при їх опроміненні будь-якою позицією, що передає, а також і сигнали за даними каналу радіотехнічної розвідки, коли сам ПО є джерелом радіовипромінювання. Така процедура суттєво збільшує обсяг сигнальної і координатної інформації та дозволяє отримати надмірні виміри сумарних дальностей та різниць відстаней, в яких міститься інформація про похилу дальність до ПО. Під надмірністю будемо розуміти вимірювання кількох однорідних фізичних величин (дальностей до ПО, сумарних дальностей та різниць відстаней), які пов'язані між собою будь-яким законом, при якому шукане значення величини (дальності до ПО) одержують шляхом обробки результатів проміжних вимірювань за рівнянням надлишкових вимірів з метою підвищення точності оцінювання.

Крім того слід зазначити, що первинний оглядовий радіолокатор визначає місце розташування ПО на основі прийому відбитих радіолокаційних сигналів, а вторинний радіолокатор використовується для передачі та прийому одержуваної на борту ПО інформації, такої як барометрична висота, розпізнавальний індекс тощо [71 – 73].

Зазначимо, що підвищення достовірності радіолокаційної інформації досягається за рахунок усунення хибних вимірів в багатопозиційній радіолокаційній системі шляхом використання багатопозиційних методів визначення координат ПО, а не за рахунок введення додаткових позицій. Використання багатопозиційних методів визначення координат ПО передбачає значне зменшення імовірності виникнення хибних вимірів без збільшення кількості приймальних позицій.

Крім усього підвищення достовірності радіолокаційної інформації, за рахунок використання кооперативного прийому відбитих сигналів в умовах багатоцільової обстановки, забезпечує зменшення імовірності виникнення хибних вимірів без використання додаткових приймально-передавальних позицій. Усунення хибних вимірів здійснюється за рахунок надмірності вимірів та використання критерію "k із n". При цьому слід зазначити, що надмірність вимірів забезпечується реалізацією сумарно-далекомірного методу без збільшення кількості приймально-передавальних позицій. Так, для випадку трьох позицій імовірність виникнення хибних вимірів в два рази вище при наявності в зоні огляду шести ПО. При розробці перспективних оглядових маловисотних автоматичних радіолокаторів з електронним скануванням та використанням цифрових активних антенних решіток доцільно передбачити режими синхронізації апаратури просторово рознесених радіолокаторів для утворення багатопозиційних радіолокаторів з кооперативним прийомом з метою підвищення живучості, завадозахищеності та підвищення якості радіолокаційної інформації.

Доцільно знайти таку процедуру обробки координатної інформації в системі радіолокаційних систем, яка при реалізації кооперативної обробки інформації дозволить підвищити

точність вимірювань дальності, при врахуванні спільної обробки всіх фізично реалізованих незалежних вимірювань похилих дальностей, сумарних дальностей та різниці відстаней.

Вторинні оглядові радіолокатори можуть бути віднесені до засобів незалежного спостереження лише умовно, оскільки координатна інформація у них дійсно визначається незалежно від бортових навігаційних систем, а додаткова польотна інформація (індивідуальний номер ПО, барометрична висота і в деяких режимах залишок палива, вектор дорожньої швидкості тощо) генерується бортовими технічними засобами, а тому для передачі відповідних повідомлень використовується літаковий відповідач, який виконує роль активного ретранслятора за лініями зв'язку "земля – борт" і "борт – земля".

Загальними перевагами вторинних радіолокаторів у порівнянні з первинними, незалежно від класу та типу радіолокаторів, є:

- підвищена, порівняно з первинними радіолокаторами, інформаційна здатність, що дозволяє автоматично ідентифікувати об'єкти спостереження та здійснювати управління повітряного руху за чотирма координатами: похилою дальністю, азимутом, висотою та часом;
- велика інструментальна дальність дії за малих енергетичних витрат;
- малий рівень завад, що викликаються відбиттям сигналів від місцевих предметів та метеоутворень;
- малий рівень випромінюваної потужності.

При цьому слід зазначити, що загальними недоліками радіолокаційних систем спостереження, що ґрунтуються на використанні вторинних радіолокаторів, є:

- необхідність оснащення всіх ПО літаковими відповідачами;
- необхідність введення в апаратуру запитувачів та відповідачів систем подавлення сигналів бічних пелюсток діаграми спрямованості антени за запитом та відповіддю;
- високий рівень внутрісистемних завад;
- можливість несанкціонованого використання літакових відповідачів як для отримання інформації, так і для паралізації літакових відповідачів постановкою внутрісистемних завад потрібної інтенсивності.

У вторинних радіолокаторах роздільна здатність і точність за азимутом гірше, ніж у первинних радіолокаторів, бо принцип дії вторинного радіолокатора заснований на обробці пакету сигналів відповіді. Це призводить до значних труднощів при поділі сигналів та декодуванні сигналів відповідей відповідачів ПО, розташованих на близьких відстанях один щодо одного і приблизно на однакових пеленгах. Для підвищення азимутальної точності таких радіолокаторів за однієї і тієї ж ширини діаграми спрямованості антени необхідно збільшувати кількість імпульсів у пакеті, тобто, збільшувати частоту запитів, що автоматично призводить до значного збільшення внутрішньосистемних завад. Компромісним вирішенням цього протиріччя є використання моноімпульсного способу прийому та обробки повідомлень відповіді, а радикальним рішенням задачі – усунення внутрішньосистемних завад та збільшення інформаційної здатності за рахунок застосування моноімпульсних дискретно-адресних вторинних радіолокаторів, що працюють у режимі S.

Завдяки підвищеним, у порівнянні з первинними радіолокаторами, інформаційним можливостям, вторинні радіолокатори в даний час відносяться до основних засобів спостереження за повітряною обстановкою. Відповідно до концепції розвитку систем CNS/ATM вторинні радіолокатори і надалі залишатимуться основним засобом спостереження повітряного простору, але їх параметри зазнають значних змін.

Оцінка якості виміру координат повітряних об'єктів синхронною мережею кооперативних радіолокаційних систем спостереження повітряного простору

Розглянемо можливість та доцільність кооперативної обробки координатної інформації в багатопозиційній системі спостереження повітряного простору при її організації на пункті обробки радіолокаційної інформації. Кооперативність прийому відбитих сигналів і випромі-

нюваних сигналів відповіді полягає у тому, що приймальні позиції здатні приймати відбиті сигнали від ПО, опромінених будь-якою з передаючих позицій, що випромінюють сигнали [56, 74].

По суті потрібно знайти таку процедуру обробки координатної радіолокаційної інформації в системі з N радіолокаційних станцій, яка при реалізації кооперативної обробки дозволить підвищити точність вимірювань дальності з врахуванням спільної обробки всіх фізично реалізованих незалежних вимірювань похилих дальностей, сумарних дальностей та різниці відстаней. Реалізація зазначених процедур випромінювання та прийому при відповідному частотному розносі на позиціях незалежних приймально-підсилювальних трактів та каскадів гетеродинування дозволяє проводити вимірювання дальностей, їх сум та різниць відстаней незалежно [56, 74]. Так, при деякому розмірі бази

$$L = R\lambda / 4l_{po},$$

де R – відстань до ПО; l_{po} – найбільший розмір ПО, приймальні пункти приймають відбиті від ПО сигнали за різними пелюстками діаграми зворотного вторинного випромінювання. Ці сигнали незалежні та некорельовані.

Кооперативність обробки радіолокаційної інформації полягає в тому, що всі позиції зазначеної інформаційної системи здатні приймати відбиті сигнали від ПО у зоні відповідальності при їх опроміненні будь-якою передавальною позицією, а також і сигнали за даними каналу радіотехнічної розвідки, коли сам ПО є джерелом радіовипромінювання. Така процедура суттєво збільшує обсяг сигнальної та координатної інформації та дозволяє отримати надмірні виміри сумарних дальностей та різниць відстаней, у яких міститься інформація про похилі дальності до ПО. Під надмірністю розуміється вимірювання кількох однорідних фізичних величин (дальностей до ПО, сумарних дальностей та різниць відстаней), які пов'язані між собою яким-небудь законом, при якому шукане значення величини (дальності до ПО) отримують шляхом обробки результатів проміжних вимірювань за рівнянням надлишкових вимірювань з метою підвищення точності оцінювання.

Перехід до синхронної мережі радіолокаційних систем спостереження [56, 74] дозволяє здійснити кооперативне приймання сигналів та розподілену обробку радіолокаційної інформації. Одночасне вимірювання дальності до ПО, що спостерігається в мережі радіолокаційних систем спостереження, дозволяє вимірювати висоту польоту повітряного об’єкту, що значно покращує інформаційне забезпечення користувачів. При цьому слід зазначити, що геометрія інформаційної мережі при вимірі висоти польоту ПО, тобто геометричний фактор, має вплив на результуючу точність вимірювань. Розглянемо геометричний фактор при вимірі висоти польоту ПО за даними виміру похилої дальності.

Будемо розглядати синхронну мережу радіолокаційних систем, що складається з n приймальних пунктів. Для первинної системи спостереження це буде n наземних приймальних пунктів (приймальним пунктом), один із яких випромінюючий, а для вторинної системи спостереження – це $n-1$ наземних приймальних пунктів і один випромінюючий відповідач ПО. З викладеного видно, що обидві задачі ідентичні. На кожному приймальному пункті здійснюється обробка сигналів відповіді та передача отриманої інформації на пункт сумісної обробки даних, на якому, як правило, розміщується запитувач. Між пунктом обробки радіолокаційної інформації та кожним приймальним пунктом здійснюється обмін інформацією, у тому числі і для забезпечення їх синхронної роботи у єдиному системному часі мережі.

Для визначення просторового положення ПО використовуються сигнали відповіді літакового відповідача, які містять інформацію про індивідуальний адрес ПО.

Корисний сигнал відповіді літакового відповідача, який прийнято i-м приймальним пунктом, може бути представлено у наступному вигляді:

$$y_i(t,\vec{\lambda}) = U_i(t)q\left[t + \Delta t_i - \frac{r_{ci}(t)}{c} - t_b\right]\cos\left[\omega t + \left(\Delta\omega_b(t) - \frac{\omega}{c}\dot{r}_i(t)\right)t + \varphi_{0i}(t)\right],$$

де $U_i(t)$ – амплітуда сигналу на вході i-го приймального пункту; t_b – час формування сигналів відповіді; r_{ci} – сумарна псевдодальність; ω – несійна частота сигналу, що приймається; Δt_i – зсув шкали часу i-го приймального пункту відносно шкал часу мережі приймальних пунктів; $\Delta\omega_b(t)$ – зсув частоти сигналу за рахунок нестабільності частоти генератора літакового відповідача; $\frac{\omega}{c}\dot{r}_i(t)$ – допплерівська частота сигналів відповіді; $\dot{r}_i(t)$ – радіальна швидкість ПО відносно i-го приймального пункту; $\varphi_{0i}(t)$ – випадкова початкова фаза.

Слід зазначити, що неузгодженості шкал часу Δt_i можуть бути виміряні, тому їх можна розглядати як відомі величини.

Зсув частоти $\Delta\omega_b(t)$, який обумовлений нестабільністю генератора літакового відповідача, може бути описаний наступним диференціальним рівнянням:

$$\Delta\dot{\omega}_b(t) = -\gamma\Delta\omega_b(t) + \sqrt{2\gamma}\sigma_\omega n_\omega(t), \qquad \Delta\omega_b(t) = \Delta\omega_{b,0},$$

де $n_\omega(t)$ – незалежний формуючий білий гаусівський шум з нульовим математичним очікуванням та одиничною інтенсивністю; γ – параметр, що характеризує ширину спектра флуктуацій частот генератора літакового відповідача; σ_ω^2 – дисперсія флуктуацій частоти генератора літакового відповідача.

Вектор параметрів радіосигналу, який безпосередньо визначає радіосигнал на вході i-го приймального пункту інформаційної системи, що розглядається, буде мати наступний вид:

$$\vec{\lambda} = \left\|r_{si}, \Delta\omega_i\right\|^T,$$

де $\Delta\omega_i = \Delta\omega_b - \frac{\omega}{c}\dot{r}_i$.

При цьому слід зазначити, що огинаюча сигналу літакового відповідача $q(t)$ буде являти собою модулюючу послідовність, сформовану на основі часового імпульсного кодування.

Сумарну псевдодальність r_{si} можна записати у наступному виді:

$$r_{si} = r_0 + r_i + \Delta r_0 + \delta r,$$

де r_0 – відстань між центральним пунктом та ПО в момент приймання сигналу запиту; r_i – відстань між i-м приймальним пунктом та ПО в момент приймання сигналу відповіді; Δr_0 – приріст відстані r_0 внаслідок руху ПО за час t_b; δr – випадкові зміни псевдодальності, викликані нестабільністю затримки відповіді у літаковому відповідачі.

Зв'язок вимірюваних значень сумарної псевдодальності r_{si} з координатами ПО та приймальним пунктом у декартовій системі координат описується рівнянням виду

$$r_{si} = \sqrt{(x_0 - x)^2 + (z_0 - z)^2 + (h_0 - h)^2} + \sqrt{(x_i - x)^2 + (z_i - z)^2 + (h_i - h)^2} + \delta r,$$

де x_0, z_0, h_0, x_i, z_i, h_i, x, z, h – координати пункту обробки інформації i-го приймального пункту та ПО відповідно. Слід зауважити, що у цьому виразі враховано, що величиною Δr_0 можна зневажити внаслідок її малості.

Випадкові зміни псевдодальності, які викликані, як правило, нестабільністю затримки сигналів відповіді у літаковому відповідачу, можуть бути описані диференціальним рівнянням

$$\dot{\delta r}(t) = -\beta \delta r(t) + \sqrt{2\beta \sigma_{\delta r} n_{\delta r}(t)}, \quad \delta r(t_0) = \delta r_0,$$

де $n_{\delta r}(t)$ – формуючий білий гаусівський шум із нульовим математичним очікуванням та одиничною інтенсивністю; β – характеризує ширину спектра флуктуацій процесу $\delta r(t)$; $\sigma_{\delta r}^2$ – стаціонарне значення дисперсії.

В подальшому будемо враховувати, що з ПО в момент часу $T_u(t)$ відбувається випромінювання сигналу відповіді ПО. Будемо враховувати, що є чотири наземні приймальні пункти. Отже, у кожному із приймальних пунктів у момент часу $T_i(t)(i = 0,...,3)$ здійснюється приймання сигналу літакового відповідача. Вважаючи шкали часу, формовані в пунктах системи, високо стабільними можна виключити залежність часових процесів від t. Час прибуття сигналу з літакового відповідача в кожний із приймальних пунктів інформаційної системи, що розглядається, можна записати у наступному виді:

$$T_i(t) = T_u(t) + R_i / c.$$

Віднімаючи час прибуття в базовий пункт обробки радіолокаційних інформації (будемо вважати його нульовим) від часу інших приймальних пунктів, можна записати:

$$R_i - R_0 = c(T_i - T_0) = r_i, \; i = 1,2,3.$$

Виходячи з геометрії розташування приймальних і випромінюючого пунктів, можна записати наступний вираз:

$$R_0^2 = x^2 + y^2 + z^2, \; R_i^2 = (x - x_i)^2 + (y - y_i)^2 + (z - z_i)^2 \; . \tag{1}$$

Відповідно до виразу (1) можливо отримати наступну залежність:

$$R_i^2 - R_0^2 = x_i^2 + y_i^2 + z_i^2 - 2(x_i x + y_i y + z_i z). \tag{2}$$

Використовуючи вирази (1) та (2), можна записати наступний вираз:

$$R_i^2 - R_0^2 = (R_i - R_0)(R_i + R_0) = (r_i + 2R_0) r_i. \tag{3}$$

Коли підставимо вираз (3) у вираз (2) та здійснимо перестановку, отримаємо:

$$2(x_i x + y_i y + z_i z + r_i R_0) = x_i^2 + y_i^2 + z_i^2 - r_i^2. \tag{4}$$

У нашому випадку потрібно оцінити вплив похибок часової синхронізації рознесених пунктів приймання сигналів відповіді на якість вимірювання висоти польоту літакового відповідача, тобто координати z. При цьому окреме диференціювання виразу (4), з урахуванням $T_{i,j} = 0,1,2,3$, дозволяє записати вираз

$$2\left(x_i \frac{dx}{dT_j} + y_i \frac{dy}{dT_j} + z_i \frac{dz}{dT_j} + r_i \frac{dR_0}{dT_j} + R_0 \frac{dr_i}{dT_j} \right) = -2 r_i \frac{dr_i}{dT_j}. \tag{5}$$

Використовуючи результати диференціювання виразу (5), можна записати:

$$\begin{Vmatrix} x & y & z & -R_0 \\ x_1 & y_1 & z_1 & r_1 \\ x_2 & y_2 & z_2 & r_2 \\ x_3 & y_3 & z_3 & r_3 \end{Vmatrix} \times \begin{vmatrix} dx/dT_0 & dx/dT_1 & dx/dT_2 & dx/dT_3 \\ dy/dT_0 & dy/dT_1 & dy/dT_2 & dy/dT_3 \\ dz/dT_0 & dz/dT_1 & dz/dT_2 & dz/dT_3 \\ dR_0/dT_0 & dR_0/dT_1 & dR_0/dT_2 & dR_0/dT_3 \end{vmatrix} = \begin{Vmatrix} 0 & 0 & 0 & 0 \\ R_1 & -R_1 & 0 & 0 \\ R_2 & 0 & -R_2 & 0 \\ R_3 & 0 & 0 & -R_3 \end{Vmatrix}. \quad (6)$$

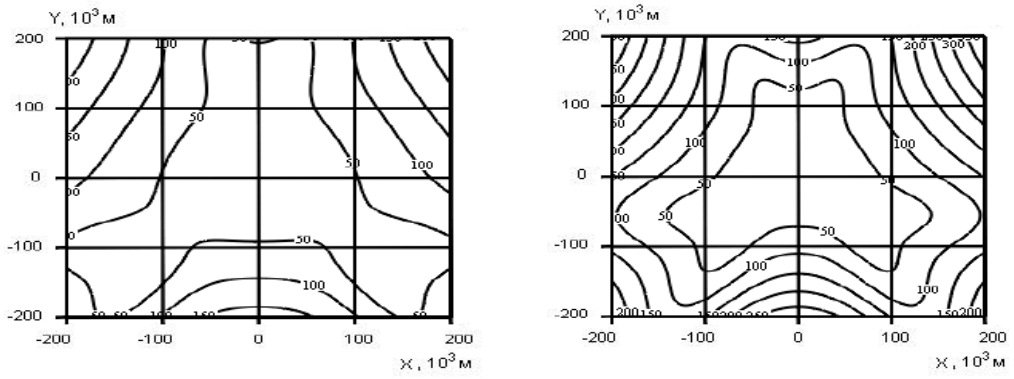
Якщо отриманий вираз (6) записати у наступному вигляді $\vec{D}\vec{A} = \vec{R}$, то рішення виразу буде мати вид

$$\vec{A} = \vec{D}^{-1}\vec{R}. \quad (7)$$

Таким чином для обраного розташування приймальних пунктів синхронної мережі радіолокаційних систем спостережень та позиції ПО матриці $\vec{D}$ і $\vec{R}$ відомі, що дає можливість розв'язати вираз (7).

При цьому слід зазначити, що у виразі (7) третій ряд оціненої матриці $\vec{A}$ являє собою ні що інше, як чутливість вимірювання висоти ПО до похибок як вимірів похилої дальності, так і синхронності формування шкал часу приймальних пунктів радіолокаційної системи, що розглядається. Якщо всі виміри похилої дальності та часові інтервали однаково чутливі до похибок формування синхронної мережі, то сума квадратичних похибок представляє собою загальне значення геометричного фактору.

Розрахунки чутливості вимірювання висоти, нормованої за швидкістю світла, наведені на рис. 2, *а* та рис. 1, *б*. Розрахунки проводились для випадку фіксованої висоти повітряного об'єкту, яка дорівнювала $z = 5$ км, та трикутного розташування наземних приймальних пунктів у точках з координатами: для рис. 1, *а* – (0; $50 \cdot 10^3$), ($50 \cdot 10^3$; $-50 \cdot 10^3$), ($-50 \cdot 10^3$; $-50 \cdot 10^3$) та для рис. 2, *б* – (0; 100·103), (100·103; -100·103), (-100·103; -100·103).



а *б*

Рис. 2. Якість вимірювання висоти повітряного об'єкту

Використання наведеної методики дозволяє висувати вимоги щодо синхронності шкал часу в єдиній синхронній інформаційній мережі радіолокаційних систем спостереження при вимірюванні координат ПО.

Введення додаткових приймальних позицій у багатопозиційну радіолокаційну систему, що розглядається, або збільшення кількості вимірюваних сум відстаней (або різниць відстаней) також покращує точність визначення координат ПО.

Однак слід зазначити, що платою за покращення точності визначення координат ПО є ускладнення системи за рахунок:

- збільшення кількості приймальних позицій;
- збільшення кількості приймально-передаючих трактів;
- необхідність синхронізації процесів випромінювання, прийому сигналів та керування режимами огляду;
- ускладнення алгоритмів ототожнення ПО.

З наведених розрахунків можливо зробити висновок, що чутливість вимірювання висоти ПО суттєво залежить від геометрії розташування приймальних пунктів синхронної мережі радіолокаційних систем спостереження. При збільшенні відстані між пунктами прийому – зростає площа, що охоплена кривими рівної чутливості.

Для визначення необхідної точності синхронізації шкал часу приймальних пунктів при вимірюванні координат ПО потрібно враховувати, що сумарна похибка виміру похилої дальності визначається наступним чином:

$$\sigma_{ds} = \sqrt{\sigma_d^2 + \sigma_{ch}^2},$$

де σ_{ch}^2 – дисперсія похибки синхронності формування шкал часу приймальних пунктів синхронної мережі, перерахована у дальність; σ_d^2 – дисперсія похибки виміру похилої дальності, яка визначається як $\sigma_d^2 = \left(\frac{c\tau_s}{q}\right)^2$, де τ_s – тривалість сигналів, які використовуються у синхронній мережі; q – відношення сигнал/шум на приймальному пункті.

Показано, що при використанні рівної ваги у складі точності виміру дальності, а отже і у вимірі висоти польоту повітряного об'єкту точність синхронності шкал часу приймальних пунктів складає величини, що досягаються сучасними засобами синхронізації часу.

Висновки

Показано, що кооперативні системи спостереження повітряного простору в складі незалежних некооперативних, незалежних кооперативних та залежних кооперативних систем відіграють значну роль в інформаційному забезпеченні системи контролю використання повітряного простору і управління повітряного руху.

Використання наведеної методики оцінки якості виміру координат повітряних об'єктів синхронною мережею кооперативних радіолокаційних систем спостереження повітряного простору дозволяє висувати вимоги щодо синхронності шкал часу в єдиній синхронній інформаційній мережі радіолокаційних систем спостереження при вимірюванні координат повітряних об'єктів.

Показано, що платою за покращення точності визначення координат повітряних об'єктів синхронною мережею кооперативних радіолокаційних систем є ускладнення системи за рахунок збільшення позицій, збільшення кількості приймально-передавальних трактів, необхідності синхронізації процесів випромінювання, прийому сигналів та керування режимами огляду.

Список літератури:

1. D. Xue, L.-T. Hsu, C.-L. Wu, C.-H. Lee, and K. K. H. Ng. Cooperative Surveillance Systems and digital-technology enabler for a real-time standard terminal arrival schedule displacement // Advanced Engineering Informatics. Vol. 50. P. 101402, 2021. doi:10.1016/j.aei.2021.101402.
2. Обод І., Свид І., Мальцев О. Обробка даних радіолокаційних систем спостереження повітряного простору : навч. посібник. Харків : Друкарня Мадрид, 2021. 255 с.
3. Обод І. І., Старокожев С. В., Свид І. В. Оптимізація виявлення сигналів запиту в кооперативних системах спостереження // VIII Міжн. наук.-пр. конф. «Обробка сигналів і негаусівських процесів», присвяч. пам'яті проф. Ю.П. Кунченка : тези доповідей. Черкаси : ЧДТУ, 2021. 117–119.
4. Обод І.І., Стрельницький О.О. Захист інформації в мережі систем спостереження повітряного простору // Системи обробки інформації. 2016. № 2(139). С. 47–49.
5. Svyd I. et al. Noise immunity of data transfer channels in Cooperative Observation Systems: Comparative Analysis // 2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), 2018. doi:10.1109/infocommst.2018.8632019.
6. Pleninger S. The testing of MLAT method application by means of usage low-cost ADS-B receivers // MAD – Magazine of Aviation Development. 2014. Vol. 2, no. 7. P. 8. doi:10.14311/mad.2014.07.02.
7. Lo S. C. and Enge P. Capacity Study of Multilateration (MLAT) based navigation for alternative position navigation and timing (APNT) services for Aviation // Navigation. 2012. Vol. 59, no. 4. P. 263–279.doi:10.1002/navi.25.

8. Garcia M. A., Mueller R., Innis E., and B. Veytsman. An enhanced altitude correction technique for improvement of WAM position accuracy // 2012 Integrated Communications, Navigation and Surveillance Conference, 2012. doi:10.1109/icnsurv.2012.6218375.

9. Обод І.І., Стрельницький О.О. Інформаційна безпека інформаційної мережі систем спостереження повітряного простору // Системи обробки інформації. 2015. № 9(134). С. 96–98.

10.Atkinson S. GPS synchronization of WAM systems – pros and cons [Electronic resource] / Simon Atkinson, Chris Heyes: paper for International Symposium on Enhanced Solutions for Aircraft and Vehicle Surveillance Applications (ESAVS 2010), 16-18 March 2010. Berlin, 2010.

11.Stefanski J. Asynchronous wide area multilateration system // Aerospace Science and Technology. 2014. Vol. 36. P. 94–102. doi: 10.1016/j.ast.2014.03.016.

12.D. He, X. Lu, W. Wang and J. Su. Analysis of Wide Area Multilateration Localization Accuracy Under Different Stations Layout ond Aircraft Height // DEStech Transactions on Engineering and Technology Research, 2017. doi: 10.12783/dtetr/iceta2016/7068.

13.J. Gao, J. Zou, and N. Guo. A secondary surveillance radar data analysis technique based on geometrical method // Lecture Notes in Electrical Engineering. 2020. Vol. 517. P. 707–715.

14.J. Ye, R. Shi, F. Liang, Y. Li, and H. Lin. Research and simulation analysis on research on secondary radar signal coverage // IAEAC 2021 – IEEE 5th Advanced Information Technology, Electronic and Automation Control Conference. 2021. P. 2308–2311.

15.Pleninger S. Relationship between the transponder triggering area and the SSR Mode S surveillance coverage map // New Trends in Civil Aviation. 2022-October. P. 81–85.

16.Minteuan G., Pastrav A., and Palade T. Monopulse secondary surveillance radar – environment impact on target detection // 2022 International Workshop on Antenna Technology, iWAT 2022.P. 86–89.

17.Stevens. Brian L., Frank L. Lewis, and Eric N. Johnson. Aircraft control and simulation: dynamics, controls design, and autonomous systems. John Wiley & Sons, 2015.

18.Svyd I. et al. Comparative quality analysis of the air objects detection by the Secondary Surveillance Radar // 2019 IEEE 39th International Conference on Electronics and Nanotechnology (ELNANO), 2019. doi:10.1109/elnano.2019.8783539.

19.Kim E. and Sivits K. Blended secondary surveillance radar solutions to improve air traffic surveillance // Aerospace Science and Technology. 2005. Vol. 45. P. 203–208.

20.Strohmeier M. Large-scale analysis of aircraft transponder data // IEEE Aerospace and Electronic Systems Magazine. 2017. Vol. 32, no. 1. P. 42–44. doi:10.1109/maes.2017.160149.

21.Leonardi M. and Fausto D. D. Secondary surveillance radar transponders classification by RF Fingerprinting // 2018 19th International Radar Symposium (IRS), 2018. doi:10.23919/irs.2018.8448244.

22.David S. and Vitolo A. J. Airborne IFF transponder antenna system with Omni and steerable cardioid patterns, Aug. 1970. P. 279–283.

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.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.

25.Svyd I., Obod I., Maltsev O., Tkachova T., and Zavolodko G. Optimal request signals detection in cooperative surveillance systems // 2019 IEEE 2nd Ukraine Conference on Electrical and Computer Engineering (UKRCON), 2019. doi:10.1109/ukrcon.2019.8879840.

26.I. Obod et al. Optimization of the quality of information support for consumers of Cooperative Surveillance Systems // Data-Centric Business and Applications. 2020. P. 133–155. doi:10.1007/978-3-030-43070-2_8.

27.Обод І.І., Стрельницький О.О., Андрусевич В.А. Порівняльний аналіз двох методів обробки сигналів відповіді запитальних систем спостереження // Системи обробки інформації. 2014. № 1(117). С. 41–43.

28.S. Ramasamy R. Sabatini and Gardi A. Cooperative and Non-Cooperative Sense-and-Avoid in the CNS+A Context: A Unified Methodology // Proceedings of IEEE International Conference on Unmanned Aircraft Systems (ICUAS 2016). Washington DC (USA), June 2016. Print ISBN: 978-1-4673-9333-1.

29.A. del Corte-Valiente and J. M. Gomez-Pulido. Identification of aircraft in a non-cooperative surveillance system. the case sutudy of aircraft type Canadair Regional Jet // Advances in Automation and Robotics Research in Latin America. 2017. P. 245–254. doi:10.1007/978-3-319-54377-2_21.

30.I. Svyd 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.

31.Обод І.І., Стрельницький О.О., Андрусевич В.А. Синтез та аналіз оптимальних виявлювачів сигналів запиту в літакових відповідачах запитальних систем спостереження повітряного простору // Зб. наук. пр. Харк. нац. ун-ту Повітряних Сил. 2014. № 4(41). С. 8–11.

32.G. Jiang, Y. Fan, and H. Yuan. Assessing the capacity of Air Traffic Control Secondary Surveillance Radar System // 2019 Cross Strait Quad-Regional Radio Science and Wireless Technology Conference (CSQRWC), 2019. doi:10.1109/csqrwc.2019.8799146.

33.Svyd I., Obod I., Maltsev O., Tkachova T., and Zavolodko G. // Improving noise immunity in identification friend or Foe Systems," 2019 IEEE 2nd Ukraine Conference on Electrical and Computer Engineering (UKRCON), 2019. doi:10.1109/ukrcon.2019.8879812.

34.Mahipathi A. C., Gunnery S., Srihari P., D'Souza J., and Jena P. Constrained Radar waveform optimization for a cooperative radar-communication system // Physical Communication. 2023. Vol. 57, p. 101984. doi:10.1016/j.phycom.2022.101984.

35.Obod I. et al. Assessing SSR relative data capacity // 2021 IEEE 3rd Ukraine Conference on Electrical and Computer Engineering (UKRCON), 2021. doi:10.1109/ukrcon53503.2021.9575971

36.Edstaller S. and Mueller D. A cooperative radar system with active reference target synchronization for kinematic target analysis // IEEE Transactions on Microwave Theory and Techniques. 2021. Vol. 69, no. 9. P. 4118–4131. doi:10.1109/tmtt.2021.3079236.

37.Obod I., Svyd I., Maltsev O., and B. Bakumenko. Comparative analysis of noise immunity systems identification friend or foe // 2020 IEEE 40th International Conference on Electronics and Nanotechnology (ELNANO), 2020. doi:10.1109/elnano50318.2020.9088856.

38.Strelnytskyi O. et al. Assessment reliability of data in the identification friend or Foe Systems // 2019 IEEE 39th International Conference on Electronics and Nanotechnology (ELNANO), 2019. doi:10.1109/elnano.2019.8783397.

39.Svyd I. et al. Method of increasing the identification friend or Foe Systems Information Security // 2019 3rd International Conference on Advanced Information and Communications Technologies (AICT), 2019. doi:10.1109/aiact.2019.8847853.

40.Svyd I., Obod I., Maltsev O., Shtykh I., and G. Zavolodko. Model and method for detecting request signals in identification friend or Foe Systems // 2019 IEEE 15th International Conference on the Experience of Designing and Application of CAD Systems (CADSM), 2019. doi:10.1109/cadsm.2019.8779322.

41.Otsuyama T., Honda J., J. Naganawa J., and Miyazaki H. Analysis of signal environment on 1030/1090MHz Aeronautical Surveillance Systems // 2018 IEEE International Symposium on Electromagnetic Compatibility and 2018 IEEE Asia-Pacific Symposium on Electromagnetic Compatibility (EMC/APEMC), 2018. doi:10.1109/isemc.2018.8394048.

42.Svyd I. et al. Fusion of Airspace Surveillance Systems Data // 2019 3rd International Conference on Advanced Information and Communications Technologies (AICT), 2019. doi:10.1109/aiact.2019.8847916

43.Svyd I., Maltsev O., Obod I., and Zavolodko G. Fusion method of primary surveillance radar data and IFF Systems Data // 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), 2020. doi:10.1109/dessert50317.2020.9125040.

44.Semenets V., Svyd I., Obod I., Maltsev O., and Tkach M. Quality Assessment of measuring the coordinates of airborne objects with a secondary surveillance radar // Data-Centric Business and Applications. 2021. P. 105–125, doi:10.1007/978-3-030-71892-3_5.

45.Обод І.І., Свид І.В.. Порівняльний аналіз якості виявлення повітряних об'єктів запитальними системами спостереження // Системи обробки інформації. 2010. Вип. 9 (90). Харків : ХУПС, 2010. С. 74–76.

46.Obod I. et al. Fusion the coordinate data of airborne objects in the networks of Surveillance Radar Observation Systems // Data-Centric Business and Applications, 2020. P. 731–746, doi:10.1007/978-3-030-43070-2_31.

47.Bliss D. W. Cooperative radar and communications signaling: The estimation and information theory odd couple // 2014 IEEE Radar Conference, 2014. doi:10.1109/radar.2014.6875553.

48.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.

49.Обод І.І., Стрельницький О.О., Буланий О.А. Просторовий метод підвищення пропускної здатності телекомунікаційних мереж // Системи обробки інформації. 2014. № 9(125). С. 140–142.

50.Обод І.І.,Стрельницький О.О.,Свид І.В.,Семенова Є.Ю. Аналіз інформаційних процесів обміну даними у системі контролю повітряного простору // Системи озброєння і військова техніка. 2016. № 3(47). С. 88–90.

51.. Черних П., Обод І.І., Свид І.В. Інформаційне забезпечення на основі мереж спостереження повітряного простору // Eastern-European Journal of Enterprise Technologies. 2011. 2/9(50). С. 23–25. doi: 10.15587/1729-4061.2011.1850.

52.Shevtsov I. et al. A Method for Increasing the Capacity of Radio Systems of Short-Range Navigation // 2022 IEEE 2nd Ukrainian Microwave Week (UkrMW), Ukraine, 2022. P. 629–633. doi: 10.1109/UkrMW58013.2022.10037138.

53.Starokozhev S. et al. Frequency Efficiency Evaluation of Query Airspace Surveillance Systems // 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T), Kharkiv, Ukraine, 2021. P. 501–505. doi: 10.1109/PICST54195.2021.9772190.

54.Starokozhev S. et al. Optimization of the Probability of Transmission of Flight Data in the Response Channel of Secondary Radar Systems // 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T), Kharkiv, Ukraine, 2021. P. 511–515. doi: 10.1109/PICST54195.2021.9772199.

55.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.

56.Свид І. В. Обробка радіолокаційної інформації систем спостереження повітряного простору : монографія. Дніпро : ЛІРА ЛТД, 2022. 224 с.

57.Jiang Y., Yang Z., Bo C., and Zhang D. Continuous IFF response signal recognition technology based on capsule network // Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, 2021, P. 455–468. doi: 10.1007/978-3-030-90196-7_39.

58.Обод І.І., Шевцова В.В. Відносна пропускна спроможність запитальних систем передачі інформації системи контроля повітряного простору // Системи обробки інформації. 2013. № 2(109). С. 74–76.

59.Обод І.І., Стрельницький О.О. Інформаційна безпека інформаційної мережі систем спостереження повітряного простору // Системи обробки інформації. 2015. № 9(134). С. 96–98.

60.I. Svyd et al. Analysis of the impact of interference on the time position of signals in requesting Airspace Observation Systems // 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T), 2021. doi:10.1109/picst54195.2021.9772138.

61.Shevtsov I. et al. Quality Evaluation of flight data transmission by the response channel of Secondary Radar // 2022 IEEE 9th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T), 2022. doi:10.1109/picst57299.2022.10238528.

62.Starokozhev S. et al. Comparative analysis of methods for processing data transmission information codes by secondary radar channels // 2022 IEEE 9th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T), 2022. doi:10.1109/picst57299.2022.10238651.

63.Starokozhev S., Shevtsov I., Datsenko O., Chumak V., and Sierikov A. Signal provision of address systems identification friend or foe // 2022 IEEE 9th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T), 2022. doi:10.1109/picst57299.2022.10238675.

64.Бакуменко Б.В., Обод І.І. Методи підвищення завадозахищеності запитувальних радіотехнічних систем // Системи обробки інформації. 2006. № 9(58). С. 10–12.

65.Свид І.В. та інш. Порівняльний аналіз методів визначення координат повітряних об’єктів системами широкозонової мультилатерації // Радіотехніка. 2022. Вип. 209, С. 162–177. doi: 10.30837/rt.2022.2.209.16.

66.Обод І.І., Яценко І.Л., Можаєв О.О. Оцінка інформаційної ємності мобільних інформаційних мереж // Системи обробки інформації. 2014. № 5(121). С. 136–138.

67.Свид І.В. Порівняльний аналіз якості виявлення повітряних об’єктів вторинними радіолокаційними системами // Радіотехніка. 2023. Вип. 213. С. 78–87. doi: 10.30837/rt.2023.2.213.09.

68.Andrusevich V., Obod I. Assessment of the quality of information support by air radar surveillance systems // Advanced Information Systems. 2021. Vol. 5, No. 2. S.78–82. DOI: https://doi.org/10.20998/2522-9052.2021.2.10

69.Свид І.В. Показники якості інформаційного забезпечення користувачів сполученими системами спостереження повітряного простору // Радіотехніка. 2011. Вип. 165. С. 157–160.

70.Черних О.П., Обод І.І., Охрименко М.Ю. Розподілена обробка інформації у сполучених мережах систем спостереження повітряного простору // Системи обробки інформації. 2011. № 2(92). С. 180–182.

71.Обод І.І., Шевцова В.В. Методи підвищення швидкості передачі запитальних систем передачі інформації // Системи обробки інформації. 2013. № 4(111). С. 23–26.

72.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.

73.Обод І.І., Шевцова В.В. Пропускна спроможність відповідачів запитальних систем передачі польотної інформації // Системи обробки інформації. 2013. № 1(108). С. 105–108.

74.Свид І. В., Обод І. І. Завадостійкість радіолокаційних систем ідентифікації за ознакою «свій-чужий»: монографія. Харків : Друкарня Мадрид, 2021. 254 с.

Надійшла до редколегії 26.08.2023

Відомості про авторів:

Свид Ірина Вікторівна – канд. техн. наук, доцент, Харківський національний університет радіоелектроніки, завідувач кафедри мікропроцесорних технологій і систем, Україна; email: iryna.svyd@nure.ua; ORCID: http://orcid.org/0000-0002-4635-6542

Обод Іван Іванович – д-р техн. наук, професор, Харківський національний університет радіоелектроніки, професор кафедри мікропроцесорних технологій і систем, Україна; email: ivan.obod@nure.ua; ORCID: https://orcid.org/0000-0002-9898-0937

Дацько Сергій Валерійович – Харківський національний університет радіоелектроніки, аспірант кафедри мікропроцесорних технологій і систем, Україна; email: serhii.datsko@nure.ua; ORCID: https://orcid.org/0000-0002-2524-8702

Головатенко Сергій Валерійович – Харківський національний університет радіоелектроніки, аспірант кафедри мікропроцесорних технологій і систем, Україна; email: serhii.holovatenko@nure.ua; ORCID: https://orcid.org/0000-0002-7169-6899

ABSTRACTS РЕФЕРАТИ

SYSTEMS AND METHODS OF INFORMATION PROTECTION
СИСТЕМИ І МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ

UDC 004.056.55

Analysis of DSTU 8961:2019 in the quantum random oracle model / *S.O. Kandii, I.D. Gorbenko* // Radiotekhnika: All-Ukr. Sci. Interdep. Mag. 2023. No 214. P. 7 – 16.

Modern cryptographic transformations require provable security against a relatively wide class of threats. Typically, such evidentiary security is achieved through formal analysis within the chosen security model. The development of quantum computers led to the emergence of new attack vectors to which classical cryptography was vulnerable. However, there are cryptographic systems that are considered resistant to quantum attacks and some of them are even standardized. The formal analysis of such systems has faced difficulties for a long time, which were associated with the impossibility of applying classical methods of proof to formal models that take into account quantum effects. However, in recent years, many new results have appeared that allow obtaining formal security proofs for quite complex cryptographic transformations, and most of the existing post-quantum asymmetric encryption and key encapsulation schemes currently have corresponding formal proofs within the quantum random oracle model, the most widespread security model for of post-quantum cryptography. DSTU 8961:2019 is the Ukrainian post-quantum standard for asymmetric encryption and key encapsulation. However, security proofs in the quantum random oracle model have not yet been published for it. As part of this work, security evidence was obtained for the design of the key encapsulation mechanism described in DSTU 8961:209. The obtained result is generalized for an arbitrary asymmetric encryption scheme, which may contain decryption errors and can be used to assess the security of not only DSTU 8961:2019, but also other similar asymmetric transformations.

Key words: post-quantum cryptography; quantum random oracle model; provable security; key encapsulation mechanisms; formal security analysis.

9 fig. Ref.: 11 items

УДК 004.056.55

Аналіз ДСТУ 8961:2019 у моделі квантового випадкового оракула / С.*О. Кандій, І.Д. Горбенко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2023. Вип. 214. С. 7 – 16.

Від сучасних криптографічних перетворень вимагається доказова безпека відносно широкого класу загроз. Зазвичай така доказова безпека досягається за допомогою формального аналізу у межах обраної моделі безпеки. Розвиток квантових комп’ютерів призвів до появи нових векторів атак, до яких класична криптографія виявилася вразливою. Втім, існують криптографічні системи, що вважаються стійкими до квантових атак, і деякі з них вже навіть стандартизовані. Формальний аналіз таких систем тривалий час стикався з труднощами, які були пов’язані з неможливістю застосування класичних методів доказу до формальних моделей, що враховують квантові ефекти. Проте, в останні роки з’явилося багато нових результатів, що дозволяють отримати формальні докази безпеки для доволі складних криптографічних перетворень, і більшість існуючих постквантових схем асиметричного шифрування та інкапсуляції ключів наразі мають відповідні формальні докази у межах моделі квантового випадкового оракула – найбільш розповсюдженій моделі безпеки для постквантової криптографії. ДСТУ 8961:2019 є українським постквантовим стандартом асиметричного шифрування та інкапсуляції ключів. Втім, для нього досі не були опубліковані докази безпеки у моделі квантового випадкового оракула. У межах роботи отримано докази безпеки для конструкції механізма інкапсуляції ключів, що описаний в ДСТУ 8961:209. Отриманий результат є узагальненим для довільної схеми асиметричного шифрування, що може містити помилки дешифрування і може бути застосованим для оцінки безпеки не тільки ДСТУ 8961:2019, але і інших схожих асиметричних перетворень.

Ключові слова: постквантова криптографія; модель квантового випадкового оракула; доказова безпека; механізми інкапсуляції ключів; формальний аналіз безпеки.

Іл. 9. Бібліогр.: 11 назв.

UDC 004.056.5

The main features of the public key infrastructure / *M. O. Bodnia, M. V. Yesina, V. A. Ponomar* // Radiotekhnika: All-Ukr. Sci. Interdep. Mag. 2023. No 214. P. 17 – 25.

Trust is the basis of any communication, whether it is built in the physical world or in the digital environment. Establishing trust in the physical world does not pose any particular challenges because communication subjects can identify each other through biometric features, identity card or other identification documents. In the digital environment, a number of difficulties arise for the identification and authentication procedure. The communicating parties do not meet face-to-face and can be at a significant distance from each other. As a result, they cannot identify uniquely and verify each other's identity using the identity verification methods used in the material world. To ensure the security of electronic communications, it is necessary for communication systems to be equipped with technical means of information protection and an additional mechanism that will contribute to the establishment of trust between the parties to the communication. The Public Key Infrastructure is used to solve problems related to trust, authentication, identity, and

security on a network. A digital certificate is a fundamental element for establishing trust in the digital world. It plays a crucial role in ensuring security and identification on the Internet and when working with electronic resources. The Public Key Infrastructure is a trusted system used to ensure the security and privacy of information across networks and platforms. This system is based on public key cryptography. It implements the management of public keys and digital certificates of various entities, such as companies, corporations, organizations, individuals, websites, servers, etc. The Public Key Infrastructure is widely deployed in government portals and systems. It is used in the electronic government system to guarantee the transparency of the provision of electronic services and to ensure the security of communication links between authorities and society. The Public Key Infrastructure represents a multifaceted structure that includes a set of standards, technologies, and procedures for managing, storing, and distributing keys and digital certificates. A certificate authority is a key component of a public key infrastructure and is an independent third party that manages digital certificates. Various technical and cryptographic means of information security are used in the Public Key Infrastructure, such as digital signatures, encryption, hash functions, hardware security modules, key management software, etc. The main purpose of this article is to analyze the main features and aspects of public key infrastructure.

Key words: authentication; identification; chain of trust; public key infrastructure paradigm; smart cards; third party; digital certificates.

7 fig. Ref.: 11 items.

УДК 004.056.5

Основні особливості інфраструктури відкритих ключів / *М. О. Бодня, М. В. Єсіна, В. А. Пономар* // Радіотехніка: Всеукр. міжвід. наук.-техн. зб. 2023. Вип. 214. С. 17 – 25.

Довіра є базисом будь-яких комунікаційних відносин, незалежно від того вибудовуються вони у фізичному світі чи у цифровому середовищі. Встановлення довірчих відносин у фізичному світі не становить особливих складнощів, оскільки суб'єкти комунікації можуть ідентифікувати один одного за біометричними ознаками, посвідченням особи або іншими ідентифікаційними документами. У цифровому середовищі виникає ряд складнощів для проведення процедури ідентифікації та автентифікації. Сторони комунікації не перетинаються віч-на-віч і можуть перебувати на великій відстані один від одного. Внаслідок чого вони не можуть однозначно ідентифікувати та перевірити особистість один одного за допомогою методів перевірки ідентичності, що застосовуються в матеріальному світі. Для забезпечення безпеки електронних комунікацій необхідно, щоб комунікаційні системи були обладнані технічними засобами захисту інформації та додатковим механізмом, який сприятиме встановленню довіри між сторонами комунікації. Інфраструктура відкритих ключів використовується для вирішення проблем, пов'язаних із довірою, автентифікацією, ідентифікацією та безпекою в мережі. Цифровий сертифікат є базовим елементом для встановлення довірчих відносин у цифровому світі. Він грає важливу роль у забезпеченні безпеки та ідентифікації в Інтернеті та при роботі з електронними ресурсами. Інфраструктура відкритих ключів є надійною системою, яка використовується для забезпечення безпеки та конфіденційності інформації у мережах та платформах. Ця система базується на криптографії з відкритим ключем. Вона реалізує управління відкритими ключами та цифровими сертифікатами різних сутностей, таких як компанії, корпорації, організації, фізичні особи, веб-сайти, сервери тощо. Інфраструктура відкритих ключів широко розгортається в урядових порталах та системах. Вона використовується в системі електронного уряду для гарантування прозорості надання електронних послуг та забезпечення безпеки комунікаційних зв’язків органів влади з суспільством. Інфраструктура відкритих ключів представляє собою багатогранну структуру, яка включає набір стандартів, технологій і процедур для управління, зберігання та розповсюдження ключів і цифрових сертифікатів. Центр сертифікації є ключовим компонентом інфраструктури відкритих ключів та являє собою незалежну третю сторону, яка здійснює управління цифровими сертифікатами. В інфраструктурі відкритих ключів використовуються різні технічні та криптографічні засоби захисту інформації, такі як цифровий підпис, шифрування, геш-функції, апаратні модулі безпеки, програмне забезпечення для управління ключами тощо. Основною метою статті є аналіз основних особливостей та аспектів інфраструктури відкритих ключів.

Ключові слова: автентифікація; ідентифікація; ланцюжок довіри; парадигма інфраструктури відкритих ключів; смарт-карти; третя сторона; цифрові сертифікати.

Іл. 7. Бібліогр.: 11 назв.

UDC 004.056.5

Analysis of two-factor authentication plugins for WordPress / *S.O. Kolomiitsev, O.V. Sievierinov, V.M. Fedorchenko, V.M. Sukhoteplyi* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2023. No 214. P. 26 – 31.

The purpose of this article is to analyze existing two-factor authentication plugins to assess their effectiveness. Due to the lack of substantial protection against unauthorized access in the WordPress system, it becomes vulnerable to types of attacks such as dictionary attacks and brute force attacks. To address this issue, plugins for two-factor authentication are used. The article examines the most popular two-factor authentication plugins to evaluate the level of security they provide.

This article will be beneficial for website owners and administrators using WordPress who need to protect their resources against unauthorized access.

Key words: WORDPRESS; PLUGIN; XML-RPC; two-factor authentication.

1 tabl. 5 fig. Ref.: 10 items.

УДК 004.056.5

Аналіз плагінів двофакторної автентифікації для системи WordPress / *С.О. Коломійцев, О.В. Сєвєрінов, В.М. Федорченко, В.М. Сухотеплий* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2023. Вип. 214. С. 26 – 31.

Метою статті є аналіз існуючих плагінів двофакторної автентифікації для оцінки їх ефективності. Через те, що система WordPress не має суттєвого захисту від несанкціонованого доступу, вона стає вразливою перед такими типами атак як: атака зі словником і атака методом повного перебору. Для вирішення цієї проблеми використовують плагіни для двофакторної автентифікації. У статті розглядаються найпопулярніші плагіни для двофакторної автентифікації, з метою оцінити рівень захищеності, який вони надають.

Стаття буде корисна власникам та адміністраторам веб-сайтів на WordPress, які мають необхідність захистити свій ресурс від несанкціонованого доступу.

Ключові слова: WORDPRESS; ПЛАГІН; XML-RPC; двофакторна автентифікація.

Табл. 1. Іл. 5. Бібліогр.: 10 назв.

UDC 004.056

Ensuring security in distributed information systems: major aspects / *V.I. Yesin, V.V. Vilihura, I.I. Svatowsky* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2023. No 214. P. 32 – 64.

Ensuring the security of distributed information systems is a critical task since these systems are used primarily to process and store large amounts of sensitive information such as financial data, medical records, personal data, etc. Information in the world is one of the most important resources of society, and without its protection, new information technologies can violate the private life of people and activities of various organizations. In the era of Big Data, the problem of protecting sensitive data is even more aggravated. And this is despite the large global security spending that organizations and companies around the world incur, including in order to meet the requirements of relevant laws and other regulations governing the activities of companies in modern conditions. To solve it, it is necessary to use a combination of legislative, organizational measures and software and hardware. Therefore, in the current situation, taking into account: (a) the current state of development of technologies of distributed information systems and its fleeting nature; (b) scientific and practical achievements in the field of information security; (c) the qualifications of attackers who are constantly improving the capabilities of malicious influence; (d) provisions and recommendations of various regulations-legal acts, information systems specialists in many cases, in order to ensure the reliable safe functioning of the latter, need appropriate knowledge of security issues. That is, knowledge of current modern methods, techniques and means of ensuring security. This paper is precisely aimed at providing such knowledge. It concisely presents a fairly wide range of issues related to the security of distributed information systems.

Key words: distributed information system; security; confidentiality; sensitive; integrity; availability.

14 fig. Ref.: 91 items.

УДК 004.056

Забезпечення безпеки у розподілених інформаційних системах: основні аспекти / *В.І. Єсін, В.В. Вілігура, І.І. Сватовський* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2023. Вип. 214. С. 32 – 64.

Забезпечення безпеки розподілених інформаційних систем є критично важливим завданням, оскільки ці системи використовуються переважно для обробки та зберігання великого обсягу чутливої/конфіденційної інформації, такої як фінансові дані, медичні записи, персональні дані тощо. Інформація у світі є одним із найважливіших ресурсів суспільства, без необхідного захисту якої нові інформаційні технології здатні порушити приватне життя людей та діяльність різних організацій. В епоху Великих Даних проблема захищеності чутливих даних ще більше загострюється. І це незважаючи на великі глобальні витрати на безпеку, на які йдуть організації та компанії у всьому світі, у тому числі, щоб відповідати вимогам відповідних законів та інших нормативно-правових актів, які регламентують діяльність компаній у сучасних умовах. Для її вирішення необхідне комплексне використання законодавчих, організаційних заходів та програмно-технічних засобів. Тому в ситуації, що склалася, враховуючи сучасний стан розвитку технологій розподілених інформаційних систем, його швидкоплинний характер, науково-практичні досягнення в галузі інформаційної безпеки, кваліфікацію зловмисників, які постійно вдосконалюють можливості шкідливого впливу, положення та рекомендації різних нормативно-правових актів, фахівцям з інформаційних систем у багатьох випадках, щоб забезпечити надійне безпечне функціонування останніх, потрібні знання з питань забезпечення безпеки. Тобто знання актуальних сучасних методів, прийомів та засобів забезпечення безпеки. Ця стаття націлена на надання таких знань, у стислому викладі представляється достатньо широке коло питань, пов'язаних із безпекою розподілених інформаційних систем.

Ключові слова: розподілена інформаційна система; безпека; конфіденційність; цілісність; доступність.

Іл. 14. Бібліогр.: 91 назв.

UDC 621.391:519.2

Method of encryption in the MST3 cryptosystem based on Automorphisms group of Suzuki's functional field / *Y. Kotukh, G. Khalimov, M. Korobchinskyi* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2023. No 214. P. 65 – 76.

This article presents a new encryption method based on the group of automorphisms of Suzuki's functional field, which enhances the security level of the existing MST3 cryptosystem. This approach is a response to the progress in

developing powerful quantum computers, which can threaten the security of many public-key encryption systems, particularly those based on factorization and discrete logarithm problems, such as RSA or ECC. Using non-commutative groups to create quantum-resistant cryptosystems has been a known approach over the last two decades. The unsolvable word problem, proposed by Wagner and Magyarik, applied in the realm of permutation groups, is key to the development of cryptosystems. Logarithmic signatures, introduced by Magliveras, represent a unique type of factorization suitable for finite groups. The latest version of such implementation, known as MST3, is based on the Suzuki group. In 2008, Magliveras presented the LS limit of transitivity for the MST3 cryptosystem. Later, Svaba proposed an improved version of the cryptosystem eMST3 with enhanced protective features, including secret homomorphic covering. In 2018, T. van Trung suggested the application of the MST3 approach using strong aperiodic logarithmic signatures for Abelian p-groups. Kong and his colleagues conducted an in-depth analysis of MST3 and noted that due to the lack of publications on the quantum vulnerability of this algorithm, it can be considered as a potential candidate for use in the post-quantum era. One of the key ideas is to increase encryption efficiency by optimizing computational resources, particularly through reducing the size of the key space. This method is applied to the calculations of logarithmic signatures within the group. It was implemented over finite fields of small sizes.

Key words: MST3; cryptosystem; word problem; logarithmic signature; random covers; Suzuki function field.

Ref.: 28 items.

УДК 621.391:519.2

Метод направленого шифрування в криптосистемі MST3 на основі автоморфізмів функціонального поля Сузукі / *Є.В. Котух, Г.З. Халімов, М.В. Коробчинський* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2023. Вип. 214. С. 65 – 76.

Представлено новий метод шифрування, заснований на групі автоморфізмів функціонального поля Сузукі, що підвищує рівень безпеки існуючої криптосистеми MST3. Цей підхід є відповіддю на прогрес у розробці потужних квантових комп'ютерів, які можуть загрожувати безпеці багатьох систем шифрування з відкритим ключем, зокрема тих, що базуються на проблемах факторизації та дискретного логарифмування, як RSA чи ECC. Використання некомутативних груп для створення квантово-стійких криптосистем є відомим підходом протягом останніх двох десятиліть. Нерозв'язна проблема слова, запропонована Вагнером і Магьяриком, застосовується у сфері перестановочних груп, є ключовою для розвитку криптосистем. Логарифмічні підписи, введені Магліверасом, представляють собою унікальний тип факторизації, придатний для скінченних груп. Найновіша версія такої реалізації, відома як MST3, базується на групі Сузукі. У 2008 р. Магліверас представив ліміт LS транзитивності для криптосистеми MST3. Згодом Сваба запропонував удосконалену версію криптосистеми eMST3 з покращеними характеристиками захисту, включаючи секретне гомоморфне накриття. У 2018 р. Т. ван Трунг вніс пропозицію щодо застосування підходу MST3 з використанням міцних аперіодичних логарифмічних підписів для абелевих *p*-груп. Конг та його колеги провели глибокий аналіз MST3 і зазначили, що через відсутність публікацій про квантову вразливість цього алгоритму, його можна розглядати як потенційного кандидата для використання в постквантову епоху. Однією з ключових ідей є підвищення ефективності шифрування за рахунок оптимізації обчислювальних ресурсів, зокрема за допомогою зменшення розміру ключового простору. Цей метод застосовується до розрахунків логарифмічних підписів у межах групи. Він був реалізований над скінченними полями малих розмірів.

Ключові слова: MST3; криптосистема; проблема слова; логарифмічний підпис; випадкове накриття; функціональне поле Сузукі.

Бібліогр.: 28 назв.

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

UDC 621.396.671

Analysis of acoustic field distribution of circular equaldistant and non-equidistant two–section electronics microphone array in free space / *R.I. Tsekhmistro, S.V. Shapovalov* // Radiotekhnika : All-Ukr. Sci. Inter-dep. Mag. 2023. No 214. P. 77 – 84.

The authors described the analysis of the spatial distribution of the acoustic field amplitude of circular microphone lattice. A model – a spherical wave emitter, represented each microphone. An analysis was carried out of the influence of the number of emitters and the radius of the array on the concentration of the acoustic field in the center and at an arbitrary distance. An algorithm has been compiled that makes it possible to take into account an arbitrary even and odd number of emitters located along the length of the arc, both uniformly and unevenly.

The distribution of the complex power of the acoustic field of a linear array of emitters is considered under the assumption that each microphone (emitter) transmits the acoustic field in the form of a spherical wave. According to the classical principles (Lorentz lemma, the “Reciprocity” theorem), we believe that there is no shape of the radiation pattern as formed at short distances (near zone), that is, the distribution of the emitter field in the mode of receiving and transmitting an acoustic signal is identical.

It is shown that at distances between the boundaries of the intermediate and far zones, local areas may appear in which a smaller number of microphones can provide the same acoustic field or even more than with a larger number.

This can be achieved by using an internal arc of microphone arrangement, then it is possible to achieve an equivalent field along the axis of the array with a smaller number of microphones located equidistant along the outer radius, it is possible to achieve an equivalent field than with an increased number of them.

Fig. 11. Ref.: 8.

Key words: microphone array (lattice); isotropic radiator; superposition; lattice radius; microphone; interference; directional pattern.

UDC 621.396.671

Особливості формування оптимального розподілу акустичного поля кільцевої еквідистантної та нееквідистантної двосекційної мікрофонної решітки з електронним керуванням / *Р.І. Цехмістро, С.В. Шаповалов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2023. Вип. 214. С. 77 – 84.

Описано аналіз просторового розподілу амплітуди акустичного поля кільцевої мікрофонної решітки. Кожен мікрофон було представлено моделлю – випромінювачем сферичної хвилі. Проведено аналіз впливу числа випромінювачів, радіусу ґрати на концентрацію акустичного поля в центрі і на довільній відстані. Складено алгоритм, що дозволяє враховувати довільне парну та непарну кількість випромінювачів, розташованих по довжині дуги як рівномірно так і нерівномірно.

Розглянуто розподіл комплексної потужності акустичного поля лінійних ґрат випромінювачів у припущенні, що кожен мікрофон (випромінювач) транслює акустичне поле у вигляді сферичної хвилі. Відповідно до класичних положень (лема Лоренца, теорема “Взаємності”) вважаємо, що форми діаграми спрямованості як сформованої немає на малих відстанях (близька зона), тобто розподіл поля випромінювача в режимі прийому та передачі акустичного сигналу ідентичний.

Показано, що на відстанях між межами проміжної та дальньої зони можливі появи локальних областей, у яких меншою кількістю мікрофонів можна забезпечити таке ж акустичне поле або навіть більше, ніж за більшої кількості. Цього можна досягти за умови використання внутрішньої дуги розташування мікрофонів, тоді можливе досягнення еквівалентного поля по осі решітки за меншою кількістю мікрофонів, розташованих еквідистантно по зовнішньому радіусу можна досягти еквівалентного поля ніж при збільшеної їх кількості.

Ключові слова: мікрофонні грати; ізотропний випромінювач; суперпозиція; радіус ґрат; нееквідистантність; інтерференція.

Іл. 11. Бібліогр.: 8 назв.

INFORMATION METHODS OF RADIO ENGINEERING, SIGNAL PROCESSING
ІНФОРМАЦІЙНІ МЕТОДИ РАДІОТЕХНІКИ, ОБРОБКА СИГНАЛІВ

UDC 629.7.022

Using coherent processing algorithms for direction finding of UAV acoustic signals / *V.M. Kartashov, M.V. Rybnykov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2023. No 214. P. 85 – 93.

Small UAVs are often used in a group, since their signals are highly correlated, their resolution is reduced when using non-coherent processing.

The article analyzes the well-known methods of coherent processing of acoustic signals in order to increase the resolution in the direction finding of signals with a high degree of correlation. Obtaining qualitative indicators of the analyzed algorithms was carried out by the method of statistical computer modeling in the Matlab environment.

Based on the simulation results, it is shown that coherent signal processing methods are the most stable in conditions of low signal-to-noise ratios, while non-coherent ones show the best results in the region of high signal-to-noise ratio, while coherent algorithms can potentially distinguish more targets. the WAVES coherent algorithm performs better in the high signal-to-noise ratio region, but loses to the CSSM algorithm in the low signal-to-noise region.

To increase the efficiency of coherent processing of multipath signals, it applies spatial filtering of the input signal.

Key words: unmanned aerial vehicle; coherent processing; direction finding station; acoustic array; signal processing.

8 fig. Ref.: 19 items.

УДК 629.7.022

Застосування алгоритмів когерентної обробки для пеленгації акустичних сигналів БПЛА / *В.М. Карташов, М.В. Рибников* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2023. Вип. 214. С. 85 – 93.

Малі БПЛА часто застосовуються в групі, оскільки їх сигнали мають високий рівень кореляції, їх роздільна здатність при використанні некогерентної обробки знижується.

Аналізуються відомі методи когерентної обробки акустичних сигналів з метою збільшення роздільної здатності при пеленгації сигналів високого ступеня кореляції. Отримання якісних показників аналізованих алгоритмів здійснювалося методом статистичного комп'ютерного моделювання в середовище Matlab.

За результатами моделювання показано, що когерентні методи обробки сигналу є найбільш стійкими в умовах низьких відносин сигнал-шум, у той час як некогерентні показують кращі результати в галузі високого відношення сигнал-шум, при цьому когерентні алгоритми можуть потенційно розрізнити більше цілей. Когере-

нтний алгоритм WAVES показує найкращі результати в області високого відношення сигнал шум, але в області низького відношення сигнал шум програє алгоритму CSSM.

Для збільшення ефективності когерентної обробки багатопроменевих сигналів застосовує просторова фільтрація вхідного сигналу.

Ключові слова: безпілотний літальний апарат; когерентна обробка; станція пеленгування, акустична решітка; обробка сигналів.

Іл. 8. Бібліогр.: 19 назв.

APPLICATION OF RADIO TECHNOLOGY METHODS
ЗАСТОСУВАННЯ МЕТОДІВ РАДІОТЕХНІКИ

UDC 615.472.03

Using the STM32f407vg microcontroller to study the amplitude-frequency characteristics of biological tissues / *V.V. Semenets, V.I. Leonidov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2023. No 214. P. 94 – 101.

The electrical properties of biological tissues of a plant origin are studied using the microcontroller STM32f407vg. The formulation of the problem of identifying informative signs of the viability of biological tissues when using the method of impedance measurement is given. It is shown that since currently in medical diagnostic practice there is no instrument base that would allow in an operational setting to diagnose the ability of biological tissue to self-heal after injury and damage as a result of thermal exposure, a gunshot wound or prolonged compression, the development of methods and means of instrumental diagnostics in this area of knowledge is an important modern task.

The results of experimental measurements of impedance characteristics in the frequency range of 20 Hz – 2.0 MHz are presented. The frequency dependences of the stress modulus of a biological tissue of a plant origin are analyzed in its intact state, as well as after exposure of samples of a biological tissue in a freezer.

A comparative analysis of the obtained frequency dependences is carried out. A significant difference between the frequency dependences of the stress modulus on a biological tissue and the frequency dependence of the stress modulus on an isotonic solution is shown. The idea was proposed that the degree of difference in the frequency distribution of the impedance module of the biological tissue from the impedance module of the isotonic solution can serve as a criterion for assessing the degree of damage to the biological tissue.

Key words: impedance measurement; viability; frequency response; informative signs; microcontroller.

7 fig. Ref.: 15 items.

УДК 615.472.03

Використання мікроконтролера STM32f407vg для дослідження амплітудно-частотних характеристик біологічних тканин / *В.В. Семенець, В.І. Леонідов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2023. Вип. 214. С. 94 – 101.

Досліджуються електричні властивості біологічних тканин рослинного походження з використанням мікроконтролера STM32f407vg. Приведена постановка задачі виявлення інформативних ознак життєздатності біологічних тканин при використанні методу імпедансометрії. Показано, що оскільки в цей час у медичній діагностичній практиці відсутня приладова база, що дозволяє в оперативній обстановці здійснювати діагностику здатності біологічної тканини до самовідновлення після одержання травм і поразок у результаті термічного впливу, вогнепального поранення або тривалого здавлювання, то розробка методів і засобів інструментальної діагностики в цій галузі знань є важливим сучасним завданням.

Наведено результати експериментальних вимірів характеристик імпедансу в діапазоні частот 20 Гц – 2,0 МГц. Аналізуються частотні залежності модуля напруги біологічної тканини рослинного походження при її неушкодженому стані, а також після витримки зразків біологічної тканини в морозильній камері.

Проведено порівняльний аналіз отриманих частотних залежностей. Показано істотну відмінність частотних залежностей модуля напруги на біологічній тканині від частотної залежності модуля напруги на ізотонічному розчині. Запропоновано ідею, що критерієм оцінки ступеня поразки біологічної тканини може служити ступінь відмінності частотного розподілу модуля імпедансу біологічної тканини від модуля імпедансу ізотонічного розчину.

Ключові слова: імпедансометрія; життєздатність; частотна характеристика; інформативні ознаки; мікроконтролер.

Іл. 7. Бібліогр.: 15 назв.

RADAR AND RADIONAVIGATION
РАДІОЛОКАЦІЯ І РАДІОНАВІГАЦІЯ

UDC 621.396.967.2

Assessment of the quality of determining the coordinates of air objects by cooperative radar systems for air surveillance / *I.V. Svyd, I.I. Obod, S.V. Holovatenko, S.V. Datsko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2023. No 214. P. 102 – 114.

In the presented work, based on the classification of airspace surveillance radar systems in the form: independent non-cooperative radar surveillance, independent cooperative radar surveillance, dependent cooperative radar surveillance; the quality of determining the coordinates of air objects by the systems under study was assessed. The place and role of these information systems in the information support of airspace control and air traffic control systems is shown. From the calculations carried out, we can draw the following conclusion that the sensitivity of measuring the height of an airborne object significantly depends on the geometry of the location of receiving points of a synchronous network of radar surveillance systems. As the distance between receiving points increases, the area covered by curves of equal sensitivity increases. It is substantiated that when using equal weight in the accuracy of range measurement and in measuring the altitude of an airborne object, the accuracy of the synchronization of the time scales of the receiving points is the value achieved by modern means of time synchronization. The use of the given methodology for assessing the quality of measuring the coordinates of air objects in a synchronous network of cooperative radar surveillance systems for airspace allows us to put forward requirements for the synchronism of time scales in a unified synchronous information network of radar surveillance systems when measuring the coordinates of air objects. It is shown that the price for improving the accuracy of determining the coordinates of air objects by a synchronous network of cooperative radar systems is the complication of the system due to an increase in positions, an increase in the number of transceiver paths, the need to synchronize emission processes, receive signals and control viewing modes.

Key words: radar system; airspace; cooperative system; synchronous system; surveillance system; air object; evaluation; quality; coordinate; distance; height.

1 fig. Ref.: 74 items.

УДК 621.396.967.2

Оцінка якості визначення координат повітряних об’єктів кооперативними радіолокаційними системами спостереження повітряного простору / *І.В. Свид, І.І. Обод, С.В. Головатенко, С.В. Дацько* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2023. Вип. 214. С. 102 – 114.

На підставі класифікації систем радіолокаційного спостереження повітряного простору у виді: незалежне некооперативне радіолокаційне спостереження, незалежне кооперативне радіолокаційне спостереження, залежне кооперативне радіолокаційне спостереження проведено оцінку якості визначення координат повітряних об’єктів досліджуваними системами. Показано місце та роль зазначених інформаційних систем в інформаційному забезпеченні систем контролю повітряного простору та управління повітряного руху. З проведених розрахунків можливо зробити наступний висновок, що чутливість вимірювання висоти повітряного об’єкту суттєво залежить від геометрії розташування приймальних пунктів синхронної мережі радіолокаційних систем спостереження. При збільшенні відстані між пунктами прийому – зростає площа, що охоплена кривими рівної чутливості. Обгрунтовано, що при використанні рівної ваги у складі точності виміру дальності та у вимірі висоти польоту повітряного об’єкту точність синхронності шкал часу приймальних пунктів складає величину, що досягається сучасними засобами синхронізації часу. Використання наведеної методики оцінки якості виміру координат повітряних об’єктів синхронною мережею кооперативних радіолокаційних систем спостереження повітряного простору дозволяє висувати вимоги щодо синхронності шкал часу в єдиній синхронній інформаційній мережі радіолокаційних систем спостереження при вимірюванні координат повітряних об’єктів. Показано, що платою за покращення точності визначення координат повітряних об’єктів синхронною мережею кооперативних радіолокаційних систем є ускладнення системи за рахунок збільшення позицій, збільшення кількості приймально-передавальних трактів, необхідності синхронізації процесів випромінювання, прийому сигналів та керування режимами огляду.

Ключові слова: радіолокаційна система; кооперативна система; синхронна система; система спостереження; повітряний об’єкт; оцінка; якість; координати; дальність; висота.

Іл. 1. Бібліогр.: 74 назви.

COLLECTION OF SCIENTIFIC PAPERS
RADIOTEKHNIKA
Issue 214
In English and Ukrainian

ЗБІРНИК НАУКОВИХ ПРАЦЬ
РАДІОТЕХНІКА
Випуск 214
Англійською та українською мовами

Коректор Л.І. Сащенко

Підп. до друку 30.09.2023. Формат 60x90/8. Папір офсет. Гарнітура Таймс. Друк. ризограф.
Ум. друк. арк. 9,9. Обл.-вид. арк. 8,6. Тираж 300 прим. Зам. № 549. Ціна договір.

Харківський національний університет радіоелектроніки (ХНУРЕ)
Просп. Науки, 14, Харків, 61166.

Оригінал-макет підготовлено і збірник надруковано у ПФ „Колегіум”, тел. (057) 703-53-74.
Свідоцтво про внесення суб’єкта видавничої діяльності до Державного реєстру видавців.
Сер. ДК №1722 від 23.03.2004.