МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ
УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ

РАДІОТЕХНІКА

Всеукраїнський
міжвідомчий науково-технічний збірник

Засновано в 1965 р.

В И П У С К 2 0 3

Харків
Харківський національний
університет радіоелектроніки
2020

УДК 621.3

Збірник включено до Переліку наукових фахових видань України, категорія "Б", технічні та фізико-математичні науки (затверджено наказами МОНУ від 17.03.2020 № 409; від 02.07.2020 № 886; від 24.09.2020 № 1188) за спеціальностями: 171 – Електроніка; 172 – Телекомунікації та радіотехніка; 173 – Авіоніка; 125 – Кібербезпека; 151 – Автоматизація та комп'ютерно-інтегровані технології; 152 – Метрологія та інформаційно-вимірювальна техніка; 153 – Мікро- та наносистемна техніка; 163 – Біомедична інженерія; 105 – Прикладна фізика та наноматеріали.

Сборник включен в Перечень научных профессиональных изданий Украины, категория «Б», технические и физико-математические науки (утверждено приказами МОНУ от 17.03.2020 № 409, от 02.07.2020 № 886, от 24.09.2020 № 1188) по специальностям: 171 – Электроника; 172 – Телекоммуникации и радиотехника; 173 – Авионика; 125 – Кибербезопасность; 151 – Автоматизация и компьютерно-интегрированные технологии; 152 – Метрология и информационно-измерительная техника; 153 – Микро- и наносистемная техника; 163 – Биомедицинская инженерия; 105 – Прикладная физика и наноматериалы.

The collection is included in the List of scientific professional publications of Ukraine, category «Б», technical and physical-mathematical sciences (approved by orders of the Ministry of Education and Science from 17.03.2020 № 409; from 02.07.2020 № 886; from 24.09.2020 № 1188) by specialties: 171 – Electronics; 172 – Telecommunications and Radio Engineering; 173 – Avionics; 125 – Cybersecurity; 151 – Automation and Computer-Integrated Technologies; 152 – Metrology and Information-Measuring Equipment; 153 – Micro- and Nanosystem Technology; 163 – Biomedical Engineering; 105 – Applied Physics and Nanomaterials.

Сайт: rt.nure.ua

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

За зміст статті відповідальні автори.

Відповідальні випускові: *І.Д. Горбенко, д-р техн. наук, проф.,*
А.І. Лучанінов, д-р фіз.-мат. наук, проф.
Технічний секретар *О.С. Полякова.*

Рекомендовано Вченою радою Харківського національного університету радіоелектроніки, протокол №11/11-1 від 23.12.2020.

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

Збірник «Радіотехніка» включено до Каталогу передплатних видань України, передплатний індекс ***08391.***

ЗМІСТ

CONTENT

METHODS AND MECHANISMS OF CRYPTOGRAPHIC PROTECTION OF INFORMATION

INFORMATION PROTECTION METHODS AND MECHANISMS

METHODS OF SYNTHESIS AND ANALYSIS OF SIGNALS

RADIO ENGINEERING SYSTEMS

ELECTRODYNAMICS, OPTICS, MICROWAVE TECHNOLOGY

APPLICATION OF METHODS OF RADIO ENGINEERING

SIGNAL PROCESSING

МЕТОДИ ТА МЕХАНІЗМИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

УДК 004.056.5 **DOI:10.30837/rt.2020.4.203.01**

В. В. СЕМЕНЕЦЬ, д-р техн. наук, О. С. МАРУХНЕНКО, І. Д. ГОРБЕНКО, д-р техн. наук, Г. З. ХАЛІМОВ, д-р техн. наук

ПОРІВНЯЛЬНИЙ АНАЛІЗ ОДНОРАЗОВИХ ПІДПИСІВ НА БАЗІ ГЕШ-ФУНКЦІЙ

Вступ

Стійкість значної частини сучасних асиметричних базується на складності рішення задач факторизації (RSA), дискретного логарифма в простому полі (DSA) або групі точок еліптичної кривої (ECDSA). Квантові комп'ютери, що можуть з'явитися в найближчі десятиліття, здатні вирішити ці задачі.

Актуальною є проблема аналізу та стандартизації постквантових криптосистем. З цією метою NIST проводить відкритий конкурс [1], в якому представлені алгоритми, побудовані на різних алгебраїчних структурах. В тому числі були представлені два алгоритми цифрового підпису на базі геш-функцій: Gravity SPHINCS [2] (брав участь тільки у першому раунді) та SPHINCS+[3] (успішно пройшов до третього [4]), які є незалежними модифікаціями раніше розробленого алгоритму SPHINCS [5].

Усі алгоритми сімейства SPHINCS мають складну структуру та включають декілька простіших алгоритмів підпису, серед яких одноразовий підпис Вінтерніца.

Метою статті є аналіз існуючих алгоритмів одноразового підпису, зокрема підписів Лампорта[6] та Вінтерніца[7]. Запропоновано та проаналізовано модифікації цих алгоритмів.

1. Огляд алгоритмів ЕЦП на базі геш-функцій

Загальна ідея підписів, що базуються на геш-функціях, полягає в тому, що у відповідність до повідомлення ставиться масив бітових рядків, елементи якого обрані та, можливо, прогешовані певну кількість разів відповідно до бітів повідомлення.

Стійкість цього класу ЕЦП базується на основних властивостях криптографічних геш-функцій – односпрямованності та стійкості до колізій. Згідно з [8] основними вимогами до функцій гешування є:

1) Складність знаходження колізії $C_{col} \geq 2^{h_{len}/2}$.

2) Складність відновлення прообразу $C_{preim} \geq 2^{h_{len}}$.

3) Складність знаходження іншого прообразу $C_{sec\_preim} \geq 2^{h_{len}}$.

Розглянемо переваги підписів на базі геш-функцій:

1) постквантовість – сучасні криптографічні геш-функції, наприклад SHA-2 та SHA-3, стійкі до квантових атак і можуть безпечно використовуватись і після створення квантових комп'ютерів;

2) легка модифікація – алгоритми ЕЦП цього класу не детермінують використовувані геш-функції, що дозволяє легко замінити механізм гешування, якщо в ньому будуть знайдені вразливості;

3) гнучкість – доповнює попередню властивість тим, що в залежності від вимог до системи можуть бути обрані геш-функції та системні параметри, що найкраще ним задовольняють, та досягається компроміс між стійкістю, швидкодією та пам'яттю.

До недоліків слід віднести:

1) обмежена кількість підписів – усі алгоритми цього класу накладають обмеження на максимальну кількість підписів, що можуть бути створені з використанням однієї пари

ключів, однак у сучасних криптосистемах ця кількість може бути дуже високою, що фактично знімає це обмеження;

2) великий розмір підпису – сучасні підписи мають складну структуру, що включає багато елементів.

ЕЦП на основі геш-функцій можна класифікувати наступним чином:

- одноразові (Лампорта [6], Вінтерніца [7 – 9]);
- багаторазові з використанням дерев Мерклі [7];
- багаторазові з поступовим зниженням стійкості (HORS[10], HORST[5], FORS[3], PORS[4]);
- багаторазові з використанням гіпердерев (SPHINCS[5], SPHINCS+[3], Gravity-SPHINCS[4], XMMS^{MT}[11]).

Стаття має наступну структуру: в розд. 2 наводиться опис алгоритмів ЦП Лампорта, Лампорта – Діффі та Вінтерніца, у розд. 3 описано модифіковані алгоритми, у розд. 4 проводиться порівняльний аналіз усіх описаних алгоритмів.

2. Алгоритми одноразового підпису

Перші алгоритми цифрового підпису на базі геш-функцій мали серйозний недолік – одна пара ключів могла бути використана для підпису тільки одного повідомлення, оскільки при підписуванні розкривалася значна частина приватного ключа і його подальше використання ставало небезпечним, ці алгоритми отримали назву одноразових підписів (One-Time Signature – OTS).

До цього класу належать:

- підпис Лампорта (LOTS);
- підпис Лампорта – Діффі (LDOTS);
- підпис Вінтерніца (WOTS);
- модифікації підпису Вінтерніца (WOTS+);
- інші варіанти.

Зауваження 1. В подальшому будемо розглядати узагальнений випадок, вважаючи, що для гешування повідомлення та елементів ключа використовуються різні геш-функції з довжинами вихідних значень m та n відповідно. На практиці, зокрема у найбільш перспективних криптосистемах сімейства SPHINCS для цього використовується одна й та сама функція з довжиною виходу n.

Зауваження 2. Далі під повідомленням мається на увазі геш-значення від фактичного повідомлення, отримане з використанням криптографічної геш-функції $H(M):\{0,1\}^{*}\to\{0,1\}^{m}$, якщо не вказано інше.

2.1. Підпис Лампорта (L-OTS)

Перший алгоритм використання геш-функції для створення підпису запропонований Лампортом в 1979 р. [6]. Схема була побудована наступним чином.

Секретний ключ. Два масиви по m елементів в кожному заповнені випадковими бітовими послідовностями довжини n.

$$SK=\begin{pmatrix} X = (x_0, x_1, \ldots, x_{m-1}) \\ Y = (y_0, y_1, \ldots, y_{m-1}) \end{pmatrix}$$

Відкритий ключ. Два масиви геш-значень елементів секретного ключа.

$$PK=\begin{pmatrix} H(X) = (H(x_0), H(x_1), \ldots, H(x_{m-1})) \\ H(Y) = (H(y_0), H(y_1), \ldots, H(y_{m-1})) \end{pmatrix}$$

Створення підпису. Підпис – масив з m значень елементів секретного ключа, обраних за таким правилом: якщо поточний біт повідомлення, що підписується, дорівнює 0, в підпис включається відповідний елемент з першого масиву секретного ключа, якщо 1 – то з другого.

Таким чином розкривається половина елементів секретного ключа, інша половина повинна бути знищена.

Перевірка підпису. Елементи підпису гешуються і порівнюються з відповідними елементами відкритого ключа.

Зауваження 3. Підпис Лампорта має два недоліки, що заважають його широкому використанню:

- може бути використаний для підпису тільки одного повідомлення;
- має великий розмір.

2.2. Підпис Лампорта-Діффі

Діффі незначно модифікував алгоритм Лампорта, уточнивши вимоги до геш-функцій, що використовуються, а саме:

- для гешування повідомлення повинна використовуватися криптографічна геш-функція;
- геш-функція, що використовується для створення відкритого ключа та перевірки підпису, повинна бути односпрямованою.

Було змінено позначення елементів секретного ключа:

$$SK = \begin{pmatrix} X_0 = (x_{0,0}, x_{0,1}, \ldots, x_{0,m-1}) \\ X_1 = (x_{1,0}, x_{1,1}, \ldots, x_{1,m-1}) \end{pmatrix}$$

Інші складові алгоритму залишилися без змін.

2.3. Підпис Вінтерніца (W-OTS)

З метою зменшення розмірів підпису Вінтерніц запропонував [7] використовувати ланцюгову (ітеративну) геш-функцію, що дозволяє підписувати одним значенням декілька біт повідомлення. Розглянемо цей алгоритм.

Параметр Вінтерніца – кількість біт повідомлення, що будуть одночасно підписані, в деяких джерелах параметром Вінтерніца називають значення 2^w, будемо дотримуватися першого варіанта.

Вводяться наступні додаткові параметри:

t_1 – блочна довжина повідомлення;

t_2 – блочна довжина контрольної суми;

t – блочна довжина повідомлення з контрольною сумою.

Секретний ключ. Масив з t випадкових n-бітових послідовностей

$SK = (sk_0, sk_1, \ldots, sk_{t-1}), sk_i = \{0,1\}^n$.

Для економії пам'яті в якості секретного ключа можна використовувати одну випадкову послідовність $x = \{0,1\}^n$, яка при необхідності буде розгорнута у SK за допомогою генератора псевдовипадкових послідовностей. Це незначно ускладнює створення підпису.

Відкритий ключ. Ітеративно прогешовані $(2^w - 1)$ разів елементи секретного ключа.

$PK = (pk_0, pk_1, \ldots, pk_{t-1}), \quad pk_i = f^{2^w-1}(sk_i)$.

Створення підпису.

Вхідні дані: M, H, SK.

Вихідні дані: σ.

1) Повідомлення розбивається на t_1 блоків довжиною w біт $H(M) = (h_0, h_1, \ldots, h_{t_1-1})$.

2) Обчислюється контрольна сума

$$S = \sum_{i=0}^{t_1} 2^w - 1 - h_i = (s_0, s_1, \ldots, s_{t_2-1}).$$

3) Контрольна сума додається до повідомлення

$B = H(M) \,||\, S = (h_0, h_1, \ldots, h_{t_1-1}, s_0, s_1, \ldots, s_{t_2-1}) = (b_0, b_1, \ldots, b_{t-1})$, де || означає конкатенацію.

4) Обчислюється підпис

$\sigma = (\sigma_1, \sigma_0, ..., \sigma_{t-1}) = (f^{b_0}(sk_0), f^{b_1}(sk_1), ..., f^{b_{t-1}}(sk_{t-1}))$.

Перевірка підпису.

Вхідні дані: M, H, PK, σ.

Вихідні дані: true або false.

1) Аналогічно пунктам 1-3 алгоритму створення підпису обчислюється

$B' = (b'_0, b'_1, ..., b'_{t-1})$.

2) Обчислюється

$Z = (z_0, z_1, ..., z_{t-1}) = (f^{2^w - b_1}(\sigma_0), f^{2^w - b_0}(\sigma_1), ..., f^{2^w - b_{t-1}}(\sigma_{t-1}))$.

3) Якщо $Z = PK$, підпис коректний.

Існують різні модифікації ЕЦП Вінтерніца, зміни в основному стосуються ітеративної функції, що використовується, серед них:

- перед черговим гешуванням на число операцією XOR накладається бітова маска, це дозволяє знизити вимоги до геш-функції [9 – 11];
- використання ключової геш-функції, де результат попередньої ітерації використовується в якості ключа [8].

3. Модифіковані алгоритми

Розглянемо декілька модифікацій класичних алгоритмів.

3.1. Підпис Лампорта-Вінтерніца

В [12] запропоновано модифікацію класичних схем Лампорта та Вінтерніца, яка потребує більше детального аналізу.

Розглянемо дві варіації вдосконаленого підпису:

- Альтернативний підпис Лампорта;
- Альтернативний підпис Вінтерніца.

Альтернативний підпис Лампорта.

Сутність даного алгоритму полягає в зменшенні розмірів ключів та підпису за рахунок зменшення кількості біт повідомлення, що підписуються.

Загальносистемні параметри:

m – довжина геш-значення повідомлення;

w – кількість бітів, які підписуються одним елементом ключа;

n – довжина елементів ключів та підпису;

$t = \left\lceil \frac{m}{w} \right\rceil$ – кількість блоків, на які буде розбито повідомлення, а також кількість елементів ключів, що будуть для цього використані;

$H_c : \{0,1\}^* \to \{0,1\}^m$ - криптографічна геш-функція;

$H : \{0,1\}^n \to \{0,1\}^n$ – односпрямована геш-функція.

Секретний ключ.

Два масиви з *t* випадкових *n*-бітових рядків.

$$SK = \begin{pmatrix} X_0 = (x_{0,0}, x_{0,1}, \ldots, x_{0,t-1}) \\ X_1 = (x_{1,0}, x_{1,1}, ..., x_{1,t-1}) \end{pmatrix}$$

Відкритий ключ.

Два масиви геш-значень секретного ключа SK.

$$PK = \begin{pmatrix} H(X_0) = (H(x_{0,0}), H(x_{0,1}), \ldots, \mathrm{H}(x_{0,t-1})) \\ H(X_1) = (H(x_{1,0}), H(x_{1,1}), ..., H(x_{1,t-1})) \end{pmatrix}$$

Створення підпису:

Геш-повідомлення розбивається на t блоків по w біт (якщо m не кратно w, у кінець додається необхідна кількість нулів).

$H(M) = (h_0, h_1, ..., h_t)$.

Відповідно до старшого біту h_i в підпис додається відповідний елемент з X_0 чи X_1.

Перевірка підпису:

Елементи підпису гешуються та порівнюються з відповідними елементами відкритого ключа.

Альтернативний підпис Вінтерніца.

Сутність полягає в об'єднанні ідей Лампорта і Вінтерніца: секретний та відкритий ключі складаються з двох масивів і відкритий обчислюється з приватного за рахунок циклічного гешування. Оскільки використовується циклічне гешування для захисту від підробки використовується контрольна сума аналогічно WOTS.

Опис алгоритму.

Загальносистемні параметри:

- H, f, w, t, t_1, t_2 – аналогічно звичайному підпису Вінтерніца

Секретний ключ.

Два масиви з t–1 випадкових n-бітових послідовностей

$$SK = \begin{pmatrix} (sk_{0,0}, sk_{0,1}, ..., sk_{0,t-1}) \\ (sk_{1,0}, sk_{1,1}, ..., sk_{1,t-1}) \end{pmatrix}, sk_{i,j} = \{0,1\}^n .$$

Відкритий ключ.

Ітеративно прогешовані $2^{w-1}-1$ разів елементи секретного ключа

$$PK = \begin{pmatrix} (pk_{0,0}, pk_{0,1}, ..., pk_{0,t-1}) \\ (pk_{1,0}, pk_{1,1}, ..., pk_{1,t-1}) \end{pmatrix}, \quad pk_{i,j} = f^{2^{w-1}-1}(sk_{i,j}) .$$

Створення підпису.

Вхідні дані: M, H, SK.

Вихідні дані: σ.

1) Повідомлення розбивається на t_1 блоків довжиною w біт (з метою зробити довжину повідомлення кратну w до повідомлення додається необхідна кількість нульових біт)

$H(M) = (h_0, h_1, ..., h_{t_1-1})$.

2) Обчислюється контрольна сума

$$S = \sum_{i=0}^{t_1} 2^w - 1 - h_i = (s_0, s_1, ..., s_{t_2}) .$$

3) Контрольна сума додається до повідомлення

$B = H(M) \,||\, S = (h_0, h_1, ..., h_{t_1-1}, s_0, s_1, ..., s_{t_2-1}) = (b_0, b_1, ..., b_{t-1})$, де || означає конкатенацію.

4) Для кожного з блоків виділяють старший та молодші біти: $b_i = bh_i \,||\, bl_i$

5) Обчислюється підпис: в залежності від значення старшого біту обирається відповідний елемент з першої чи другої частини приватного ключа та гешується у відповідності до значення молодших біт.

$$\sigma = (\sigma_1, \sigma_0, ..., \sigma_{t-1}) = (f^{bl_0}(sk_{bh_0,0}), f^{bl_1}(sk_{bh_1,1}), ..., f^{bl_{t-1}}(sk_{bh_{t-1},t-1})) .$$

Перевірка підпису.

Вхідні дані: M, H, PK, σ.

Вихідні дані: true або false.

1) Аналогічно пунктам 1-3 алгоритму створення підпису обчислюється $B' = (b'_0, b'_1, ..., b'_{t-1})$.

2) Обчислюється $Z = (z_0, z_1, ..., z_{t-1}) = (f^{2^{w-1}-bl_1}(\sigma_0), f^{2^{w-1}-bl_0}(\sigma_1), ..., f^{2^{w-1}-bl_{t-1}}(\sigma_{t-1}))$.

3) Обчислюється $T = (pk_{bh'_0,0}, pk_{bh'_1,1}, ..., pk_{bh'_{t-1},t-1})$.

4) Якщо $Z = T$, підпис коректний.

3.2. Розширений підпис Лампорта

В класичному варіанті алгоритму Лампорта кожному біту відповідає один з двох можливих станів (елементів підключів), що призводить до значних витрат: кількість елементів підпису дорівнює кількості бітів в геш-значенні повідомлення, що підписується. Зменшення довжини геш-значення призводить до зниження стійкості. Пропонується об'єднувати біти геш-значення повідомлення в групи та ставити кожній групі бітів у відповідність по одному елементу з секретного ключа. Для цього необхідно збільшити кількість підключів до 2^w, де w – довжина групи, вибір підключа для поточного елементу здійснюється відповідно до бітового значення конкретної групи бітів. Назвемо це розширеним алгоритмом Лампорта.

Загальносистемні параметри.

Криптографічна геш-функція $H_c : \{0,1\}^* \to \{0,1\}^m$.

Односпрямована геш-функція $H : \{0,1\}^n \to \{0,1\}^n$.

w – довжина групи бітів, яка підписується одним значенням.

Секретний ключ.

2^w масиви по m/w випадкових n-бітових рядків.

$SK = \left(X_0, X_1, ..., X_{2^w-1}\right)$;

$X_i = (x_{i,0}, x_{i,1}, \ldots, x_{i,(m-1)/w})$.

Відкритий ключ.

2^w масиви по m / w геш-значень елементів секретного ключа.

$PK = H(SK) = \left((H(X_0), H(X_1), \ldots, H(X_{2^w-1}))\right)$;

$H(X_i) = (H(x_{i,0}), H(x_{i,1}), \ldots, H(x_{i,(m-1)/w}))$.

Створення підпису.

Вхідні дані: SK.

Вихідні дані: σ.

Підпис – масив з m / w значень секретного ключа, які обираються відповідно до пар бітів повідомлення.

$H_c(M) = \{h_0, h_1, ..., h_{(m-1)/w}\}, \ h_i = \{0,1\}^w$;

$\sigma = \left(x_{h_0,0}, x_{h_1,1}, ..., x_{h_{(m-1)/w},(m-1)/w}\right)$.

Перевірка підпису.

Вхідні дані: PK, σ.

Вихідні дані: true або false.

Елементи підпису гешуються і порівнюються з відповідними елементами відкритого ключа.

$H'_c(M) = \{h'_0, h'_1, ..., h'_{(m-1)/w}\}$;

$H(\sigma) = \left(H(x_{h_0,0}), H(x_{h_1,1}), ..., H(x_{h_{(m-1)/w},(m-1)/w})\right)$;

$Z = \left(H(x_{h'_0,0}), H(x_{h'_1,1}), ..., H(x_{h'_{(m-1)/w},(m-1)/w})\right)$.

Якщо $H(\sigma) = Z$ підпис коректний.

4. Аналіз параметрів одноразових підписів

До основних параметрів, за якими можливо порівнювати алгоритми ЕЦП незалежно від їх математичної бази відносяться:

- стійкість до криптоаналізу;
- розміри ключів та підписів;
- обчислювальна складність генерації ключів, створення та перевірки підпису.

У контексті одноразових підписів узагальнено можна виділити два класи атак:

- при відомому публічному ключі;
- при відомому публічному ключі та підписі.

Зауваження 4. Більш складні атаки, зокрема із вибором або адаптивним вибором повідомлення, розглядатися не будуть, оскільки наявніть декількох підписів, створених із використанням однієї ключової пари є неможливою за визначенням одноразового підпису. Також виникнення такої пари підписів свідчить про порушення у роботі схеми підпису і призводить до миттєвого зниження стійкості системи.

До другого класу належить атака типу «екзестенційна підробка», що може бути застосовано до довільного алгоритму підпису, а саме знаходження другого прообразу до геш-значення підписаного повідомлення. При використанні криптографічної геш-функції її складність складає m біт та не може бути зменшена за рахунок накопичення аналітиком великої кількості повідомлень, оскільки, за визначенням, ключі одноразового підпису використовуються лише один раз. З іншого боку особливості підписів на основі геш-функцій дозволяють зменшити складність пошуку підходящого повідомлення, геш якого співпадає з підписаним лише частково. Детальний аналіз стосовно кожного з алгоритмів наводиться далі.

4.1. Аналіз підпису Лампорта

1) Стійкість.

а) Атака при відомому відкритому ключі.

Для успішного втілення подібної атаки зловмиснику необхідно знайти перший чи другий прообраз для m n-бітних геш-значень (можливістю коллізій між елементами приватного ключа знехтуємо, що для його генерації використовувався генератор з необхідними криптографічними властивостями). Якщо використовується криптографічна геш-функція, то складність такої атаки складає 2^{m*n}, що відповідає стійкості $m*n$ біт. Наприклад, якщо $m = n = 256$, стійкість алгоритму складає 65536 біт.

б) Атака при відомому відкритому ключі та підписі.

Зловмисник може спробувати знизити складність атаки «екзистенційна підробка», а саме пошуку другого прообразу для підписаного повідомлення, підібравши повідомлення, геш якого співпадає з підписаним лише частково, наприклад, співпадають $(m–k)$ біт. Однак в цьому випадку йому буде необхідно знайти прообраз (перший чи другий) для кожного невідомого елементу відкритого ключа, тобто зниження складності пошуку повідомлення на 1 біт призводить до збільшення складності створення підробного підпису на n біт. Складність такої атаки буде становити $(m – k + n*k = m + (n – 1)*k)$ біт.

Таким чином, стійкість криптоалгоритму складає не менше m біт. Якщо невикористані елементи секретного ключа не були знищенні під час створення підпису і частина з них стала відома зловмиснику, складність підробки зменшується. Кожен зкомпрометований елемент фактично знижує ентропію геш-значення повідомлення на 1 біт, якщо криптоаналітику відомі k додаткових елементів секретного ключа, то складність підробки складає $(m–k)$ біт.

2) Розміри підпису та ключа.

Довжина секретного та відкритого ключів у схемі підпису Лампорта визначається як $2*m*n$ біт, довжина ЕП $m*n$ біт. Результати оцінки розмірів секретних та відкритих одноразових ключів та розмірів ЕП для механізмів Лампорта та Лампорта – Діффі в залежності від параметрів безпеки наведені в табл. 1.

Таблиця 1

Розміри секретних та відкритих ключів
та ЕП для механізму Лампорта в кілобайтах

Параметр безпеки (n)	Розмір секретного ключа	Розмір відкритого ключа	Розмір ЕП
128	4	4	2
192	9	9	4.5
256	16	16	8
384	36	36	18
512	64	64	32

Розміри підпису Лампорта становлять від одиниць до десятків кілобайт в залежності від рівня стійкості.

3) Обчислювальна складність.

Створення пари ключів підпису Лампорта вимагає генерації випадкових значень та їх гешування, створення підпису вимагає тільки відбору необхідних значень, перевірка підпису вимагає тільки гешування. У випадку, якщо підписувач за якихось причин не зберігає публічний ключ, для створення підпису йому необхідно прогешувати відповідні елементи приватного ключа. Обчислювальну складнсть механізму наведено в табл. 2.

Таблиця 2

Обчислювальна складність механізму Лампорта

Параметр	Генерація ключів	Створення підпису	Перевірка
Генерація випадкового значення	$2m$	-	-
Обчислення геш-функції	$2m$	$-/m$	m

Усе зазначене також актуально для підпису Лампорта – Діффі, що фактично відрізняється тільки позначеннями та вимогами до геш-функцій.

4.2. Аналіз підпису Вінтерніца

Детальний аналіз стійкості підпису Вінтерніца та його модифікацій проведено у роботах [8, 9, 13]. В даній роботі ми будемо використовувати спрощену модель.

1) Стійкість.

а) Атака при відомому відкритому ключі.

Розглянемо три можливі для зловмисника випадки: найгірший, звичайний та найгірший, складність пошуку повідомлення, геш якого має необхідні властивості, не враховуємо.

В найгрішному випадку геш-значення підробного повідомлення містить тільки нульові біти, в такому випадку зловмиснику необхідно знайти прообрази для декількоразового гешування t_1 елементів (ймовірністю колізій знехтуємо), тобто стійкість складає не менше $n * t_1$ біт.

У звичайному (найбільш ймовірному) випадку значення груп пікселів будуть рівномірно розподілені в діапазоні $[0;2^w–1]$, тобто максимальне значення $2^w–1$, якому відповідає елемент відкритого ключа приймуть близько $(t_1/(2^w–1))$. Складність підробки при цьому складає не менше $(t_1 – t_1/(2^w–1))*n$ біт, а з урахуванням елементів, що відповідають контрольній сумі, стійкість стає вищою.

В найкращому для зловмисника випадку геш-значення підробного повідомлення містить тільки одиничні біти, в такому випадку t_1 елементів підпису дорівнюють елементам відкритого ключа, що відомий зловмиснику. Однак залишаються t_2 елементів, що відповідають контрольній сумі, яка в цьому випадку дорівнює нулю. Таким чином, зловмиснику необхідно знайти прообрази для декількоразового гешування t_2 елементів. Стійкість до цієї атаки дорівнює не менше t_2*n біт.

б) Атака при відомому відкритому ключі та підписі.

Зловмисник може знизити складність пошуку другого прообразу, підібравши повідомлення, геш якого співпадає з підписаним лише частково. Якщо зловмисник має коректний підпис, то через певну кількість обчислень він зможе створити повідомлення, з геш-значенням $H(M') = (h'_0, h'_1, ..., h'_{t_1-1})$, таким що $h'_i \geq h_i$, таким чином після додаткових ітерацій початковий підпис стане коректним для повідомлення M'. Використання контрольної суми дозволяє захистити підпис від підробки: при збільшені h_i значення контрольної суми зменшується, отже елементи ключа, використані для підписування контрольної суми, повинні бути прогешовані меншу кількість разів, ніж у початковому повідомленні, що зловмисник зробити не може через односторонню природу функції *f*. Таким чином, зловмиснику необхідно знайти прообраз хоча б одного *n*-бітного значення, що призводить до стійкості не менше *n* біт.

2) Розміри підпису та ключа.

Розмір підпису в схемі Вінтерніца дорівнює розміру відкритого ключа та складає *SignSize = t * n* біт. Нехай до повідомлення та елементів ключа застосовується одна й та ж сама криптографічна геш-функція з довжиною геш-значення $n = \{128; 192; 256; 384; 512\}$ біт, параметр Вінтерніца $w = [2, 3, ..., 16]$. Залежність розмірів підпису від *n* та *w* наведено у табл. 3.

Таблиця 3
Залежність розміру підпису Вінтерніца
від *n* та *w* в кілобайтах

N / *w*	128	192	256	384	512
2	1.063	2.367	4.156	9.234	16.313
3	0.719	1.570	2.813	6.188	10.938
4	0.547	1.195	2.094	4.641	8.188
5	0.438	0.984	1.719	3.750	6.625
6	0.375	0.797	1.406	3.094	5.563
7	0.328	0.703	1.219	2.672	4.750
8	0.281	0.609	1.063	2.344	4.125
9	0.266	0.563	0.969	2.109	3.688
10	0.234	0.516	0.875	1.922	3.375
11	0.219	0.469	0.813	1.734	3.063
12	0.203	0.422	0.750	1.594	2.813
13	0.188	0.398	0.688	1.500	2.625
14	0.188	0.375	0.656	1.406	2.438
15	0.172	0.352	0.625	1.313	2.313
16	0.156	0.328	0.563	1.219	2.125

3) Обчислювальна складність.

Для генерації приватного ключа підпису Вінтерніца необхідно згенерувати *t* випадкових *n*-бітних значень, для обчислення публічного ключа необхідно виконати $N = t * (2^w - 1)$ операцій гешування. Створення та перевірка підпису разом фактично повторюють процедуру обчислення публічного ключа, однак обчислювальна складність виконання кожної з цих процедур окремо залежить від повідомлення, що підписується. Залежність кількості гешувань для обчислення відкритого ключа схеми Вінтерніца від *n* та *w* наведено у табл. 4.

Зауваження 5. З таблиці видно, що на практиці можна використовувати лише невеликі значення параметра Вінтерніца, оскільки кількість ітерацій для генерації відкритого ключа, створення та перевірки підпису експоненційно залежить від даного параметру. Оптимальним, на наш погляд, є значення *w* = 4, розмір підпису в такому випадку складає 0,5 – 8 кілобайт та потребує близько 500 – 2000 операцій гешування, в залежності від рівня стійкості, що є прийнятною величиною. Також розбиття даних, що підписуються, на 4-бітні блоки легко реалізується як програмно, так і апаратно.

Таблиця 4

Залежність кількості гешувань для обчислення відкритого ключа підпису Вінтерніца від *n* та *w*

N \ *w*	128	192	256	384	512
2	204	303	399	591	783
3	322	469	630	924	1225
4	525	765	1005	1485	1965
5	868	1302	1705	2480	3286
6	1512	2142	2835	4158	5607
7	2667	3810	4953	7239	9652
8	4590	6630	8670	12750	16830
9	8687	12264	15841	22995	30149
10	15345	22506	28644	41943	55242
11	28658	40940	53222	75739	100303
12	53235	73710	98280	139230	184275
13	98292	139247	180202	262112	344022
14	196596	262128	344043	491490	638937
15	360437	491505	655340	917476	1212379
16	655350	917490	1179630	1703910	2228190

4.3. Аналіз альтернативного підпису Лампорта

Вдосконалений алгоритм відрізняється від класичного підпису Лампорта тим, що підписуються не всі біти геш-значення, а лише кожен *w*-й, що є еквівалентним до використання у підписі геш-функції з більш коротким вихідним значенням.

1) Стійкість.

Для цього алгоритму справедливі ті ж самі припущення, що і для стандартного підпису Лампорта.

а) Атака при відомому відкритому ключі.

В цьому випаку зловмиснику необхідно *t* разів знайти прообраз для *n*-бітової геш-функції, що за умови стійкості до пошуку прообразів еквівалентно вгадуванню *t*n* випадкових біт.

б) Атака при відомому відкритому ключі та підписі.

Для класичної схеми Лампорта складність пошуку другого прообразу дорівнює 2^n, в модифікованій схемі при підписі враховуються лише *t* бітів геш-значення, відповідно складність пошуку повідомлення, що дасть геш зі співпадаючими відповідними бітами, дорівнює 2^t.

Криптоаналітик може спростити задачу пошуку повідомлення, яке має відповідний геш, дозволивши відмінності у «критичних» *t* бітах, при цьому, як і у звичайному підписі Лампорта, відмінність у одному біті вимагає пошуку прообразу для одного з елементів відкритого ключа, складність цієї задачі 2^n. Стійкість при ігноруванні *k* критичних біт складатиме $t + (n - 1)*k$.

Зауваження 6.

1. Найнебезпечнішою є друга атака, яка унеможливлює використання великих значень *w*.

2. Доцільність використання альтернативного підпису Лампорта викликає сумніви через його уразливість.

2) Розміри підпису та ключа.

Альтернативний підпис Лампорта повністю еквівалентний звичайному підпису Лампорта з довжиною геш-значення повідомлення *t* біт.

Розміри приватного та публічного ключів становлять 2**t***n* біт. Розміри підпису *t***n* біт.

3) Обчислювальна складність.

Аналогічно стандартному агоритму Вінтерніца генерація ключа включає генерацію 2t випадкових значень та їх гешування. Створення та перевірка підпису вимагає t гешувань кожне.

4.4. Аналіз альтернативного підпису Вінтерніца

1) Стійкість

Властивості альтернативний підпису Вінтерніца в цілому схожі на властивості звичайного підпису Вінтерніца з деякими уточненнями.

а) Атака при відомому відкритому ключі.

Аналогічно звичайному підпису Вінтерніца можна виділити декілька випадків складності підробки відносно бітів геш-значення підробного повідомлення – усі біти 0, біти рівномірно розподілені, усі біти 1. Як і у стандартній схемі, стійкість до підробки у найгіршому випадку складає $n * t_1$ біт, у найкращому $n * t_2$ біт. Оскільки обидві частини відкритого ключа відомі зловмиснику, він може обирати довільний елемент у кожній парі, відповідно до повідомлення, що підписується.

б) Атака при відомому відкритому ключі та підписі.

Аналогічно механізму Лампорта криптоаналітик може спростити пошук другого прообразу для геш-значення повідомлення, ігноруючи відмінності у бітах, що визначають вибір елементу з першої чи другої підмножини. В цьому випадку для створення коректного підпису необхідно знайти невідомі елементи приватного ключа. Знаходження k елементів приватного ключа означає знаходження прообразів для k значень ітеративної геш-функції.

Аналогічно механізму Вінтерніца можна підібрати повідомлення, усі блоки геш-значення якого будуть більше за блоки підписаного повідомлення, як було зазначено раніше, від цього захищає використання контрольної суми. Тобто стійкість складає не менше n біт.

Таким чином, зміна одного біту геш-значення у частині блоку, що відповідає за Лампортову складову, або у частині, що відповідає за складову Вінтерніца, неодмінно вимагає знаходження хоча б одного прообразу для геш-функції і стійкість залишається не нижче n біт.

2) Розміри підпису та ключа.

Розмір підпису альтернативного алгоритму Внітерніца залишився незмінним і складає $SignSize = t * n$. Розміри ключів збільшилися вдвічі і дорівнюють $KeySize = 2 * t * n$.

Залежність розмірів ключів від n та w наведено у табл. 5.

Таблиця 5

Залежність розміру ключів (в кілобайтах) альтернативного підпису Вінтерніца від n та w

N \ w	128	192	256	384	512
2	2.125	4.734	8.313	18.469	32.625
3	1.438	3.141	5.625	12.375	21.875
4	1.094	2.391	4.188	9.281	16.375
5	0.875	1.969	3.438	7.500	13.250
6	0.750	1.594	2.813	6.188	11.125
7	0.656	1.406	2.438	5.344	9.500
8	0.563	1.219	2.125	4.688	8.250
9	0.531	1.125	1.938	4.219	7.375
10	0.469	1.031	1.750	3.844	6.750
11	0.438	0.938	1.625	3.469	6.125
12	0.406	0.844	1.500	3.188	5.625
13	0.375	0.797	1.375	3.000	5.250
14	0.375	0.750	1.313	2.813	4.875
15	0.344	0.703	1.250	2.625	4.625
16	0.313	0.656	1.125	2.438	4.250

3) Обчислювальна складність.

Кількість ітерацій ланцюгової функції для обчислення публічного ключа в альтернативному підписі Вінтерніца $N_{key} = N_{key\_WOTS} - t$. Кількість ітерацій ланцюгової

функції для створення та перевірки підпису $N_{sign} = (N_{sign\_WOTS} - t) / 2$. Залежність кількості гешувань для створення та перевірки підпису та обчислення відкритого ключа від n та w наведено у табл. 6, 7.

Таблиця 6

Залежність кількості гешувань для підпису від n та w

N / w	128	192	256	384	512
2	68	101	133	197	261
3	138	201	270	396	525
4	245	357	469	693	917
5	420	630	825	1200	1590
6	744	1054	1395	2046	2759
7	1323	1890	2457	3591	4788
8	2286	3302	4318	6350	8382
9	4335	6120	7905	11475	15045
10	7665	11242	14308	20951	27594
11	14322	20460	26598	37851	50127
12	26611	36846	49128	69598	92115
13	49140	69615	90090	131040	171990
14	98292	131056	172011	245730	319449
15	180213	245745	327660	458724	606171
16	327670	458738	589806	851942	1114078

Таблиця 7

Залежність кількості гешувань для обчислення відкритого ключа від n та w

N / w	128	192	256	384	512
2	136	202	266	394	522
3	276	402	540	792	1050
4	490	714	938	1386	1834
5	840	1260	1650	2400	3180
6	1488	2108	2790	4092	5518
7	2646	3780	4914	7182	9576
8	4572	6604	8636	12700	16764
9	8670	12240	15810	22950	30090
10	15330	22484	28616	41902	55188
11	28644	40920	53196	75702	100254
12	53222	73692	98256	139196	184230
13	98280	139230	180180	262080	343980
14	196584	262112	344022	491460	638898
15	360426	491490	655320	917448	1212342
16	655340	917476	1179612	1703884	2228156

Зауваження 7.

1. Вдосконалений алгоритм потребує менше обчислень для створення та перевірки підпису, однак більше пам’яті для зберігання секретного та відкритого ключів.

2. Оскільки відкритий ключ неможливо повністю обчислити з підпису, цей ЕЦП не так зручно використовувати в схемах з геш-деревами – разом з підписом необхідно передавати іншу половину елементів відкритого ключа, що подвоює реальний розмір підпису.

4.5. Аналіз розширеного підпису Лампорта

1) Стійкість.

а) Атака при відомому відкритому ключі.

Аналогічно звичайному підпису Лампорта, для підробки розширеного алгоритму необхідно знайти прообрази для усіх елементів відкритого ключа, що будуть використані. Стійкість дорівнює $m / w * n$ біт.

б) Атака при відомому відкритому ключі та підписі.

Так само, як і для класичної схеми, криптоаналітик повинен або виконати атаку типу «єкзистенційна підробка» зі складністю 2^m, або віднайти прообрази до елементів ключа, що відповідають зміненим бітам.

2) Розміри ключів та підпису.

Довжина секретного та відкритого ключів у модифікованому алгоритмі Лампорта визначається як $2^w * (m / w) * n$, довжина ЕП $(m / w) * n$. Результати оцінки розмірів секретних та відкритих одноразових ключів та розмірів ЕП для розширеного алгоритму Лампорта в залежності від параметрів безпеки наведені в табл. 8.

Таблиця 8

Залежність розміру ключів та підписів (в кілобайтах) розширеного підпису Лампорта від *n* та *w*

	Ключ					Підпис				
N \ *w*	128	192	256	384	512	128	192	256	384	512
2	4	9	16	36	64	1,00	2,25	4,00	9,00	16,00
3	5,333	12	21,333	48	85,333	0,67	1,50	2,67	6,00	10,67
4	8	18	32	72	128	0,50	1,13	2,00	4,50	8,00
5	12,8	28,8	51,2	115,2	204,8	0,40	0,90	1,60	3,60	6,40
6	21,333	48	85,333	192	341,333	0,33	0,75	1,33	3,00	5,33
7	36,571	82,286	146,286	329,143	585,143	0,29	0,64	1,14	2,57	4,57
8	64	144	256	576	1024	0,25	0,56	1,00	2,25	4,00
9	113,778	256	455,111	1024	1820,44	0,22	0,50	0,89	2,00	3,56
10	204,8	460,8	819,2	1843,2	3276,8	0,20	0,45	0,80	1,80	3,20
11	372,364	837,818	1489,45	3351,27	5957,82	0,18	0,41	0,73	1,64	2,91
12	682,667	1536	2730,67	6144	10922,7	0,17	0,38	0,67	1,50	2,67
13	1260,31	2835,69	5041,23	11342,8	20164,9	0,15	0,35	0,62	1,38	2,46
14	2340,57	5266,29	9362,29	21065,1	37449,1	0,14	0,32	0,57	1,29	2,29
15	4369,07	9830,4	17476,3	39321,6	69905,1	0,13	0,30	0,53	1,20	2,13
16	8192	18432	32768	73728	131072	0,13	0,28	0,50	1,13	2,00

3) Обчислювальна складність.

Генерація приватного ключа розширеної схеми Лампорта еквівалентна генерації $2^m * m / w$ *n*-бітних значень. Для обчислення відкритого ключа необхідно прогешувати кожен з елементів приватного ключа. У табл. 9 наведена залежність кількості гешувань для обчислення відкритого ключа від *n* та *w*.

Таблиця 9

Залежність кількості гешувань для обчислення відкритого ключа від *n* та *w*

N \ *w*	128	192	256	384	512
2	256	384	512	768	1024
3	342	512	683	1024	1366
4	512	768	1024	1536	2048
5	820	1229	1639	2458	3277
6	1366	2048	2731	4096	5462
7	2341	3511	4682	7022	9363
8	4096	6144	8192	12288	16384
9	7282	10923	14564	21846	29128
10	13108	19661	26215	39322	52429
11	23832	35747	47663	71494	95326
12	43691	65536	87382	131072	174763
13	80660	120990	161320	241980	322639
14	149797	224695	299594	449390	599187
15	279621	419431	559241	838861	1118482
16	524288	786432	1048576	1572864	2097152

Висновки

Підписи на основі геш-функцій є перспективним класом постквантових асиметричних криптоалгоритмів. Важливим компонентом криптосистем сімейства SPHINCS є одноразові підписи, зокрема підпис Вінтерніца.

В рамках роботи були проаналізовані загальновідомі одноразові ЕЦП – Лампорта, Лампорта – Діффі, Вінтерніца – та ряд можливих модифікацій, які за певних умов дозволяють досягнути кращих результатів. Особливо цікавим є розширений підпис Лампорта, що зберігає обчислювальну складність та розміри ключів оригінального алгоритму і при цьому дозволяє вдвічі зменшити розмір підпису. Проте, він не має важливої переваги підпису Вінтерніца – можливості повного обчислення публічного ключа з підпису, що є особливо важливим при використанні алгоритму у багаторівневих структуруах гіпердерев, зокрема в підписах сімейства SPHINCS.

Список літератури:

1. [Електронний ресурс] https://csrc.nist.gov/projects/post-quantum-cryptography.
2. Jean-Phillippe Aumasson and Guillaume Endignoux.: Gravity- SPHINCS – Submission to the NIST's post-quantum cryptography standardization process. (2017).
3. Daniel J. Bernstein et al.: SPHINCS+ – Submission to the NIST's post-quantum cryptography standardization process. (2019).
4. [Електронний ресурс] https://csrc.nist.gov/Projects/post-quantum-cryptography/round-3-submissions.
5. Daniel J. Bernstein et al. Sphincs: practical stateless hash-based signatures. Cryptology ePrint Archive, Report 2014/795, 2014.
6. Leslie Lamport. Constructing digital signatures from a one-way func- tion. Technical. Report SRI-CSL-98, SRI International Computer Science Laboratory, 1979.
7. Ralph C. Merkle. A certified digital signature. In Gilles Brassard, editor, CRYPTO, volume 435 of LNCS, pages 218–238. Springer, 1989.
8. Johannes Buchmann, Erik Dahmen, Sarah Ereth, Andreas Hulsing, and Markus Ruckert. On the security of the Winternitz one-time signature scheme. In A. Nitaj and D. Pointcheval, editors, Africacrypt 2011, volume 6737 of Lecture Notes in Computer Science, pages 363–378. Springer Berlin / Heidelberg, 2011.
9. Andreas Huülsing. W-OTS+ – shorter signatures for hash-based signa- ture schemes. In Amr Youssef, Abderrahmane Nitaj, and Aboul-Ella Hassanien, editors, Progress in Cryptology // AFRICACRYPT 2013, volume 7918 of LNCS, pages 173–188. Springer, 2013.
10. Leonid Reyzin and Natan Reyzin. Better than biba: Short one-time signatures with fast signing and verifying. In Lynn Batten and Jennifer Seberry, editors, Information Security and Privacy, volume 2384 of Lecture Notes in Computer Science, pages 1–47. Springer Berlin / Heidelberg, 2002.
11. Andreas Huülsing, Lea Rausch, and Johannes Buchmann. Optimal parameters for XMSSMT. In Alfredo Cuzzocrea, Christian Kittl, Dimitris E. Simos, Edgar Weippl, and Lida Xu, editors, Security Engineering and Intelligence Informatics, volume 8128 of Lecture Notes in Computer Science, pages 194–208. Springer Berlin Heidelberg, 2013.
12. Ю.І. Горбенко, Т.В. Мельник, І.Д. Горбенко. Аналіз потенційних постквантових механізмів електронних підписів на основі геш-функцій // Радиотехника. 2017. Вып. 189.
13. M.A. Kudinov, E.O. Kiktenko, A.K. Fedorov. Security analysis of the W-OTS+ signature scheme: Updating security bounds – 2020.

Надійшла до редколегії 30.10.2020

Відомості про авторів:

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

Марухненко Олександр Сергійович – студент кафедри безпеки інформаційних технологій, Харківський національний університет радіоелектроніки, Україна, e-mail: oleksandr.marukhnenko@nure.ua, ORCID: https://orcid.org/0000-0002-0583-3752

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

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

УДК 004.056.55 **DOI:10.30837/rt.2020.4.203.02**

М.В. ЄСІНА, канд. техн. наук, Б.С. ШАХОВ

АНАЛІЗ ТА ДОСЛІДЖЕННЯ АЛГОРИТМУ ЦИФРОВОГО ПІДПИСУ PICNIC

Вступ

Важливою особливістю постквантового періоду у криптографії є суттєва невизначеність щодо вихідних даних для криптоаналізу та протидії в частині можливостей квантових комп'ютерів, їх математичного та програмного забезпечення, а також застосування квантового криптоаналізу до існуючих криптоперетворень та криптопротоколів. В якості основних методів обрано математичні методи цифрового підпису (ЦП), що пройшли суттєвий аналіз та обґрунтування в процесі широких досліджень криптографами та математиками на найвищому рівні. Вони детально описані та пройшли дослідження на першому етапі міжнародного конкурсу NIST США. В процесі другого етапу прийнято ряд рішень стосовно об'єднання деяких кандидатів на постквантовий стандарт ЦП [6].

Для подальших досліджень на 2-му етапі залишили 9 кандидатів: CRYSTALS-DILITHIUM, FALCON, GeMSS, LUOV, MQDSS, Picnic, qTESLA, Rainbow та SPHINCS+. Три з них (Dilithium, FALCON, qTeSLA) засновані на стійкості алгебраїчних решіток (Lattice-based), чотири (GeMSS, LUOV, MQDSS, Rainbow) – на основі багатовимірних перетворень (MQ-перетворення), один (SPHINCS+) – на стійкості геш-функції, один (Picnic) – на стійкості геш-функції та блокових потокових шифрів [4].

За результатами досліджень перспективних постквантових криптографічних алгоритмів типу цифровий підпис протягом 2-го раунду конкурсу NIST США було отримано наступні результати – обрані алгоритми-фіналісти та альтернативні алгоритми. У якості алгоритмів-фіналістів були обрані такі алгоритми ЦП як CRYSTALS-DILITHIUM, FALCON та Rainbow. У якості альтернативних алгоритмів – GeMSS, Picnic та SPHINCS+ [7].

Далі у роботі більш детально розглянемо перспективний постквантовий алгоритм ЦП, що входить до переліку альтернативних алгоритмів – Picnic.

1. Опис та параметри алгоритму Picnic

1.1. Опис алгоритму

Алгоритм цифрового підпису Picnic – це схема підпису, яка не використовує теоретико-числових або структурованих припущень складності. Зменшення безпеки відносяться до геш-функцій і симетричних блокових шифрів. Підпис Picnic базується на неінтерактивному нульовому доказі знання секретного ключа. Підписується відкритий текст таким чином (через гешування), що тільки власник секретного ключа може вивести доказ і перевірити текст на правильність. Алгоритм ЦП Picnic має невеликий розмір відкритого ключа, але великі підписи. Підпис як і перевірка підписаного тексту досить повільні. Генерація ключів досить ефективна. Довжина підпису залежить від мультиплікативної складності схеми шифрування і від конкретної методики побудови доказу нульового знання (з області безпечних багатоваріантних обчислень). Picnic має модульну схему проектування. Криптографічні примітиви – геш-функції та блоковий шифр – можуть бути створені різними способами. Представлена конструкція використовує LowMC, блоковий шифр з низькою мультиплікативною складністю. LowMC не вивчався так багато, як AES, і, отже, потребує набагато більшого аналізу. Ефект використання AES замість LowMC в Picnic полягає в розширенні довжини підпису на коефіцієнт, який коливається від 6 до 9, в залежності від розміру блоку. Поліпшення обчислень призведе до зменшення підписів. Варто зазначити, що вимоги безпеки для базового блочного шифру менш суворі, ніж загальні вимоги безпеки блокового шифру, тому що тільки одна (випадковий відкритий текст, шифртекст) пара коли-небудь розкривається [2].

1.2. Порівняння постквантових алгоритмів

В табл. 1 порівнюються алгоритми, що пройшли до другого етапу міжнародного конкурсу NIST США. Алгоритм ЦП Picnic є унікальним серед представлених кандидатів, бо він єдиний заснований на стійкості геш-функції та блокових потокових шифрів сімейства LowMC [7].

З табл. 1 можна зробити висновок, що алгоритм Picnic досить збалансований за усіма критеріями. Але він має набагато більший розмір підпису порівняно з іншими алгоритмами, що у свою чергу безперечно впливає на швидкодію.

Таблиця 1

Порівняння постквантових алгоритмів

Схема підпису	Безпека	Захищеність від часових атак	Цикли підписання	Цикли перевірки підпису	Розмір відкритого ключа, байти	Розмір підпису, байти
Dilithium	125	Так	789	209	1472	2701
FALCON (NTRU-GVP)	>>128	Ні	-	-	1792	1200
qTESLA	98	Так	143402	19284	12582912	2444
GeMSS (HmFEv)	128	Так	1497	15	83100	61
LUOV	128	Так	659000	290000	34100	421
MQDSS	128	Так	8510	5752	72	40952
Rainbow	128	Так	68	22	145500	48
Picnic	128	Так	1034	194	64	195458
SPHINCS+	128	Так	51636	1451	1056	41000

1.3. Параметри Picnic

У цьому розділі коротко описано кожен з наборів параметрів для Picnic.

В табл. 2 наведені параметри для трьох рівнів безпеки L1, L3 і L5, відповідних безпеці AES-128, AES-192 і AES-256. Для кожного з трьох рівнів безпеки існує два алгоритми підпису, які використовують систему перевірки ZKB, засновану на перетворенні Fiat-Shamir (FS): pincic-L1-FS, picnic-L3-FS і picnic-L5-FS та засновану на перетворенні Unruh (UR): picnic-L1-UR, picnic-L3-UR і picnic-L5-UR. Існує також три набори налаштувань, що використовують перетворення FS і систему підтвердження з алгоритму покращення неінтерактивних нульових знань за допомогою додатків для постквантових підписів [2].

Всі параметри обрані так, що очікується, що вони забезпечать S біт безпеки від класичних атак, і як мінімум S/2 біт безпеки від квантових атак [2].

Параметр u, кількість оспорюваних повторень застосовано лише до наборів параметрів picnic2. Параметр N, кількість сторін в імітації MPC завжди 64 для наборів параметрів picnic2 [2, 3].

Для варіантів FS довжина підпису змінюється в залежності від виклику, тому вказується максимально можливий розмір разом із середнім розміром і стандартним відхиленням, що обчислюється за 100 підписами [3].

Таблиця 2

Параметри рівня безпеки

Набір параметрів	S	n	s	r	Hash/KDF	L_h	T	u
picnic-L1-FS	128	128	10	20	SHAKE128	256	219	-
picnic-L1-UR							219	-
picnic2-L1-FS							343	27
picnic-L3-FS	192	192	10	30	SHAKE256	384	329	-
picnic-L3-UR							329	-
picnic2-L3-FS							570	39
picnic-L5-FS	256	256	10	38	SHAKE256	512	438	-
picnic-L5-UR							438	-
picnic2-L5-FS							803	50

Таблиця 3

Розмір ключа і підпису (в байтах) за рівнем безпеки

Набір параметрів	Відкритий ключ	Секретний ключ	Підпис (max)	Підпис (avg., std. dev.)
picnic-L1-FS	32	16	34016	32838, 107
picnic-L1-UR			53945	-
picnic2-L1-FS			13786	12359, 213
picnic-L3-FS	48	24	76764	74134, 198
picnic-L3-UR			121837	-
picnic2-L3-FS			29742	27173, 315
picnic-L5-FS	56	32	132856	128176, 315
picnic-L5-UR			209506	-
picnic2-L5-FS			54732	46282, 613

2. Аналіз відомих атак на алгоритм

У цьому розділі аналізується схема підпису Picnic стосовно відомих атак. По-перше, надається спостереження, що коли ми маємо справу з ідеальними примітивами, Corollary 5.4 вже дає нам перевірену прив'язку до безпеки EUF-CMA (Existentially Unforgeable under Chosen Message Attacks – екзистенційна непідроблюваність при атаках на основі (адаптивно) вибраних повідомлень). Оскільки це примітиви, що створені за допомогою конкретних будівельних блоків, ми розглядаємо конкретні атаки на ці будівельні блоки. У цій схемі використовується класичний підхід, щоб перетворити Σ-протоколи в схеми підпису з випадковою моделлю оракула. На основі того факту, що з моменту введення випадкової моделі оракула не було виявлено жодної атаки, яка виникає з припущення, що геш-функція веде себе як випадкова модель оракула (за виключенням деяких штучних контрприкладів), тому можна стверджувати, що найкращими атаками на підпис є атаки, які роблять недійсними твердження, зроблені для базових симетричних примітивів [2].

Всі криптографічні примітиви, за винятком односторонньої функції LowMC, спираються на SHA-3 функцію SHAKE, визнаний і стандартизований примітив, і вона використовується стандартним способом. Що стосується цих примітивів, то вже досягнуто значної згоди в питаннях безпеки завдяки широкому криптоаналізу всередині спільноти. Тому ці будівельні блоки не розглядаються як центральна поверхня атаки. Покращення атак на ці примітиви також призводить до покращення атак на схему підпису [2].

2.1. Використання та безпека LowMC

Отже, надалі робиться акцент на атаки на односторонню функцію f. По суті функція f може бути будь-якою односторонньою функцією, але в Picnic використовується сімейство блочних шифрів LowMC, так як саме ці блочні шифри дали в результаті найбільш ефективні підписи. Зокрема, потрібно виходити з того, що використання LowMC, як вказано нижче, дає відповідне сімейство односпрямованих функцій $\{f_u\}_{u \in K_к}$. Ця функція використовується для встановлення відповідних відносин між секретними та відкритими ключами. Зокрема, нехай

$$f_u(x) := E(x, u) \quad (1)$$

і нехай E позначає шифрування LowMC щодо одного блоку u на ключі X. Ключі у використаній схемі підпису генеруються наступним чином. По-перше, вибирають ключ шифрування LowMC – x, а також один блок u рівномірно випадковим чином. Потім відкритий ключ підпису pk, а також секретний ключ підпису sk визначаються наступним чином:

$$pk := (y, u) = (f_u(x), u), \; sk := (pk, x). \quad (2)$$

Вибір кількості раундів у LowMC поставляється з показовим запасом безпеки. Для L1 рівня безпеки з 20 раундами найбільш відома атака на 12 раундів. Для L3 рівня безпеки з 30 раундами найбільш відома атака на 19 раундів. Для L5 рівня безпеки з 38 раундів, найбільш

відома атака – 26 раундів. І навіть ці атаки вимагають від зловмисника знання двох пар відкритого зашифрованого тексту для однієї й тієї самої пари ключів, в той час як у використаній схемі підпису зловмисник бачить лише одну пару вводу-виводу для кожного ключа [2].

2.2. Атаки в режимі розрахованому на одного користувача

В режимі, розрахованому на одного користувача, зловмисник завжди бачить тільки одну пару ключів схеми підпису Picnic, тобто одну пару відкритий текст-шифртекст ($f_u(x)$, u) LowMC відносно рівномірно випадкового ключа x і рівномірно випадкового блоку u. Отже, в цьому налаштуванні криптоаналітичні результати для LowMC також безпосередньо застосовані до схеми, що використовується. Слід зазначити, що можна навіть глобально використовувати x для подальшого скорочення розміру ключа pk загальнодоступної версії [2].

2.3. Атаки в режимі розрахованому на багато користувачів

Багатокористувацький режим точніше моделює реальність, тому, що є кілька користувачів, кожен з відкритим ключем, і зловмисник вважається успішним, якщо він може атакувати будь-якого з користувачів.

Багатокористувацький EUF-CMA. Приділяється особлива увага сценаріям атак, які стають можливими при переході до налаштування розрахованого на багато користувачів. Тут зловмисник може побачити багато пар ключів підписання, і варто бути обережним у відношенні більш складних атак, які можуть мати місце. Зокрема – на відміну від атак в режимі, розрахованому на одного користувача, – рішення вибрати незалежний і рівномірно випадковий блок u, будучи криптографічною функцією E (·, u) LowMC, на одну пару підписуючих ключів, виявляється важливим. В цих атаках один з n блочних ключів шифрування може бути відновлений за менший час, ніж час відновлення єдиного ключа і атаки стають дуже ефективними для великого n. Інтуїтивно, випадковий блок вибирає унікальну функцію за користувача і роботу для атаки на одного користувача (функцію) не можна використовувати для одночасної атаки на іншого користувача (функцію). Крім того, Банегас і Бернштейн нещодавно показали, що паралельні атаки пошуку співпадінь також можуть бути застосовані для квантових значень параметрів, які також підтримують випадковий вибір u на користувача. Можна вибрати менше значення, яке буде унікальним для кожного користувача (з потенційним зниженням безпеки), щоб зменшити розмір відкритого ключа. Однак, оскільки відкриті ключі в схемах вже малі (максимум 64 байта), в конструкції використовується повний випадковий блок, щоб бути максимально консервативним [2].

2.4. Атаки із заміною ключа

Це атаки, де є зловмисник, який має підпис σ_A повідомлення M з відкритим ключем pk_A, що дозволяє створити відкритий ключ pk_E (з pk_A) таким чином, що підпис σ_A підтвердиться з ключем pk_E та повідомленням M. Menezes і Smart надають формальну модель для захисту від таких атак, які не покриваються моделлю безпеки EUF-CMA. Безпека від цих типів атак може бути досягнута в цілому. Це було показано в їх роботі, і нижче подана їх теорема.

Теорема 1: Нехай (Gen, Sign, Verify) є EUF-CMA безпечною схемою підпису. Потім, (Gen, Sign', Verify) з Sign': = Sign (sk, pkm) та pk є однозначним кодуванням відкритого ключа є безпечною схемою підпису в налаштуванні, розрахованому на багато користувачів [3].

Вищевикладене призводить, зокрема, до утримання захищеності схем підпису sEUF-CMA. Відкритий ключ додається до повідомлення про підписання, а опис забезпечує однозначне кодування (оскільки відкритий ключ є парою бітових рядків, кодування є тривіальним). Отже, ми маємо наступний наслідок.

Наслідок 1: picnic-FS і picnic-UR забезпечують безпеку в режимі, розрахованому на багато користувачів [5].

2.5. Багатоцільові атаки

Дінур і Надлер описують атаки на Picnic версії 1.0 (набори параметрів picnic-FS і picnic-UR). В той час набори параметрів Picnic2 не були визначені, але атака в рівній мірі відноситься до прямого створення примітивів протоколу KKW. Їхні атаки являють собою багатоцільові атаки, де у атакуючого є список значень виду y_i: = H (x_1),..., y_S: = H (x_S), а відновлення будь-якого з x_i призводить до успішної атаки. Спеціально значення x_i мають довжину k біт, і зловмисник може відновити ключ k біт. Значення y_i можна взяти з [3]:

- одного підпису (у підписі є близько 2^7 значень),
- з декількох підписів при умові одного й того самого підписувача,
- з декількох підписів при умові різних підписувачів.

В атаці Дінура і Надлера значення x_i є параметром, що використовується для кожної сторони, в кожному примірнику MPC [3]. Функція H розширює x_i до випадкової довжини, що використовується під час моделювання протоколу MPC. В Picnic нащадки двох із трьох сторін розкриваються перевіряючому, а в Picnic2 розкриваються n–1 з n. Якщо зловмисник дізнається відсутнього нащадка, він може відновити секретний та загальний ключ підпису. Вихідна довжина залежить від набору параметрів, але завжди перевищує 600 біт. Що робить атаку неочевидною, так це те, що вихід H (випадкової довжини) не розкривається безпосередньо. Вони показують, що це – власність протоколів MPC, яка не робить звичайне поняття безпеки MPC (протокол MPC повинен гарантувати секретність вихідних даних, але припустима деяка хаотичність, якщо через це не виникають проблеми з секретністю даних). Вони також визначають кількість випадкових бітів, які можуть бути відновлені з примірника MPC. У всіх випадках можна ефективно відновити понад k бітів, так що може бути виконано тестування значення кандидата x_i. Однак у бітів від кожної цілі є різні позиції у випадковій довжині, що ускладнює ефективність проведення атаки. При типовій багатоцільовий атаці атакуючий обчислює x_0, обчислює y_0 = H (x_0), потім зрівнює y_0 з y_i, ефективно використовує структури даних (наприклад, геш-таблиця або дерево пошуку). Але тут порівняння довжини кандидата y_0 (з усіма відомими бітами) з цільовою довжиною y_i (де для кожної з них відома підмножина бітів), не є очевидним. Дінур і Надлер показують, що його можна зробити таким і точно кількісно оцінити витрати при різних налаштуваннях. У кращому випадку, коли всі підписи створюються одним підписувачем, їх атаки коштують 2k–7/S (інформація теоретично оптимальна). В інших випадках атака коштує дорожче, але все одно нижче очікуваного рівня безпеки [3].

Пом’якшення наслідків. Версія специфікації 2.0 вносить зміни, щоб пом’якшити ці атаки (у всіх наборах параметрів). Зміна додає додаткову інформацію до входу H (названою *salt*), так, щоб нащадок кандидата x_0, не міг бути перевірений, витримавши порівняння y_0 до всього y_i, оскільки кожний y_0 вираховується з використанням різної *salt*. *Salt* гарантує, що y_0 потрібно буде перерахувати з правильною *salt* перед кожним порівнянням. Для вирішення всіх трьох варіантів атаки *salt* повинна бути унікальною для кожного підпису, для кожного підписувача і для кожного виклику H. Першою зміною є вибір випадкової завади для кожного підпису довжиною 256 біт. Це гарантує, що (з високою ймовірністю) *salt* унікальна. Потім, щоб гарантувати, що *salt* є унікальною у підписах, також включаємо пару лічильників, перше значення відповідає номеру примірника MPC, а друге відповідає номеру виклику H. Спеціалізація вже використовує метод поділу домену, де різні геш-функції створюються для різних цілей наступним чином – $H_i(x)=H(i||x)$. Цей механізм також допомагає гарантувати, що *salt* є унікальною, наприклад при обчисленні дерева нащадків, ми можемо використовувати H_i та при обчисленні дерева Меркле використовувати H_j, і не турбуватися про те, що (salt, counters) пари повторюються в обох деревах. Деякі додаткові дані також повинні бути гешовані, але витрати на ЦП в еталонних показниках суттєво не зросли. Ймовірно, це пов’язано з тим, що геш-входи були короткими для початку, і залишаються короткими (меншими, ніж розмір блока геш-функції), навіть з *salt* [3].

Висновки

1. У ході семінару другого етапу NIST США рекомендував до подальших досліджень 9 криптографічних примітивів типу ЦП. Порівняння постквантових алгоритмів можна дослідити за табл. 1.

2. За результатами досліджень перспективних постквантових криптографічних алгоритмів типу цифровий підпис протягом 2-го раунду конкурсу NIST США було отримано наступні результати – обрані алгоритми-фіналісти та альтернативні алгоритми. У якості алгоритмів-фіналістів обрані такі алгоритми ЦП як CRYSTALS-DILITHIUM, FALCON та Rainbow. У якості альтернативних алгоритмів – GeMSS, Picnic та SPHINCS+.

3. На конкурс NIST США щодо стандарту ЕП було подано механізм ЕП, що ґрунтується на стійкості геш-функції та блокових потокових шифрів (Picnic). Наразі він досліджується на третьому етапі конкурсу NIST США у якості альтернативного алгоритму.

4. Побудова ЕП в алгоритмі Picnic заснована на перетворенні Fiat-Shamir (FS) та на перетворенні Unruh (UR).

5. Оцінка параметрів алгоритму говорить про те, що сам алгоритм досить збалансований за усіма критеріями, але має великий розмір підпису. Спроби зменшення розміру підпису призводять до зменшення безпеки алгоритму.

6. Після аналізу відомих атак на алгоритм можна зробити висновок, що алгоритм є безпечним і його можна рекомендувати для використання.

7. Великою перевагою алгоритму є великий простір для покращення та змін, які постійно проводяться, та коли буде представлена кінцева версія алгоритму, його можна затверджувати для застосування.

Список літератури:

1. Daniel Kales Efficient FPGA Implementations of LowMC and Picnic / Daniel Kales, Sebastian Ramacher, Christian Rechberger, Roman Walch, Mario Werner. Режим доступу: https://eprint.iacr.org/2019/1368.pdf.

2. The Picnic Signature Scheme. Design Document / Melissa Chase, David Derler, Steven Goldfeder, Claudio Orlandi, Sebastian Ramacher, Christian Rechberger, Daniel Slamanig, Greg Zaverucha //. November 29, 2017. Version 1.0. Режим доступу: https://csrc.nist.gov/Projects/post-quantum-cryptography/round-1-submissions.

3. The Picnic Signature Scheme Design Document / Melissa Chase, David Derler, Steven Goldfeder, Jonathan Katz, Vladimir Kolesnikov, Claudio Orlandi, Sebastian Ramacher, Christian Rechberger, Daniel Slamanig, Xiao Wang, Greg Zaverucha. March 30, 2019. Version 2.0. Режим доступу: https://csrc.nist.gov/Projects/post-quantum-cryptography/round-2-submissions.

4. NIST submissions. Picnic. Picnic-FS. Picnic-UR. Non-interactive Proof of Knowledge. Електронний ресурс. Режим доступу: https://pqc-wiki.fau.edu/w/Special:DatabaseHome.

5. Itai Dinur The Picnic Post-Quantum Signature Scheme and its Security Analysis. Режим доступу: https://www.cs.technion.ac.il/~biham/Workshops/Cryptoday/2018/Slides/cryptoday-2018-itai-dinur-picnic.pdf.

6. Горбенко І. Д. Методи, методика та результати порівняльного аналізу кандидатів на постквантовий стандарт електронного підпису / І. Д. Горбенко, О. Г. Качко, М. В. Єсіна, В. А. Пономар // XX Ювілейна Міжнар. наук.-практ. конф. "Безпека інформації в інформаційно-телекомунікаційних системах", 22-24 травня, 2018, м. Буча. С. 96-97.

7. Gorbenko I. Electronic signature mechanisms. The Current State, the Existing Contradictions and Prospects of Practical Use for the Post-Quantum Period / I. Gorbenko, A. Kuznetsov, Yu. Gorbenko, S. Kavun, O. Kachko, M. Yesina // ASC Academic Publishing Minden, Nevada, USA, 2017. 165 p.

Надійшла до редколегії 29.10.2020

Відомості про авторів:

Єсіна Марина Віталіївна – канд. техн. наук, старший викладач кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук, Харківський національний університет імені В. Н. Каразіна, Україна; e-mail: rinayes20@gmail.com, ORCID: https://orcid.org/0000-0002-1252-7606

Шахов Богдан Сергійович – студент кафедри безпеки інформаційних систем і технологій, факультету комп'ютерних наук, Харківський національний університет імені В. Н. Каразіна, Україна; e-mail: bogdanshahov2000@gmail.com

УДК 004.056.5 **DOI:10.30837/rt.2020.4.203.03**

Н.А. ПОЛУЯНЕНКО, канд. техн. наук, Ю.І. ГОРБЕНКО, канд. техн. наук,
В.Э. САФОНЕНКО, А.А. КУЗНЕЦОВ, д-р техн. наук

УТОЧНЕНИЕ ОЦЕНОК ВЕРОЯТНОСТИ УСПЕХА АТАКИ ДВОЙНОЙ ТРАТЫ НА БЛОКЧЕЙН СИСТЕМЫ НА ОСНОВЕ МОДЕЛИ НЕЗАВИСИМЫХ ИГРОКОВ

Введение

Технология блокчейн исследуется во многих инновационных приложениях [1], таких как: криптовалюты [2 – 4]; умные контракты [5, 6]; системы связи [7 – 9]; здравоохранение [10 – 14]; Интернет вещей [15 – 19]; финансовые системы [20 – 23]; разработка программного обеспечения [24 – 26]; электронное голосование [27 – 31]; в [32 – 34] авторы предложили безопасную и легковесную архитектуру на основе блокчейна для умного дома; и многие другие. Институты исследования глобального рынка Gartner и Deloitte выбрали блокчейн в качестве одного из технологических трендов 2017 г. [35]. Построенная на основе блокчейн технологии криптовалюта Bitcoin была оценена как самая эффективная валюта в 2015 г. [36] и самый эффективный товар в 2016 г. [37], а также имела более 400 000 подтвержденных транзакций [38] ежедневно в декабре 2018 и мае 2019 г., что указывает на значительную вовлеченность в данную сферу.

Используя прозрачную и полностью распределенную одноранговую архитектуру блокчейн, приложения выигрывают от модели, в которой возможно только добавление данных, в которой «транзакции» принимаются в блокчейн реестр и при правильном функционировании системы не могут быть модифицированы или удалены. Прозрачность блокчейн систем позволяет хранить общедоступные и неопровержимые записи [39]. Одноранговая блокчейн система обеспечивает проверяемое ведение реестра без централизованного управления, что позволяет решать проблемы единой точки отказа и единой точки доверия [40].

Технология блокчейн позволяет изменить способ реализации всех типов транзакций и предоставляет широкий спектр возможностей в других областях, таких как децентрализованный протокол конфиденциального вычисления (Secure multi-party computation) [41], использование в децентрализованных автономных корпорациях (decentralized autonomous corporation) [42].

Со времени появления технологии блокчейн в 2009 г. (в качестве основного механизма работы сети Bitcoin) она показала многообещающие перспективы применения и привлекла большое внимание ученых и промышленности. Внедрение полнофункциональных языков программирования Turing, позволяют пользователям разрабатывать интеллектуальные контракты, работающие на блокчейне. Благодаря децентрализованному механизму блокчейна интеллектуальные контракты позволяют взаимно не доверяющим пользователям осуществлять обмен данными или транзакциями без необходимости получения каких-либо сторонних доверенных прав.

Однако, несмотря на все перечисленные достоинства, достижение единого состояния во всех распределенных узлах децентрализованной системы является сложной задачей. Согласованные алгоритмы должны быть устойчивы к сбоям узлов, разбиению сети, задержкам сообщений и сообщениям, которые приходят не в порядке очереди и повреждены. Им также приходится иметь дело с корыстными и намеренно вредоносными узлами, которые заинтересованы в некорректной работе сети. Для решения этой проблемы было предложено несколько алгоритмов, называемых консенсусами, каждый из которых реализует набор необходимых предположений, касающихся синхронизации, передачи сообщений, сбоев, вредоносных узлов, производительности и безопасности при обмене сообщениями. Для блокчейн сети достижение консенсуса гарантирует, что все узлы в сети согласовывают единообразное глобальное состояние блокчейн реестра.

Несмотря на функциональные особенности, которые блокчейн привносит в пространство разработки приложений, в последних отчетах подчеркиваются риски безопасности, связанные с этой технологией [15, 43 – 46]. Например, в июне 2016 г. неизвестному злоумышленнику удалось воспользоваться рекурсивной уязвимостью вызовов смарт-контрактов и вывести более 50 миллионов долларов США из «The DAO», децентрализованной автономной организации, которая работает на основе интеллектуальных контрактов, основанных на блокчейне, или заранее запрограммированных правил, управляющих организацией [47, 48]. В августе 2016 г. с биржи Bitfinex в Гонконге были похищены биткойны на сумму 72 миллиона долларов США [49]. В июне 2017 г. Bitfinex также испытал атаку распределенного отказа в обслуживании (DDoS), которая привела к её временной остановке.

Несколько бирж Bitcoin и Ethereum также часто страдают от DDoS-атак и DNS-атак, что затрудняет доступность сервиса для пользователей. Так, блокчейн Bitcoin является мишенью для пылевых или спам-операций, чтобы задержать обработку законных сделок. В мае, августе и ноябре 2017 г. пулы памяти Биткойна были заполнены пылевыми транзакциями, что привело к задержкам в проверке транзакций и увеличению платы за майнинг биткойнов [50]. Например, в результате приостановки транзакции в ноябре 2017 г. была задержана оплата биткойнов на сумму 700 миллионов долларов США [51]. Часто целью таких атак является мотивация пользователей Bitcoin переходить на другие криптовалюты с более быстрым временем обработки транзакций.

Из-за публично проверяемого характера криптовалюты, на основе блокчейна, они уязвимы для некоторых мошеннических действий. Так, MtGox, занимавшийся обменом валюты Bitcoin в Японии, в марте 2014 г. подвергся нападению двух злоумышленников, похитивших биткойны на сумму 460 миллионов долларов США [52, 53]. Злоумышленники собрали полезную информацию из блокчейна Bitcoin и создали фальшивую систему транзакций, чтобы повысить рыночную цену. Из-за такой деятельности, MtGox понес тяжелую потерю, что привело к его банкротству.

Одной из основных атак на блокчейн системы, в протоколах которых используются алгоритмы консенсуса на основе доказательств выполненной работы, является атаки связанные с возможностью проведения двойных расходов. Более того, данный тип атак является конструктивной особенностью таких систем, и от которых не существует абсолютной защиты.

Двойные расходы – это результат успешного расходования одних и тех же средств более одного раза. Предотвращение данной возможности является одной из наиболее важных задач любой цифровой учетной системы. Так, перефразируя фразу из вики биткойна [54], можно утверждать: в блокчейн системе Bitcoin всё (майнинг, доказательство работы, сложность и т.д.) существует для создания истории транзакций, которую невозможно изменить в вычислительном отношении, что делает существующие транзакции необратимыми. Сама возможность удвоения расходов резко ухудшает доверие к системе и ценность решений на её основе.

Двойные траты – это проблема, которая существует с момента появления блокчейн систем, и остается актуальной по сегодняшний день. Для понимания важности и масштабов убытков приведем некоторые инциденты, связанные с удачно реализованными атаками двойного расходования средств.

1. Примеры проведенных атак двойной траты

Печальным побочным эффектом для блокчейн-технологий стал рост числа злоумышленников, использующих публичные блокчейн системы в незаконных целях. Ниже приведены некоторые примеры успешного проведения атак двойных трат.

Один из форков Биткойна, Bitcoin Gold (BTG), дважды подвергся такой атаке в сети:

- с 16 по 18 мая 2018 г. (было похищено 388 000 BTG, убытки составили более 18,6 миллионов долларов США) [55 – 58];

- в 2020 г. (в ходе атаки 23 января проведена реорганизация 14 блоков и 24 января – 15 блоков, убыток составил 7 167 BTG (более 70 000 $ США) ориентировочная стоимость каждой атаки по реорганизации блокчейна составила около 1 700 долларов США) [59, 60].

Неоднократно на протяжении последних нескольких лет были проведены успешные атаки на Ethereum Classic (ETC):

- с 05.01.2019 по 07.01.2019 г., по информации биржи Coinbase [61], было осуществлено 15 реорганизаций цепочки блокчейна Ethereum Classic, 12 из которых содержали двойные траты на общую сумму 219 500 ETC (1,1 миллионов долларов США);

- по информации компании Bitfly, которая является оператором майнинг-пула Ethermine [62] 01.08.2020 г., начиная с блока 10 904 146, блокчейн Ethereum Classic подвергся реорганизации глубиной в 3 693 блоков, что соответствует примерно 12 часам майнинга [63]. Как говорится в сообщении, реорганизация проведена, вероятно, с помощью атаки 51 %. Для проведения атаки злоумышленник арендовал посторонние мощности на сумму 17,5 BTC (192 тысячи долларов США), при этом он вывел на несколько кошельков 807 260 ETC (5,6 миллионов долларов США) [64];

- с 05.08.2020 по 06.08.2020 г. на блоке 10 935 622 блокчейн Ethereum Classic подвергся реорганизации глубиной в 4 236 блоков [65, 66]. Злоумышленник успешно дважды потратил 238 306 ETC (1,68 миллиона долларов США), кроме того, злоумышленник также получил 14 234,30 ETC в качестве награды за найденные блоки [67];

- 30.10.2020 г. также по информации компании Bitfly [68] еще одна атака 51 % состоялась на сеть Ethereum Classic, что повлекло реорганизацию более 7 000 блоков, что соответствует примерно двум дням майнинга. Команда Ethereum Classic порекомендовала [69] майнерам, биржам и другим сервисам на некоторое время установить количество подтверждений транзакций не менее 7 000.

Ориентированная на конфиденциальность криптовалюта Verge (XVG) 22 мая 2018 г. позволила злоумышленнику скрыться с примерно 1,75 миллиона долларов США. Протокол Verge использует ротацию пяти алгоритмов майнинга. Предположительно злоумышленник получил контроль над двумя из них – scrypt и lyra2re (используя ложные временные метки), что позволило практически без труда сформировать блоки и тем самым заставить сеть принять их в основную цепь [70].

Несмотря на то, что на самую большую и популярную блокчейн сеть Bitcoin на сегодняшний день неизвестны удачные реализации атаки двойной траты, но повышение стоимости данной криптовалюты повысило популярность её майнинга, который определяется как использование вычислительной мощности (то есть мощности хеширования) для генерации новых блоков [71]. Увеличенное количество майнеров уменьшило вероятность того, что отдельный майнер сможет добыть новый блок и, следовательно, получить награду. Следовательно, мелкомасштабная добыча стала очень рискованной. Поэтому, как естественная защита от специфического риска, большинство майнеров присоединились к майнинговым пулам. Пулы приобрели такую популярность, что с 2015 г. от 95 до почти 100 процентов мощности хэша (обработки) в сети Bitcoin контролируется пулами. Ситуация аналогична во всех основных криптовалютах [71].

В подтверждение угроз потери децентрализации в наиболее крупных блокчейн системах приведем данные из [72]. В Bitcoin еженедельная мощность майнинга одним объектом никогда не превышала 21 % от общей мощности. В отличие от этого, главный майнер Ethereum никогда не имел менее 21 % мощности майнинга. Более того, четверка лучших майнеров Bitcoin имеет более 53 % средней мощности майнинга. В среднем 61 % еженедельной мощности было разделено только тремя майнерами Ethereum. Хотя майнеры меняют ранги в течение периода наблюдения, каждое место оспаривается лишь несколькими майнерами. В частности, только два майнера Bitcoin и три майнера Ethereum когда-либо занимали высшие позиции. Один и тот же майнинг пул находился на верхнем уровне в течение 29 % времени в Bitcoin и 14 % времени в Ethereum. Более 50 % майнинговых мощностей было распределено

исключительно между восьмью майнерами в Bitcoin и пятью майнерами в Ethereum в течение всего наблюдаемого периода. Даже 90 % майнинговых мощностей, похоже, контролируются только 16 майнерами в Bitcoin и только 11 майнерами в Эфириуме. Следовательно, для поддержки блокчейна обе платформы в значительной степени зависят от очень небольшого числа отдельных объектов майнинга.

Наиболее эффективной защитой от двойных расходов является проверка участниками учетных блокчейн систем включения платежа в блокчейн реестр и дополнительное ожидание нескольких подтверждений. Подтверждения происходят всякий раз, когда формируется новый блок, ссылающийся на цепочку блоков содержащую транзакцию с платежом. Для системы Bitcoin это происходит в среднем каждые 10 минут. До включения транзакции в блок (иногда называемым «нулевым подтверждением») нет никакой гарантии, что транзакция не будет израсходована дважды. Более того, могут быть веские легальные причины для изменения транзакции, главным образом для добавления дополнительных комиссий к «зависшей» транзакции, которая в противном случае могла бы оставаться не добавленной в реестр блокчейна в течение нескольких дней.

Пользователи учетных блокчейн систем могут значительно снизить вероятность проведения успешных атак двойной траты, максимально увеличивая необходимое число подтверждений и, следовательно, время проведения сделки. И хотя это решение просто по своей концепции, его часто чрезвычайно сложно реализовать на практике.

Интересная информация предоставлена в [73], где описываются случаи и механизмы контратак блокчейн сетей на попытку злоумышленников реорганизовать их блокчейн реестр. Так, в статье приходят к выводам, что растущая глубина рынков по аренде хешрейта может ставить под угрозу безопасность криптовалют на основе алгоритма доказательства выполненной работы. В то же время возможность контратак может остановить атакующих от каких-либо действий. Если этого баланса сил достаточно, чтобы защитить цепь, это ведет к вопросу о том, какое именно количество мощностей необходимо для предотвращения атак.

Но, несмотря на то, какую стратегию мы выбираем (увеличения времени подтверждения или возможность проведения контрмер), необходимо иметь четкое представление о мощностях, которые необходимо задействовать (как при потенциальной атаке, так и при проведении защиты) для оптимизации затрачиваемых ресурсов и сокращении потенциальных рисков.

Анализ работ, посвященных количественной оценке вероятности успешного проведения атаки двойной траты на блокчейн системы, подробно описан в [76, 83]. Наиболее известными и цитируемыми являются работы Сатоши Накамото [74] и более точные результаты получены Мени Розенфельдом [75].

В статье приведен сравнительный анализ упомянутых работ с предлагаемой моделью, которая, на наш взгляд, более адекватно описывает реальные процессы консенсуса на основе доказательства выполненной работы, происходящей в блокчейн системах.

2. Корректировка формул С. Накамото та М. Розенфельда на основе модели независимых игроков

2.1. Используемые модели

Упомянутые работы формируют свои выводы на основании модели «разорение игрока». На основе данной модели получается формула для расчета вероятности успешного проведения атаки. В основу этой модели положен факт, что в каждом испытании или выигрывает злоумышленник (формируя очередной блок) или злоумышленник проигрывает и при этом считается, что выигрывает честная сеть (формируя очередной блок). Авторы предполагают, что если блок не сформировал злоумышленник, то в таком случае блок обязательно формирует честная сеть, причем это предположение никак не обосновано.

Мы предлагаем использовать модель «независимых игроков». В данной модели, в отличие от модели «разорение игрока», формирование очередного блока у злоумышленника и

честной сети происходит полностью независимо друг от друга. Пусть вероятность сформировать блок злоумышленником будет q, а честной сетью – p, отказавшись от обязательного для модели «разорение игрока» выполнения условия $p = 1 - q$, мы получаем в результате каждой попытки (или серии попыток в течение заданного интервала времени) пространство элементарных событий, содержащих следующие события:

– элементарное событие «блок сформирован честной сетью и атакующий не сформировал блок» с вероятностью $p \cdot (1 - q)$;

– элементарное событие «блок не сформирован честной сетью и атакующий сформировал блок» с вероятностью $(1 - p) \cdot q$;

– элементарное событие «блок не сформирован честной сетью и атакующий не сформировал блок» с вероятностью $(1 - p) \cdot (1 - q)$;

– элементарное событие «блок сформирован честной сетью и атакующий сформировал блок» $p \cdot q$.

Множество всех элементарных событий составляет полную группу событий:

$$p \cdot (1 - q) + (1 - p) \cdot q + (1 - p) \cdot (1 - q) + p \cdot q = 1.$$

Рассмотрим трансформацию формул Сатоши Накамото [74] и Мени Розенфельда [75] при переходе от модели разорения игрока к модели независимых игроков.

Вероятность удачного проведения атаки двойной траты (обозначим ее как PI), согласно примерам, приведенным в упомянутых работах, можно представить следующим образом:

$$PI = PI_1 \cdot Q_v + PI_2 \cdot Q_2, \tag{1}$$

где PI_1 – вероятность злоумышленника сформировать z блоки позже честной сети. Символом z обозначим количество подтверждений (сформированных блоков), которые ожидает продавец перед тем, как признать транзакцию с переводом средств действительной; Q_v – вероятность восполнения злоумышленником честной сети с учетом отставания на v блоках (при неограниченном количестве попыток); PI_2 – вероятность злоумышленника сформировать z блоки одновременно или ранее честной сети; Q_2 – вероятность восполнения злоумышленником честной сети с учетом того, что злоумышленником уже сформировано необходимое количество блоков, то есть $Q_2 = 1$.

Заметим, что в данной работе рассматривается вероятность удачного проведения атаки двойной траты при условии неограниченного количества попыток злоумышленника догнать честную сеть. Случай, когда количество попыток ограничено, рассматривается в [76, 77].

Рассмотрим каждый из приведенных компонентов отдельно и сравним формулы для разных моделей.

2.2. Вычисление значения Q_v

Q_v – вероятности злоумышленника догнать честную сеть после того, как честная сеть сформировала необходимое количество блоков (z), и при этом злоумышленник отстает на $0 < v \le z$ блоков.

Для получения формулы определения Q_v воспользуемся материалами, приведенными в [78], и адаптируем их для случая формирования блоков в блокчейн системах.

Случайным блужданием называют случайный процесс специального вида, исторически связанный с моделью перемещения какой-либо частицы под действием некоторого случайного процесса в произвольном фазовом пространстве. При этом предполагается, что изменение на каждом шаге не зависит от предыдущих состояний и от времени.

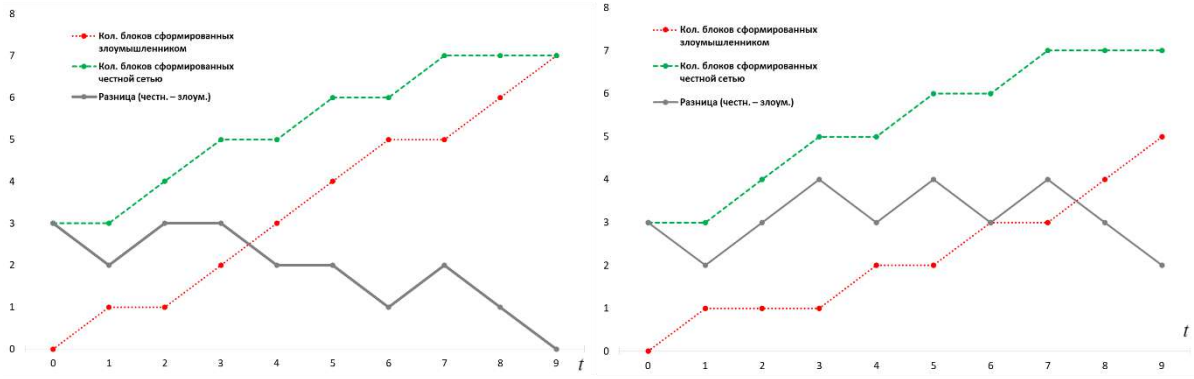
Основные черты общих случайных блужданий можно охарактеризовать на примере простейшего случайного блуждания, порождаемого схемой испытаний Бернулли. Подробно схема Бернули рассматривается во многих книгах по теории вероятностей, например в [79].

Пусть $\xi_0, \xi_1, \xi_2, \ldots$ – произвольная последовательность случайных величин, принимающих значения из множества $\{1, 2, \ldots, n\}$. Тогда последовательность $\xi_0, \ldots, \xi_n$ является последовательностью независимых случайных величин,

модель разорения игрока	*модель независимых игроков*
$\{\xi_i = 1\} = p,$	$\{\xi_i = 1\} = p',$
$\{\xi_i = 0\} = 0,$	$\{\xi_i = 0\} = r',$
$\{\xi_i = -1\} = q,$	$\{\xi_i = -1\} = q',$
$p + q = 1.$	$p' + r' + q' = 1.$

Положим $S_0 = x_0$, $S_t = x_0 + \xi_1 + \ldots + \xi_t = x_t$, $1 \le t \le n$. Последовательность $(S_t)_{t \le n}$ можно рассматривать как траекторию случайного блуждания некоторой «частицы», выходящей из нуля. При этом $S_{t+1} = S_t + \xi_{t+1}$. Данная траектория будет соответствовать разнице между количеством блоков, сформированных честной сетью и злоумышленником. Перемещение осуществляется скачками в дискретные моменты времени. В результате каждого перемещения (шага) частица, находящаяся в точке x_t в момент времени t, в следующий момент $t+1$ перемещается либо на единицу вверх (с вероятностью p для модели разорения игрока и с вероятностью p' для модели независимых игроков), либо на единицу вниз (с вероятностью q для модели разорения игрока и с вероятностью q' – для модели независимых игроков) или остается на месте (с нулевой вероятностью для модели разорения игрока и с вероятностью r' для модели независимых игроков), совершая таким образом случайное блуждание на полупрямой $[0; \infty)$.

При введенных условиях траектории случайного блуждания заметно отличаются для двух рассматриваемых моделей. Пример таких траекторий представлен на рис. 1. На рисунках показано одинаковое изменение сформированных блоков для честной сети (зеленая пунктирная линия). Для злоумышленника (красная линия точками), на рис. 1, *а* изменения происходят случайным образом, на рис. 1, *б* – в строгой зависимости от событий честной сети. В двух представленных случаях траектория разницы количества сформированных блоков (серая сплошная линия) значительно отличается для двух рассматриваемых моделей.



а *б*

Рис. 1. Пример траектории случайного блуждания: *а* – для модели независимых игроков; *б* – для модели разорения игрока

При этом вероятность траектории «частицы» достигнуть нуля будет соответствовать в моделях вероятности злоумышленником догнать честную сеть.

Для *модели разорения игрока* вероятность догнать злоумышленником честную сеть с учетом отставания на v блоков будет определяться (подробный вывод формулы можно найти, например, в [80, 81]) так:

$$Q_v = \begin{cases} \frac{1-\left(\frac{p}{q}\right)^v}{1-\left(\frac{p}{q}\right)^{N-v}}, \text{якщо}, p \neq q \\ \frac{v}{N}, \text{якщо}, p = q = 0{,}5 \end{cases}, \quad (2)$$

где q – вероятность злоумышленником создать блок; p – вероятность создать блок честной сетью (считаем, что $p+q=1$); N – позиция поглощающего экрана, в нашем случае достаточно большое число; $0 < v \leq N$.

В предельном случае, когда $N \to \infty$, получаем:

$$Q_v = \begin{cases} 1, & \text{якщо } p \leq q \\ \left(\frac{q}{p}\right)^v, & \text{якщо } p > q \end{cases}, \quad (3)$$

Для *модели независимых игроков* вероятность догнать злоумышленником честную сеть с учетом отставания на v блоков (подробный вывод формулы можно найти, например, в п. 3.3 [82]):

$$Q_v = \frac{\left(q'/p'\right)^v + \left(q'/p'\right)^{v+1} + \left(q'/p'\right)^{v+2} + \ldots + \left(q'/p'\right)^{N-1}}{1 + \left(q'/p'\right)^1 + \left(q'/p'\right)^2 + \left(q'/p'\right)^3 + \ldots + \left(q'/p'\right)^{N-1}}. \quad (4)$$

где q' – вероятность сократить отставание между злоумышленником и честной сетью (то есть вероятность того, что злоумышленник сформирует блок, а у честной сети сформировать блок не получится, определяется как $q' = q \cdot (1-p)$ и может принимать значения $0 \leq q' \leq 1$); p' – вероятность увеличить отставание (то есть вероятность того, что злоумышленник не сформирует блок, а у честной сети сформировать блок получится, определяется как $p' = p \cdot (1-q)$ и может принимать значения $0 \leq p' \leq 1$), при этом в общем случае $p' + q' \neq 1$; N – позиция поглощающего экрана, в нашем случае достаточно большое число; $0 < v \leq N$.

На рис. 2 представлены вероятности догнать злоумышленником честную сеть Q_v в зависимости от первоначального отставания v для двух рассматриваемых моделей (при q = 0,3; p = 0,7; N = 100).

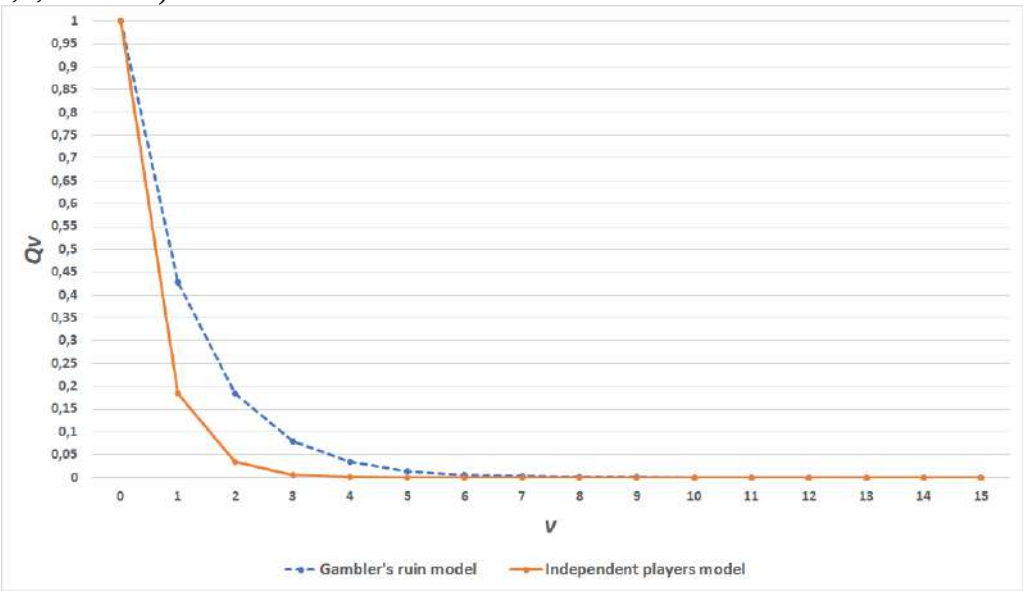


Рис. 2. Вероятность догнать злоумышленником честную сеть Q_v в зависимости от первоначального отставания v для модели разорения игрока (пунктирная линия) и модели независимых игроков

2.3. Вычисление значений PI_1 та PI_2 (модель независимых игроков)

В случае допущения, что функция распределения вероятности создать блок соответствует отрицательному биномиальному закону, как это делается в работе Мени Розенфельда [75], то вероятность честной сети сформировать z блоков ровно за $z+k_p$ попыток (где $k_p = 0,1,\ldots$):

$$P_p(p,z,k_p) = \binom{k_p+z-1}{k_p} p^z (1-p)^{k_p}, \tag{5}$$

где $\binom{n}{k} = \frac{n!}{(n-k)!k!}$ – биномиальный коэффициент.

При этом вероятность злоумышленника сформировать v блоков ($v = 0,1,\ldots,z+k_p$) за такое же количество попыток (то есть ровно за $z+k_q$ попыток):

$$P_q(q,z,k_p,v) = \binom{z+k_p}{v} q^v (1-q)^{z+k_p-v}. \tag{6}$$

Таким образом, вероятность злоумышленника отстать от честной сети (то есть сформировать менее блоков)

$$P_q(q,z,k_p,0 \le v < z) = \sum_{v=0}^{z-1} \left\{ \binom{z+k_p}{v} q^v (1-q)^{z+k_p-v} \right\}. \tag{7}$$

Чтобы подсчитать вероятность того, что злоумышленнику удалось догнать и опередить честную сеть (то есть сформировать z или более блоков) за количество попыток, которое не превышает значения $z+k_p$, необходимо суммировать все вероятности для $z \le v \le z+k_p$, т.е.

$$P_q(q,z,k_p,z \le v \le z+k_p) = \sum_{v=z}^{z+k_p} \left\{ \binom{z+k_p}{v} q^v (1-q)^{z+k_p-v} \right\}. \tag{8}$$

Учитывая, что честная сеть способна сформировать z блоков за произвольное (от z и более) количество попыток, вероятность злоумышленника сформировать z блоков одновременно или ранее честной сети, возможно вычислить из выражения

$$PI_2 = \sum_{k_p=0}^{\infty} \left[P_p(p,z,k_p) \cdot \sum_{v=z}^{z+k_p} P_q(q,z,k_p,v) \right]. \tag{9}$$

Аналогичным образом будет подсчитываться вероятность злоумышленника сформировать z блоков позднее честной сети:

$$PI_1 = \sum_{k_p=0}^{\infty} \left[P_p(p,z,k_p) \cdot \sum_{v=0}^{z-1} P_q(q,z,k_p,v) \right]. \tag{10}$$

Подставляя выражения (PI_1), (PI_2) и (Q_v) в (1) и вынося общие составляющие, получаем

$$PI = \sum_{k_{p=0}}^{\infty} \left(P_p(p,z,k_p) \cdot \left[\sum_{v=0}^{z-1} \left\{ P_q(q,z,k_p,v) \cdot Q_{(z-v)} \right\} + \sum_{v=z}^{z+k_p} \left\{ P_q(q,z,k_p,v) \cdot 1 \right\} \right] \right) \tag{11}$$

или, подставляя (P_p) и (P_q),

$$PI = \sum_{k_p=0}^{\infty}\left(\binom{k_p+z-1}{k_p} p^z (1-p)^{k_p}\left[\sum_{v=0}^{z-1}\left\{\binom{z+k_p}{v} q^v (1-q)^{z+k_p-v}\cdot Q_{(z-v)}\right\} + \sum_{v=z}^{z+k_p}\left\{\binom{z+k_p}{v} q^v (1-q)^{z+k_p-v}\cdot 1\right\}\right]\right). \quad (12)$$

Напомним, что значение $Q_{(z-v)}$ вычисляется по формуле (4).

Согласно модели разорения игрока, приведенной в работе Мени Розенфельда [75], вероятность удачного проведения атаки двойной траты рассчитывается по выражению

$$PI = \begin{cases} 1 - \sum_{k=0}^{z-1}\binom{k+z-1}{k}\left(q^k p^z - p^k q^z\right), если\ p > q \\ 1, если\ p \le q \end{cases}. \quad (13)$$

На рис. 3 приведено сравнение результатов вероятности удачного проведения атаки двойной траты, рассчитанных согласно модели независимых игроков (для наглядности положено, что $p+q=1$) и модели разорения игрока.

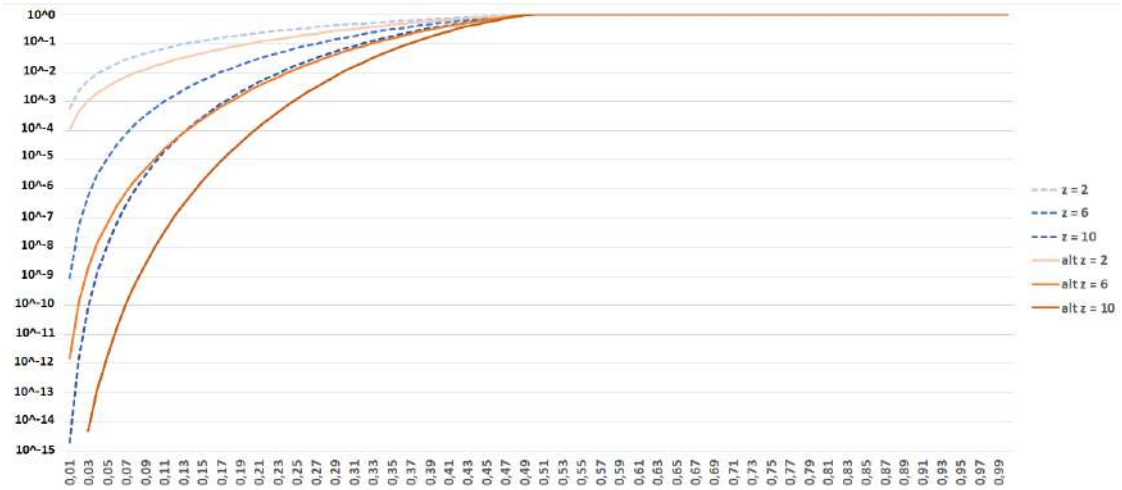


Рис. 3. Вероятности удачного проведения атаки двойной траты
рассчитанные согласно модели независимых игроков (по формуле (13))
и модели разорения игрока (формула 1 работы Розенфельда [39]) при различных значениях Z

Выводы

Рассмотрена вероятность успешного проведения атаки двойной траты на блокчейн системы, которые построены с помощью алгоритмов консенсуса по Доказательствам выполненной работы (PoW).

Показано, что проблема двойных трат в блокчейн системах не является чисто теоретической. Приведен ряд примеров проведения удачных атак на децентрализованные учетные системы с существенными (миллионными) убытками.

Проанализирована вероятность удачного проведения атак двойной траты с учетом скорректированной аналитической модели, основанной на «независимых игроках». Работа является логическим дополнением работ [76, 77, 83] и рассматривает корректировки аналитических выражений, приведенных в работах Сатоши Накамото [74] и Мени Розенфельда [75], основанных на моделях «разорения игрока».

Отмечено значительное отличие результатов, полученных по приведенным двум моделям. Получены аналитические оценки вероятностей успешной реализации атак двойной траты на блокчейн системы, которые существенно отличаются от результатов, полученных с использованием модели «разорения игрока».

Приведенные результаты свидетельствуют, что безопасность децентрализованных блокчейн систем, которые построены с консенсусами на основе доказательств выполненной работы, имеют более высокую надежность, чем считалось ранее. В качестве примера, при хэш-рейте злоумышленника $q = 0{,}1$ и $z = 6$ подтверждениях, вероятность удачного проведения атаки двойной траты будет составлять 0,00001 в соответствии с моделью «независимых игроков», против вероятности в 0,0006 полученного на основании модели «разорения игрока».

Полученные результаты могут быть полезными при обосновании конкретных показателей и параметров протокола консенсуса для блокчейн систем на основе доказательства проделанной работы, при применении его в качестве основного механизма установления консенсуса перспективных децентрализованных распределенных систем и сетей, построенных по технологии блокчейн.

Список литературы:

1. Saad M., Spaulding J., Njilla L., Kamhoua C.,Shetty S., Nyang D., Mohaisen A. Exploring the Attack Surface of Blockchain: A Systematic Overview. (2019) https://www.researchgate.net/publication/331806569_Overview_of_Attack_Surfaces_in_Blockchain

2. L. Mauri, S. Cimato, and E. Damiani. A comparative analysisof current cryptocurrencies // Proceedings of the 4th InternationalConference on Information Systems Security and Privacy, ICISSP, Funchal, Madeira – Portugal, Jan. 2018, pp. 127–138. https://doi.org/10.5220/0006648801270138

3. G. Danezis and S. Meiklejohn. Centrally banked cryptocurrencies // Proceedings of the 2016 Annual Network and Distributed SystemSecurity Symposium (NDSS), San Diego, CA, Feb. 2016. http://wp.internetsociety.org/ndss/wp-content/uploads/sites/25/2017/09/centrally-banked-cryptocurrencies.pdf

4. J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, andE. W. Felten. Research perspectives and challenges for bitcoin andcryptocurrencies // IACR Cryptology ePrint Archive, vol. 2015, p. 261, 2015. http://eprint.iacr.org/2015/261

5. A. E. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou Hawk:The blockchain model of cryptography and privacy-preserving smartcontracts // Proceedings of the 37th IEEE Symposium on Securityand Privacy (Oakland), San Jose, CA, May 2016, pp. 839–858. https://doi.org/10.1109/SP.2016.55

6. K. Bhargavan, A. Delignat-Lavaud, C. Fournet, A. Gollamudi,G. Gonthier, N. Kobeissi, N. Kulatova, A. Rastogi, T. Sibut-Pinote, N. Swamy, and S. Z. Béguelin. Formal verificationof smart contracts: Short paper // Proceedings of the 23rdACM Conference on Computer and Communications Security(CCS), Vienna, Austria, Oct. 2016, pp. 91–96. http://doi.acm.org/10.1145/2993600.2993611

7. P. K. Sharma, S. Rathore, and J. H. Park. Distarch-scnet: Blockchain-based distributed architecture with li-fi communication for a scalable smart city network // IEEE Consumer Electronics Magazine, vol. 7, no. 4, pp. 55–64, 2018. Available: https://doi.org/10.1109/MCE.2018.2816745

8. K. Fan, Y. Ren, Y. Wang, H. Li, and Y. Yang. Blockchain-based efficient privacy preserving and data sharing scheme of content-centric network in 5g // IET Communications, vol. 12, no. 5, pp. 527–532, 2018. Available: https://doi.org/10.1049/iet-com.2017.0619

9. Sharma P.K., Singh S., Jeong Y.-S., Park J.H. DistBlockNet: A Distributed Blockchains-Based Secure SDN Architecture for IoT Networks // IEEE Communications Magazine, 2017, vol. 55 (9), pp. 78–85

10. R. Guo, H. Shi, Q. Zhao, and D. Zheng. Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems // IEEE Access, vol. 6, pp. 11 676–11 686, 2018. Available: https://doi.org/10.1109/ACCESS.2018.2801266

11. D. Rakic. Blockchain technology in healthcare // Proceedings of the 4th International Conference on Information and Communication Technologies for Ageing Well and e-Health, Funchal, Madeira, Portugal, March 2018., pp. 13–20. Available: https://doi.org/10.5220/0006531600130020

12. A. Ekblaw, A. Azaria, J. D. Halamka, A. Lippman. A case study for blockchain in healthcare: “medrec” prototype for electronic health records and medical research data (2016). URL https://www.media.mit.edu/publications/medrec-whitepaper/

13. A. Azaria, A. Ekblaw, T. Vieira, A. Lippman. Medrec: Using blockchain for medical data access and permission management // International Conference on Open and Big Data (OBD), 2016, pp. 25-30.

14. Yue, H. Wang, D. Jin, M. Li, W. Jiang. Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control // Journal of medical systems, 2016, p. 218

15. E. F. Jesus, V. R. L. Chicarino, C. V. N. de Albuquerque, and A. A. de A. Rocha. A survey of how to use blockchain to secure internet of things and the stalker attack // Security and Communication Networks, vol. 2018, pp. 9. 675 050:1–9 675 050:27, 2018. Available: https://doi.org/10.1155/2018/9675050

16. P. K. Sharma, S. Singh, Y. Jeong, and J. H. Park. Distblocknet: A distributed blockchains-based secure SDN architecture for iot networks // IEEE Communications Magazine, vol. 55, no. 9, pp. 78–85, 2017. Available: https://goo.gl/UBv1Sf

17. A. Dorri, S. S. Kanhere, R. Jurdak, P. Gauravaram. Blockchain for iot security and privacy: The case study of a smart home // IEEE Percom workshop on security privacy and trust in the internet of thing, 2017

18. Y. Zhang, J. Wen. The iot electric business model: Using blockchain technology for the internet of things // Peer-to-Peer Networking and Applications, 2016, pp. 1-12.

19. J. Sun, J. Yan, K. Z. Zhang, Blockchain-based sharing services: What blockchain technology can contribute to smart cities // Financial Innovation, 2016, p. 26.

20. H. Hyvärinen, M. Risius, and G. Friis. A blockchain-based approach towards overcoming financial fraud in public sector services // Business & Information Systems Engineering, vol. 59, no. 6, pp. 441–456, 2017. Available: https://doi.org/10.1007/s12599-017-0502-4

21. F. Holotiuk, F. Pisani, and J. Moormann. The impact of blockchain technology on business models in the payments industry // Towards Thought Leadership in Digital Transformation: 13. Internationale Tagung Wirtschaftsinformatik, St.Gallen, Switzerland, Feb, 2017. Available: http://aisel.aisnet.org/wi2017/track09/paper/6

22. S. Huckle, R. Bhattacharya, M. White, N. Beloff. Internet of things, blockchain and shared economy applications // Procedia Computer Science, Vol. 98, 2016, pp. 461-466.

23. P. Hurich, The virtual is real: An argument for characterizing bitcoins as private property // Banking & Finance Law Review, Vol. 31, Carswell Publishing, 2016, p. 573.

24. Xu, C. Pautasso, L. Zhu, V. Gramoli, A. Ponomarev, A. B. Tran, S. Chen. The blockchain as a software connector // The 13th Working IEEE/IFIP Conference on Software Architecture, 2016

25. E.Nordstr¨om., Personal clouds: Concedo, Masters thesis, Lulea University of Technology (2015).

26. J. S. Czepluch, N. Z. Lollike, S. O. Malone. The use of block chain technology in different application domains // The IT University of Copenhagen, Copenhagen, 2015.

27. G. G. Dagher, P. B. Marella, M. Milojkovic, and J. Mohler, Broncovote: Secure voting system using ethereum's blockchain // Proceedings of the 4th International Conference on Information Systems Security and Privacy, ICISSP, Funchal, Madeira – Portugal, Jan 2018, pp. 96–107. Available: https://doi.org/10.5220/0006609700960107

28. F. S. Hardwick, R. N. Akram, and K. Markantonakis. E-voting with blockchain: An e-voting protocol with decentralisation and voter privacy // CoRR, vol. abs/1805.10258, 2018. Available: http://arxiv.org/abs/1805.10258

29. K.-H. Wang, S. K. Mondal, K. Chan, and X. Xie. A review of contemporary e-voting: Requirements, technology, systems and usability // Data Science and Pattern Recognition, vol. 1, no. 1, pp. 31–47, 2017

30. D. A. Gritzalis. Principles and requirements for a secure e-voting system // Computers & Security, vol. 21, no. 6, pp. 539–556, 2002

31. R. Anane, R. Freeland, and G. Theodoropoulos. E-voting requirements and implementation // The 9th IEEE CEC/EEE 2007. IEEE, 2007, pp. 382–392

32. A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram.LSB: A lightweight scalable blockchain for IoT security and anonymity // J. Parallel Distrib. Comput., vol. 134, pp. 180–197, 2019

33. Arif S., Khan M.A., Rehman S.U., Kabir M.A. & Imran M. Investigating Smart Home Security: Is Blockchain the Answer? // IEEE Access, 2020, 8, 117802-117816

34. Younghun Lee, Shailendra Rathore, Jin Ho Park, Jong Hyuk Park. A blockchain-based smart home gateway architecture for preventing data forgery // Human-centric Computing and Information Sciences, 2020, Volume 10, Number 1, Page 1

35. PR Wire (2016) Gartner: blockchain and connected home are almost at the peak of the hype cycle. https://prwire.com.au/pr/62010/gartner-blockchain-andconnected-home-are-almost-at-the-peak-of-the-hype-cycle

36. J. DESJARDINS, Its official: Bitcoin was the top performing currency of 2015 (2016). URL http://money.visualcapitalist.com/its-official-bitcoin-was-the-top-performing-currency-of-2015/

37. J. Adinolfi, And 2016s best-performing commodity is ... bitcoin? (2016). URL http://www.marketwatch.com/story/and-2016s-best-performing-commodity-is-bitcoin-2016-12-22

38. Blockchain.info. Confirmed transactions per day (2020). URL https://blockchain.info/charts/n-transactions?timespan=all#

39. G. Zyskind, O. Nathan, and A. Pentland. Decentralizing privacy: Using blockchain to protect personal data // 2015 IEEE Symposium on Security and Privacy Workshops, SPW, San Jose, CA, USA, May 2015, pp. 180–184. Available: https://goo.gl/kTNim3

40. A. Back, M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell, A. Miller, A. Poelstra, J. Timón, and P. Wuille. Enabling blockchain innovations with pegged sidechains. 2014

41. G. Zyskind, O. Nathan, and A. Pentland. Enigma: Decentralized Computation Platform with Guaranteed Privacy, 2015. https://arxiv.org/abs/1506.03471

42. M. Swan. Blockchain thinking: The brain as a dac (decentralized autonomous organization) // Proceedings of the Texas Bitcoin Conferenc, pp. 27–29, 2015.

43. X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen. A survey on the security of blockchain systems // CoRR, vol. abs/1802.06993, 2018. Available: http://arxiv.org/abs/1802.06993

44. I.-C. Lin and T.-C. Liao. A survey of blockchain security issues and challenges // IJ Network Security, vol. 19, no. 5, pp. 653–659, 2017

45. N. Atzei, M. Bartoletti, T. Cimoli. A survey of attacks on Ethereum smart contracts sok // Proceedings of the 6th International Conference on Principles of Security and Trust -Volume 10204, 2017, pp. 164–186. Available: https://doi.org/10.1007/978-3-662-54455-6_8

46. M. C. K. Khalilov and A. Levi. A survey on anonymity and privacy in bitcoin-like digital cash systems // IEEE Communications Surveys and Tutorials, vol. 20, no. 3, pp. 2543–2585, 2018. Available: https://doi.org/10.1109/COMST.2018.2818623

47. D. Siegel. Understanding The DAO Attack. https://www.coindesk.com/understanding-dao-hack-journalists/

48. V. Buterin, Critical update re: Dao vulnerability (2016). URL https://blog.ethereum.org/2016/06/17/critical-update-re-dao-vulnerability/

50. M. Saad, M. T. Thai, and A. Mohaisen. POSTER: deterring ddos attacks on blockchain-based cryptocurrencies through mempool optimization // Proceedings of Asia Conference on Computer and Communications Security, ASIACCS, Incheon, Republic of Korea, Jun 2018, pp. 809–811. Available: https://goo.gl/4kgiCM

51. I. Eyal, A. E. Gencer, E. G. Sirer, and R. van Renesse. Bitcoin-ng: A scalable blockchain protocol // Proceedings of the 13th USENIX Symposium on Networked Systems Design and Implementation (NSDI), Santa Clara, CA, Mar. 2016, pp. 45–59. Available: https://goo.gl/VGN4yw

52. R. McMillan.The inside story of mt. gox, bitcoin's 460 million usd disaster. 2014. Available: https://www.wired.com/2014/03/bitcoin-exchange/

53. J. Adelstein, Behind the biggest Bitcoin heist in history: Inside the implosion of mt.gox (2016). URL http://www.thedailybeast.com/articles/2016/05/19/behind-the-biggest-bitcoin-heist-in-history-inside-the-implosion-of-mt-gox.html

54. Irreversible Transactions https://en.bitcoin.it/wiki/Irreversible_Transactions.

55. Partz H. Bittrex to Delist Bitcoin Gold by Mid-September, Following $18 Million Hack of BTG in May. 04.09.2018 https://cointelegraph.com/news/bittrex-to-delist-bitcoin-gold-by-mid-september-following-18-million-hack-of-btg-in-may

56. Cimpanu C. Hacker Makes Over $18 Million in Double-Spend Attack on Bitcoin Gold Network 24.05.2018 https://www.bleepingcomputer.com/news/security/hacker-makes-over-18-million-in-double-spend-attack-on-bitcoin-gold-network/

57. Iskra E. Responding to Attacks 24.05.2018 https://bitcoingold.org/responding-to-attacks/

58. Wilmoth J. Spend Attack, Exchanges Lose Millions https://www.ccn.com/bitcoin-gold-hit-by-double-spend-attack-exchanges-lose-millions/

59. Martin J. Bitcoin Gold Blockchain Hit by 51% Attack Leading to $70K Double Spend 27.01.2020 https://cointelegraph.com/news/bitcoin-gold-blockchain-hit-by-51-attack-leading-to-70k-double-spend

60. Lovejoy J. Bitcoin Gold (BTG) was 51% attacked. 25.01.2020 https://gist.github.com/metalicjames/71321570a105940529e709651d0a9765

61. Coinbase: Deep Chain Reorganization Detected on Ethereum Classic (ETC) https://blog.coinbase.com/ethereum-classic-etc-is-currently-being-51-attacked-33be13ce32de

62. Bitfly (@etherchain_org) / Твиттер https://twitter.com/etherchain_org/status/1289489999004463111

63. HackMD: ETC Chain Split Diagnosis https://hackmd.io/@cUBb4hAvQciAEPoU2yfrzQ/Skd4X6MZw

64. Bitquery: Attacker Stole 807K ETC in Ethereum Classic 51% Attack https://blog.bitquery.io/attacker-stole-807k-etc-in-ethereum-classic-51-attack

65. Bitfly (@etherchain_org) / Твиттер https://twitter.com/etherchain_org/status/1291216063628226562

66. Binance (@binance) / Твиттер https://twitter.com/binance/status/1291225022866944000

67. Bitquery: Ethereum Classic Attack, 8 August: Catch me if you can https://blog.bitquery.io/ethereum-classic-attack-8-august-catch-me-if-you-can

68. Bitfly (@etherchain_org) / Твиттер https://twitter.com/etherchain_org/status/1299822510607917056

69. Ethereum Classic (@eth_classic) / Твиттер https://twitter.com/eth_classic/status/1299824170260340737

70. Wilmoth J. Privacy Coin Verge Succumbs to 51% Attack [Again] 22.05.2020 https://www.ccn.com/privacy-coin-verge-succumbs-to-51-attack-again/

71. Ville Savolainen, Jorge Soria Ruiz-Ogarrio. Too Big to Cheat: Mining Pools' Incentives to Double Spend in Blockchain Based Cryptocurrencies. 2019.
https://helda.helsinki.fi//bitstream/handle/10138/309233/SSRN_id3506748.pdf

72. Gencer, A. E., Basu, S., Eyal, I., Van Renesse, R., and Sirer, E. G. (2018). Decentralization in bitcoin and ethereum networks. https://arxiv.org/pdf/1801.03998.pdf

73.Lovejoy J. Reorgs on Bitcoin Gold: Counterattacks in the wild. 11.03.2020 https://medium.com/mit-media-lab-digital-currency-initiative/reorgs-on-bitcoin-gold-counterattacks-in-the-wild-da7e2b797c21

74. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2009. 9 p.

75. Rosenfeld M. Analysis of hashrate-based double-spending. 2014. 13 p. (arXiv preprint arXiv:1402.2009).

76. Poluyanenko N., Kuznetsov A., Lisickiy K., Datsenko S., Nakisko O., Rudenko S. (2021) The Problem of Double Costs in Blockchain Systems // Hu Z., Petoukhov S., Dychka I., He M. (eds) Advances in Computer Science for Engineering and Education III. ICCSEEA 2020. Advances in Intelligent Systems and Computing, vol 1247. Springer,

Cham. PP 640-652. ISSN 2194-5357, ISSN 2194-5365 (electronic), ISBN 978-3-030-55505-4, ISBN 978-3-030-55506-1 (eBook) https://doi.org/10.1007/978-3-030-55506-1_57

77. Poluyanenko N, Kuznetsov A., Lazareva E., Marakushyn A. Extrapolation to calculate the probability of a double spending attack. CMIS 2020: 610-620.

78. Малахов Е.И. Случайные блуждания на полупрямой с поглощающим экраном с возможностью остановки http://math.isu.ru/ru/chairs/tpdm/docs/Platonovskie2017/Malahov.pdf

79. Гмурман В.Е. Теория вероятностей и математическая статистика. Москва : Высш. шк., 1997.

80. Ширяев А. Н. Вероятность : в 2-х кн. ; 4-е изд., переработ. и доп. Москва : МЦНМО, 2007.

81. K. Sigman. Gambler's ruin problem. www.columbia.edu/~ks20/FE-Notes/4700-07-Notes-GR.pdf , June 7 2016

82. Зубков А.М. Конспект лекций по теории случайных процессов. Москва : МГУ. Мех.-мат. факультет. 6-й семестр. 2008. – 90 с. https://epdf.pub/-6-88e2c451ff9dcbefcfbfacfb1bca654742391.html

83. Poluyanenko N., Pisarenko N., Safonenko V., Makushenko T., Pushko O., Zaburmekha Y., Kuznetsova K. Simulation of a double spending attack on the proof of work consensus protocol // CEUR Workshop Proceedings. Volume 2654, 2020, Pages 32-59. 2019 International Workshop on Cyber Hygiene, CybHyg 2019; Kyiv; Ukraine; 30 November 2019. ISSN: 16130073.

Поступила в редколлегию 12.10.2020

Сведения об авторах:

Полуяненко Николай Александрович – канд. техн. наук, доцент, доцент кафедры безопасности информационных систем и технологий, факультет компьютерных наук, Харьковский национальный университет имени В.Н. Каразина, Украина; e-mail: nlfsr01@gmail.com, ORCID: https://orcid.org/0000-0001-9386-2547

Горбенко Юрий Иванович – канд. техн. наук, первый заместитель главного конструктора, АТ «Институт информационных технологий», Украина; e-mail: gorbenkou@iit.kharkov.ua, ORCID: https://orcid.org/0000-0003-0073-9107

Сафоненко Владислав Едуардович – доцент кафедры безопасности информационных систем и технологий, факультет компьютерных наук, Харьковский национальный университет имени В.Н. Каразина, Украина; e-mail: vladyslavsafonenko@gmail.com, ORCID: https://orcid.org/0000-0002-2983-8689

Кузнецов Александр Александрович – д-р техн. наук, профессор, профессор кафедры безопасности информационных систем и технологий, факультет компьютерных наук, Харьковский национальный университет имени В.Н. Каразина, Украина; e-mail: kuznetsov@karazin.ua, ORCID: https://orcid.org/0000-0003-2331-6326

УДК 004.056.5 **DOI:10.30837/rt.2020.4.203.04**

А.А. КУЗНЕЦОВ, д-р техн. наук, А.А. СМИРНОВ, д-р техн. наук, А.С. КИЯН, Т.Ю. КУЗНЕЦОВА

СОКРЫТИЕ ДАННЫХ НА ОСНОВЕ АДРЕСАЦИИ ШУМОПОДОБНЫХ СИГНАЛОВ

Введение

Для передачи секретных сообщений используются различные вычислительные методы [1 – 4]. Например, криптографические методы скрывают смысловое содержание передаваемых сообщений, представляя их в виде шумоподобных бессмысленных данных [1, 5]. Стеганографические методы скрывают сам факт существования информационных сообщений [3, 6]. Для этого сообщения скрываются внутри контейнеров (cover files) – избыточных данных, которые передаются открытым способом и не вызывают ни у кого подозрений [2, 3]. Сторонний наблюдатель может перехватывать cover files, анализировать и исследовать их, однако детектировать сокрытые данные и, тем более, их восстанавливать, для него очень сложно или вообще невозможно.

Сегодня стеганографические методы развиты очень хорошо. В литературе описаны различные способы сокрытия информационных сообщений избыточных cover files [7 – 10]: в изображениях, звуке, текстовых документах, видео и пр. Наиболее распространенные примеры описаны для контейнеров-изображений (cover images). При этом используются различные вычислительные приемы.

Наиболее перспективным направлением в сокрытии данных является стеганография на основе расширения спектра (Spread Spectrum Steganographic) [6, 11 – 14]. Эти методы используют достижения теории сложных дискретных сигналов для организации широкополосной высокоскоростной цифровой связи. Например, современные системы мобильной связи 4G и 5G используют широкополосные шумоподобные сигналы (специальным образом сформированные псевдослучайные последовательности), обеспечивая высокую помехоустойчивость, безопасность и экологичность связи [15 – 17]. Эти положительные свойства можно использовать и для сокрытия данных внутри cover files, например в изображениях [18 – 24].

В данной работе обсуждаются методы сокрытия данных в cover images с использованием технологии прямого расширения спектра. Мы показываем, что некоторые базовые предположения и гипотезы, принимаемые для организации широкополосной высокоскоростной цифровой связи, могут не выполняться при сокрытии данных внутри cover files. Это приводит к негативным эффектам:

- cover files сильно искажаются;
- интенсивность ошибок в восстановленных сообщениях очень высока.

В статье предлагается новый метод, который заключается в прямой адресации расширяющей последовательности. С одной стороны, это значительно уменьшает искажение cover file. С другой стороны, интенсивность ошибок в восстановленных сообщениях не увеличивается. Приводятся наглядные примеры и показываются преимущества предложенного метода. Также приводятся результаты экспериментов, оценивается качество изображений по различным показателям.

Обзор литературы

В первых работах по стеганографии на основе расширенного спектра (Spread Spectrum Steganographic) введены базовые понятия и определения, показана принципиальная возможность сокрытия данных в cover files с использованием сложных шумоподобных дискретных сигналов и прямого расширения спектра [18 – 20, 25]. В то же время рассмотренные методы имеют определенные недостатки:

• битовая интенсивность ошибок (bit error rate – BER) восстановленных сообщений очень высокая. Например, в [18, с. 12, табл. 2] показано, что в большинстве случаев BER принимает значения 15 – 30 %. Даже при очень высокой «энергии» сокрытого сообщения BER не удается уменьшить ниже 10 %;

• искажения cover images очень высоки. Например, в [18] показано, что, увеличивая «энергию» сокрытого сообщения, удается снизить BER до 12 – 15 %, однако качество cover image при этом значительно снижается.

Таким образом, основная проблема рассмотренных стеганографических методов состоит в необходимости существенного снижения BER при сохранении приемлемого качества cover image. Например, в [18, с. 22] указано: «The BER is always higher than the desired value of 12 %. A power of 150 has an error rate of 16 %+ and the picture quality is becoming unacceptable. Increasing the stego power results in smaller improvements of the BER, approaching a limit of just under 16 %».

Дальнейшие исследования были направлены на снижение BER и повышение качества cover image. Для этого использовались различные методы [23, 26]: помехоустойчивое кодирование, фильтрация и пр. В работах [22, 27] исследуются варианты Spread Spectrum Steganographic при использовании аудио- и видео- cover files. В [28 – 31] сокрытие сообщение реализуется в DCT-области. Эти методы позволяют реализовать сокрытие сообщений, устойчивое к атакам сжатия. Например, наиболее распространенный способ сжатия JPEG использует DCT. Сокрытие данных в DCT-области снижает BER, т.е. число ошибок восстановленных сообщений уменьшается.

Еще один из возможных способов снижения BER – это подбор расширяющих шумоподобных последовательностей [32, 33]. Например, в работе [32] предложено формировать расширяющие последовательности с учетом статистических свойств cover files. Это позволило существенно снизить BER. В отдельных случаях удается добиться BER≈0, однако при этом время формирования расширяющих последовательностей очень велико. Кроме того, приемной стороне для восстановления сообщения нужен список расширяющих последовательностей (или компактное правило их формирования). Качество изображений остается на прежнем уровне. При увеличении объема сокрытого сообщения качество изображений неизбежно снижается.

В данной работе предлагается новый способ сокрытия данных в cover files. Этот подход позволяет минимизировать искажения cover files даже при большом объеме одновременно скрываемых сообщений. В работе показаны примеры изображений с различными способами сокрытия. Предлагаемый способ действительно выигрывает по качеству cover image. Однако вычислительная сложность предлагаемого способа существенно выше – сложность восстановления сообщений растет экспоненциально по мере повышения пропускной способности. Это основной недостаток предлагаемого способа. Однако всегда можно найти компромисс между вычислительной сложностью и качеством cover files.

Известные методы сокрытия данных

Известные примеры Spread Spectrum Steganography используют псевдослучайные последовательности для сокрытия сообщений. При этом в качестве cover files могут использоваться различные данные: изображения, аудио, видео и пр. Кроме того, сокрытие может реализовываться как в пространственной области, так и в области DCT. Мы не будем акцентировать на этом внимание, поскольку предлагаемый ниже способ также может применяться в различных вариантах. Для описания базовой технологии будем следовать публикациям [18 – 20], предлагая, тем не менее, некоторые собственные интерпретации.

Обозначим информационное сообщение как последовательность $m_0, m_1, ..., m_{k-1}$ бит, записанных в полярном виде:

$$\forall i \in \{0,1,...,k-1\} : m_i \in \{-1,1\}.$$

Для реализации технологии прямого расширения спектра используются дискретные сигналы [18 – 20]:

$$\Phi_i \in \Phi = \{\Phi_0, \Phi_1, ..., \Phi_{N-1}\},\ k \le N,$$

причем каждый сигнал представляет собой псевдослучайную последовательность (ПСП):

$$\forall i \in \{0,1,...,N-1\} : \Phi_i = \left(\varphi_{i_0}, \varphi_{i_1}, ..., \varphi_{i_{n-1}}\right),\ \forall j \in \{0,1,...,n-1\} : \varphi_{i_j} \in \{-1,1\}.$$

Предполагается, что различные сигналы из множества Φ слабокоррелированы, т.е. коэффициент их взаимной корреляции примерно равен нулю:

$$\forall i \ne j : \rho\left(\Phi_i, \Phi_j\right) = \sum_{u=0}^{n-1} \varphi_{i_u} \varphi_{j_u} \approx 0.$$

Стегано-контейнер (cover) S формируется посредством прибавления к исходному cover file C усиленного модулированного сигнала E [18 – 20]:

$$E = G \cdot \sum_{i=0}^{k-1} m_i \Phi_i,$$

т.е.

$$S = C + G \cdot E = C + G \cdot \sum_{i=0}^{k-1} m_i \Phi_i, \tag{1}$$

где $G > 0$ – коэффициент усиления, который задает «энергию» модулированного сигнала E.

Восстановление информационного сообщения на приемной стороне осуществляется с помощью корреляционного приема. При этом предполагается, что каждый сигнал из множества Φ не коррелирован с исходным cover file C:

$$\forall i : \rho\left(\Phi_i, C\right) \approx 0. \tag{2}$$

Тогда значение коэффициента корреляции определяется как

$$\rho\left(\Phi_i, S\right) = \rho\left(\Phi_i, C + G \cdot E\right) =$$
$$= \rho\left(\Phi_i, C\right) + G \cdot \rho\left(\Phi_i, E\right) \approx G \cdot \sum_{j=0}^{k-1} m_j \sum_{u=0}^{n} \varphi_{i_u} \varphi_{j_u}.$$

Принимая предположение

$$\forall j \ne i :\ \rho\left(\Phi_i, \Phi_j\right) = \sum_{u=0}^{n} \varphi_{i_u} \varphi_{j_u} \approx 0,$$

имеем

$$\rho\left(\Phi_i, S\right) \approx G \cdot m_i \cdot n,$$

т.е. знак $\rho\left(\Phi_i, S\right)$ совпадает со значением m_i [18 – 20]:

$$m_i = sign\left(\rho\left(S, \Phi_i\right)\right) = \begin{cases} -1,\ \rho\left(S, \Phi_i\right) < 0; \\ +1,\ \rho\left(S, \Phi_i\right) > 0. \end{cases} \tag{3}$$

Очевидно, что число k сокрытых информационных бит не может быть велико. Действительно, если $k = 1$, тогда cover file будет искажен незначительно. Как следует из (1), к значениям cover file C будет прибавлено $G \cdot m_0 \Phi_0$, т.е. искажения cover file будут в диапазоне $-G...G$. Если G невелико, тогда $S \approx C$. Например, для cover images искажения визуально

будут незаметны. Однако при увеличении $k>1$ искажения cover file будут возрастать пропорционально и находиться в диапазоне $-Gk...Gk$. Например, для $k=10$ искажения возрастут в 10 раз, и это невозможно изменить.

Напомним, что в реальных ситуациях для уменьшения BER значение G также приходится увеличивать. Например, в [18] даже для больших значений G значение BER не удалось уменьшить ниже 12 %. И это основное противоречие: снижение BER и сохранение качества cover file возможны только при небольшой пропускной способности, т.е. при малых k.

Мы предлагаем новый метод сокрытия данных, основанный на других правилах, отличных от (1) и (3).

Предлагаемый метод сокрытия данных

Обозначим информационное сообщение как последовательность $m_0, m_1, ..., m_{(k-1)K}$ бит:

$$\forall i \in \{0,1,...,(k-1)K\} : m_i \in \{0,1\}.$$

Сокрытие сообщения осуществляется блоками по k бит. Для удобства представим информационное сообщение в виде последовательности неотрицательных целых чисел:

$$M_1, M_2, ..., M_K,$$

где

$$\forall i \in \{1,2,...,K\} : M_i = \sum_{j=0}^{k-1} 2^j m_{k(i-1)+j}.$$

Эти числа $M_i \in \{0,1,...,N-1\}$, $N=2^k$, $i \in \{1,2,...,K\}$ будем интерпретировать как адреса (порядковые номера) псевдослучайных последовательностей

$$\Phi_{M_i} \in \Phi = \{\Phi_0, \Phi_1, ..., \Phi_{N-1}\},$$

где, как и прежде:

$$\forall i \in \{0,1,...,N-1\} : \Phi_i = \left(\varphi_{i_0}, \varphi_{i_1}, ..., \varphi_{i_{n-1}}\right),\ \forall j \in \{0,1,...,n-1\} : \varphi_{i_j} \in \{-1,1\}.$$

Для снижения искажений cover file мы предлагаем скрывать информационные сообщения на основе адресации расширяющих последовательностей. Правило кодирования расширяющей последовательностью предлагается реализовать следующим образом:

$$E_i = \Phi_{M_i} = \left(\varphi_{M_{i_0}}, \varphi_{M_{i_1}}, ..., \varphi_{M_{i_{n-1}}}\right),$$

т. е. есть модуляция осуществляется через адресацию этого сигнала в множестве $\Phi = \{\Phi_0, \Phi_1, ..., \Phi_{N-1}\}$.

Предлагаемый подход минимизирует вносимые искажения используемых контейнеров. Действительно, стегано-контейнер формируется, как и прежде, поэлементным сложением модулированного сигнала и данных контейнера, т.е. вместо (1) теперь имеем:

$$S_i = C_i + G \cdot E_i = C_i + G \cdot \Phi_{M_i}, \quad (4)$$

что приведет к внесению вносимых искажений в диапазоне $-G...G$ (при любом значении k).

Таким образом, предлагаемый метод за счет использования правила (4) позволяет одновременно сокрыть блок из $k \geq 1$ сокрытых информационных бит, а искажения cover file будут такие же, как и в известном способе (1) для $k=1$. В общем случае величина вносимых искажений в предлагаемом методе будет определяться только величиной коэффициента

усиления G, и не будет зависеть от k, т.е. от пропускной способности стеганосистемы. Это основное преимущество предлагаемого способа.

Для восстановления каждого блока $M_i \in \{0,1,...,N-1\}$ информационного сообщения на приемной стороне необходимо определить номер расширяющей последовательности

$$\Phi_{M_i} \in \Phi = \{\Phi_0, \Phi_1, ..., \Phi_{N-1}\}.$$

Для этого предлагается поочередно вычислять коэффициенты корреляции $\rho(\Phi_\ell, S)$ для всех $\forall \ell \in \{0,1,...,N-1\}$. Адрес (порядковый номер) ℓ того дискретного сигнала Φ_ℓ, для которого вычисленный коэффициент корреляции $\rho(\Phi_\ell, S)$ будет максимальным (по всем ℓ), задает десятичное значение блока информационного сообщения $M_i = \ell$, которое было сокрыто на передающей стороне.

Формализуем описанный выше процесс. Для восстановления блока M_i сокрытого сообщения используем корреляционный приемник, правило работы которого состоит в вычислении коэффициента корреляции:

$$\rho(\Phi_\ell, S) = \rho(\Phi_\ell, C + G \cdot E) = \rho(\Phi_\ell, C) + G \cdot \rho(\Phi_\ell, E).$$

Принимая предположение (2) имеем:

$$\rho(\Phi_\ell, S) \approx G \cdot \rho(\Phi_\ell, E) = G \cdot \Phi_\ell \cdot \Phi_{M_i} = G \cdot \sum_{u=0}^{n} \varphi_{\ell_u} \varphi_{M_{i_u}}.$$

Принимая предположение

$$\forall \ell \neq M_i : \ \rho(\Phi_\ell, \Phi_{M_i}) = \sum_{u=0}^{n} \varphi_{\ell_u} \varphi_{M_{i_u}} \approx 0$$

имеем возможные значения:

$$\rho(\Phi_\ell, S) \approx \begin{cases} 0, \ell \neq M_i; \\ G, \ell = M_i. \end{cases}$$

Тогда значение блока M_i информационного сообщения определим по правилу

$$M_i = \ell : \rho(\Phi_{M_i}, S) = \max_{\ell} \rho(\Phi_\ell, S). \quad (5)$$

Таким образом, для восстановления каждого блока M_i информационного сообщения необходимо вычислить не более $N = 2^k$ коэффициентов корреляции $\rho(\Phi_\ell, S)$ и выбрать максимальное значение. Индекс (номер, адрес) ℓ такого ПСП Φ_ℓ и задает значение блока $M_i = \ell$.

Очевидно, что с увеличением размерности блока k вычислительная сложность восстановления сообщения быстро (экспоненциально) возрастает. Это основной недостаток нашего способа. Например, для $k = 10$ необходимо вычислить не более $2^{10} \approx 10^3$ коэффициентов $\rho(\Phi_\ell, S)$, а для $k = 20$ уже $2^{20} \approx 10^6$. В то же время для каждого такого случая качество cover file будет снижаться минимально (так же, как и для способа из раздела 3 при $k = 1$). Рациональным, на наш взгляд, является поиск компромисса между ожидаемой вычислительной сложностью и пропускной способностью стеганосистемы.

Следует отметить, что суть предложенного способа сокрытия данных использует несколько базовых предположений:

• предположение (2) о том, что каждый сигнал из множества Φ не коррелирован с исходным cover file C. В реальных случаях это предположение может не выполняться, однако в работе [32] предложен эффективный способ гарантированного выполнения условия (2) за счет адаптивной (учитывающей статистические свойства cover file) генерации множества Φ;

• предположение о том, что различные сигналы из множества Φ слабокоррелированы, т.е. коэффициент их взаимной корреляции примерно равен нулю: $\forall i \neq j : \rho\left(\Phi_i, \Phi_j\right) \approx 0$. Выполнение этого предположения также обеспечивается на этапе генерации множества Φ.

Экспериментальные исследования

Для оценки качества cover files обычно используют отношения сигнал/шум [34]. Например, пиковое отношение сигнал/шум (Peak signal-to-noise ratio, PSNR), которое характеризует отношение между максимально возможной мощностью сигнала и мощностью искажающего шума. Для удобства PSNR обычно выражается в логарифмической шкале, т.е. в децибелах.

Для монохромного изображения PSNR рассчитывают по среднеквадратической ошибке (mean squared error – MSE) [34]. Например, для монохромного изображения C размером $N_1 \times N_2$ пикселей и его искаженного ошибками приближения S значение MSE определяют по формуле

$$C_{MSE} = \frac{1}{N_1 N_2} \sum_{i=0}^{N_1-1} \sum_{j=0}^{N_2-1} [C(i, j) - S(i, j)]^2 ,$$

где $C(i, j)$ и $S(i, j)$ – значения яркости пикселей с координатами i, j.

Значение PSNR, выраженное в логарифмической шкале (т.е. в децибелах), определяют как

$$PSNR = 10 \cdot \log_{10}\left(\frac{C_{\max}^2}{C_{MSE}}\right) = 20 \cdot \log_{10}\left(\frac{C_{\max}}{\sqrt{C_{MSE}}}\right) =$$
$$= 20 \cdot \log_{10}\left(C_{\max}\right) - 10 \cdot \log_{10}\left(C_{MSE}\right),$$

где $C_{\max}$ – максимально возможное значение пикселя изображения.

Если для кодирования яркости каждого пикселя используется m бит, тогда $C_{\max} = 2^m - 1$. Например, для $m = 8$ имеем $C_{\max} = 255$ и PSNR рассчитывается по формуле

$$PSNR = 20 \cdot \log_{10}\left(255\right) - 10 \cdot \log_{10}\left(C_{MSE}\right).$$

Для проведения экспериментов мы использовали стандартное тестовое изображение (standard test image) Lenna, размером 256×256 пикселей, при кодировании каждого монохромного полутонового пикселя одним байтом (см. рис. 1). На рис. 2 – 5 приведены примеры соответствующих cover images при сокрытии информационных сообщений с использованием правила (1) с $G = 4$:

- рис. 2 соответствует случаю $k = 1$;
- рис. 3 соответствует случаю $k = 2$;
- рис. 4 соответствует случаю $k = 4$;
- рис. 5 соответствует случаю $k = 8$.

На рис. 6 приведен пример cover image при сокрытии информационных сообщений с использованием правила (5) с $k = 8$ и $G = 4$.

Рис. 1. Стандартное тестовое изображение Lenna

Рис. 2. Cover image, правило сокрытия (1), $k=1$, $G=4$

Рис. 3. Cover image, правило сокрытия (1), $k=2$, $G=4$

Рис. 4. Cover image, правило сокрытия (1), $k=4$, $G=4$

Рис. 5. Cover image, правило сокрытия (1), $k=8$, $G=4$

Рис. 6. Cover image, правило сокрытия (5), $k=8$, $G=4$

Сокрытие информационных сообщений было реализовано программно с использованием системы компьютерной алгебры MathCad. Для формирования множества $\text{ПСП}\,\Phi=\{\Phi_0,\Phi_1,...,\Phi_{N-1}\}$ использован встроенный в MathCad генератор случайных чисел,

длина ПСП была выбрана $n = 256$. Для снижения BER дополнительно осуществлялась отбраковка ПСП по критерию

$$\forall i : \left|\rho\left(\Phi_i, C\right)\right| \le \rho_{\max} = 1000,$$

так как это было реализовано в [32].

Сокрытие k информационных бит последовательно осуществлялось в каждую из 256 строк изображения. Таким образом, в качестве C использовалась одна из строк контейнера-изображения 256×256 пикселей.

Для таких параметров и при $G = 4$ имеем

$$\rho_{\max} = 1000 < G \cdot n = 1024.$$

Практически достигается безошибочное (BER≈0) восстановление информационных сообщений [32].

На рис. 7 и 8 представлены зависимости MSE и PSNR от k для различных значений G. Сплошные линии соответствуют правилу сокрытия информации (1), пунктирные линии – правилу (2).

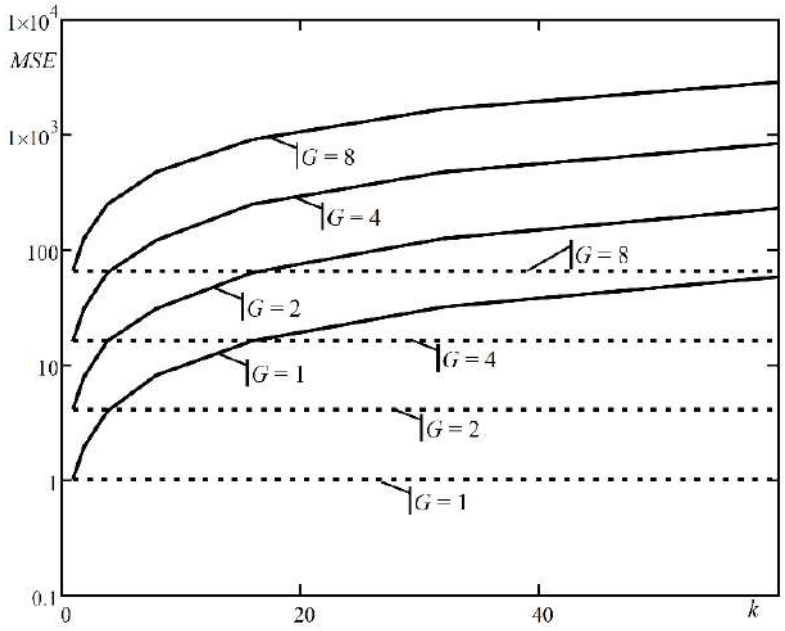


Рис. 7. Зависимости MSE от k

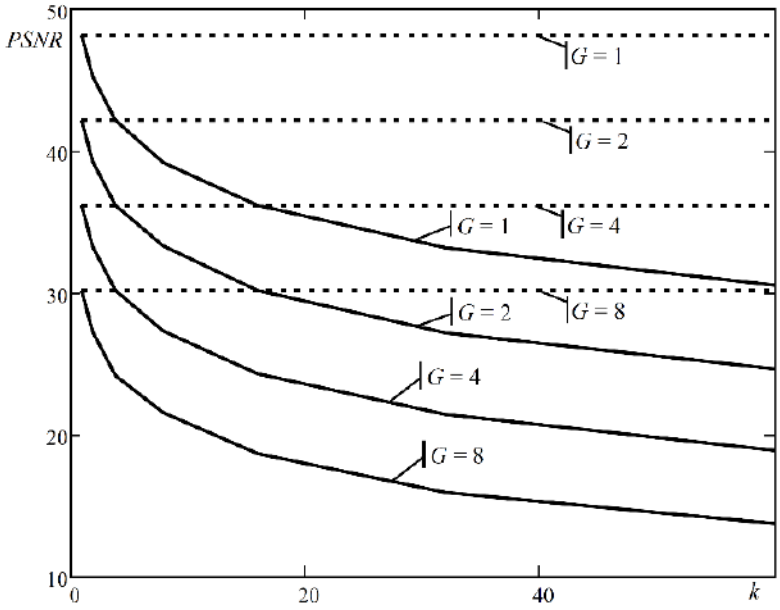


Рис. 8. Зависимости PSNR от k

Как видно из приведенных результатов, предлагаемый способ действительно позволяет существенно снизить искажения cover file. Например, качество изображения на рис. 6 сопоставимо с качеством рис. 2. Однако число сокрытых бит данных при использовании правила (4) увеличено в $k=8$ раз. Дальнейшее увеличение значения k не приводит к снижению качества cover images и рис. 7, 8 наглядно это подтверждают. Напротив, повышение числа k при использовании известного правила (1) приводит к неизбежному снижению качества изображения.

Выводы

Технология прямого расширения спектра успешно применяется в стеганографических задачах. С использованием расширяющих ПСП удается надежно скрывать информационные сообщения в cover files. Однако при этом возникают естественные противоречия:

- повышение объема сокрытых данных приводит к снижению качества cover files, например изображений;
- для снижения интенсивности ошибок (BER) в восстановленных сообщениях приходится усиливать ПСП, что еще больше искажает cover files.

В нашей предыдущей работе [32] мы показали, что, используя специальные способы формирования ПСП, можно существенно снизить BER (при выполнении ряда ограничений добиться практически безошибочного восстановления сообщений, т.е. BER≈0). Однако качество cover files при сокрытии все равно снижается.

В данной работе мы предложили новый метод сокрытия информации на основе адресации ПСП. Этот способ ведет к резкому увеличению вычислительной сложности (для восстановления сообщений необходимо многократно вычислять коэффициенты корреляции со всеми возможными ПСП). Однако качество cover files при этом практически не снижается. Наши эксперименты наглядно это подтверждают.

Перспективным направлением дальнейших исследований является использование ПСП с особыми корреляционными свойствами, например из [35 – 37]. Это направление представляется особенно актуальным для одновременного снижения BER и MSE. Кроме того, важным является также обоснование рекомендаций по выбору компромисса между величиной k и ожидаемой вычислительной сложностью при реализации правила (5).

Список литературы:

1. Menezes A.J., Oorschot P.C. van Vanstone S.A., Oorschot P.C. van Vanstone S.A. Handbook of Applied Cryptography. CRC Press (2018). https://doi.org/10.1201/9780429466335.
2. Cox I., Miller M., Bloom J., Fridrich J., Kalker T. Digital Watermarking and Steganography. 2nd Ed. Morgan Kaufmann, Amsterdam; Boston (2007).
3. Fridrich J. Steganography in Digital Media Principles, Algorithms, and Applications. Cambridge University Press, Cambridge; New York (2009).
4. Rubinstein-Salzedo S. Cryptography. Springer International Publishing, Cham (2018). https://doi.org/10.1007/978-3-319-94818-8.
5. Delfs H., Knebl H. Introduction to Cryptography. Springer Berlin Heidelberg, Berlin, Heidelberg (2015). https://doi.org/10.1007/978-3-662-47974-2.
6. Singh A.K., Kumar B., Singh G., Mohan A. Secure Spread Spectrum Based Multiple Watermarking Technique for Medical Images // Singh A.K., Kumar B., Singh G. and Mohan A. (eds.) Medical Image Watermarking: Techniques and Applications. pp. 125–157. Springer International Publishing, Cham (2017). https://doi.org/10.1007/978-3-319-57699-2_6.
7. Menon N., Vaithiyanathan A survey on image steganography // 2017 International Conference on Technological Advancements in Power and Energy (TAP Energy). pp. 1–5 (2017). https://doi.org/10.1109/TAPENERGY.2017.8397274.
8. Qin J., Luo Y., Xiang X., Tan Y., Huang H. Coverless Image Steganography: A Survey // IEEE Access. 7, 171372–171394 (2019). https://doi.org/10.1109/ACCESS.2019.2955452.
9. Schöttle P., Böhme R.: Game Theory and Adaptive Steganography // IEEE Transactions on Information Forensics and Security. 11, 760–773 (2016). https://doi.org/10.1109/TIFS.2015.2509941.
10. Yahya A. Introduction to Steganography // Yahya, A. (ed.) Steganography Techniques for Digital Images. pp. 1–7. Springer International Publishing, Cham (2019). https://doi.org/10.1007/978-3-319-78597-4_1.

11. Li M., Guo Y., Wang B., Kong X. Secure spread-spectrum data embedding with PN-sequence masking // Signal Processing: Image Communication. 39, 17–25 (2015). https://doi.org/10.1016/j.image.2015.07.014.

12. Pomponiu V., Cavagnino D., Botta M. SS-SVD: Spread spectrum data hiding scheme based on Singular Value Decomposition // 2015 International Symposium on Consumer Electronics (ISCE). pp. 1–2 (2015). https://doi.org/10.1109/ISCE.2015.7177769.

13. Hua G. Over-Complete-Dictionary-Based Improved Spread Spectrum Watermarking Security // IEEE Signal Processing Letters. 27, 770–774 (2020). https://doi.org/10.1109/LSP.2020.2986154.

14. Kokui N., Kang H., Iwamura K., Echizen I. Best embedding direction for spread spectrum-based video watermarking // 2016 IEEE 5th Global Conference on Consumer Electronics. pp. 1–3 (2016). https://doi.org/10.1109/GCCE.2016.7800389.

15. Torrieri D.: Principles of Spread-Spectrum Communication Systems // Springer International Publishing (2018). https://doi.org/10.1007/978-3-319-70569-9.

16. Ipatov V.P. Spread Spectrum and CDMA: Principles and Applications. John Wiley & Sons, Ltd, Chichester, UK (2005). https://doi.org/10.1002/0470091800.

17. Sklar B. Digital Communications: Fundamentals and Applications. Prentice Hall, Upper Saddle River, NJ (2017).

18. Marvel L.M., Boncelet C.G., Retter C.T. Spread spectrum image steganography // IEEE Transactions on Image Processing. 8, 1075–1083 (1999). https://doi.org/10.1109/83.777088.

19. Marvel L.M., Boncelet C.G., Retter C.T. Methodology of Spread-Spectrum Image Steganography. ARMY RESEARCH LAB ABERDEEN PROVING GROUND MD (1998).

20. Brundick F.S., Marvel L.M. Implementation of Spread Spectrum Image Steganography: Defense Technical Information Center, Fort Belvoir, VA (2001). https://doi.org/10.21236/ADA392155.

21. Eze P.U., Parampalli U., Evans R.J., Liu D. Spread Spectrum Steganographic Capacity Improvement for Medical Image Security in Teleradiology* // 2018 40th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC). pp. 1–4 (2018). https://doi.org/10.1109/EMBC.2018.8512344.

22. Nugraha R.M. Implementation of Direct Sequence Spread Spectrum steganography on audio data // Proceedings of the 2011 International Conference on Electrical Engineering and Informatics. pp. 1–6 (2011). https://doi.org/10.1109/ICEEI.2011.6021662.

23. Youail R.S., Samawi V.W., Kadhim A.-K.A.-R. Combining a spread spectrum technique with error-correction code to design an immune stegosystem // Security and Identification 2008 2nd International Conference on Anti-counterfeiting. pp. 245–248 (2008). https://doi.org/10.1109/IWASID.2008.4688395.

24. Yadav, P., Dutta, M.: 3-Level security based spread spectrum image steganography with enhanced peak signal to noise ratio. In: 2017 Fourth International Conference on Image Information Processing (ICIIP). pp. 1–5 (2017). https://doi.org/10.1109/ICIIP.2017.8313696.

25. Smith J.R., Comiskey B.O. Modulation and information hiding in images // Anderson, R. (ed.) Information Hiding. pp. 207–226. Springer, Berlin, Heidelberg (1996). https://doi.org/10.1007/3-540-61996-8_42.

26. US-6557103-B1 – Spread Spectrum Image Steganography | Unified Patents, https://portal.unifiedpatents.com/patents/patent/US-6557103-B1, last accessed 2020/09/14.

27. Zarmehi N., Akhaee M.A. Video steganalysis of multiplicative spread spectrum steganography // 2014 22nd European Signal Processing Conference (EUSIPCO). pp. 2440–2444 (2014).

28. Ustubioglu A., Ulutas G., Ulutas M. DCT based image watermarking method with dynamic gain // 2015 38th International Conference on Telecommunications and Signal Processing (TSP). pp. 550–554 (2015). https://doi.org/10.1109/TSP.2015.7296323.

29. Agrawal N., Gupta A. DCT Domain Message Embedding in Spread-Spectrum Steganography System // 2009 Data Compression Conference. pp. 433–433 (2009). https://doi.org/10.1109/DCC.2009.86.

30. Weihua X., Yongbing W., Shuiyuan Y. H.264 Video Watermark Algorithm Using DCT Spread Spectrum // 2015 3rd International Conference on Applied Computing and Information Technology/2nd International Conference on Computational Science and Intelligence. pp. 447–450 (2015). https://doi.org/10.1109/ACIT-CSI.2015.84.

31. Ling Lu, Xinde Sun, Leiting Cai. A robust image watermarking based on DCT by Arnold transform and spread spectrum // 2010 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE). pp. V1-198-V1-201 (2010). https://doi.org/10.1109/ICACTE.2010.5579033.

32. Kuznetsov A., Smirnov O., Onikiychuk A., Makushenko T., Anisimova O., Arischenko A. Adaptive Pseudo-Random Sequence Generation for Spread Spectrum Image Steganography // 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT). pp. 161–165 (2020). https://doi.org/10.1109/DESSERT50317.2020.9125032.

33. Kuznetsov A., Smirnov A., Gorbacheva L., Babenko V. Hiding data in cover images using a pseudo-random sequences // Subbotin S. (ed.) Proceedings of The Third International Workshop on Computer Modeling and Intelligent Systems (CMIS-2020), Zaporizhzhia, Ukraine, April 27-May 1, 2020. pp. 646–660. CEUR-WS.org (2020).

34. Korhonen J., You J. Peak signal-to-noise ratio revisited: Is simple beautiful? // 2012 Fourth International Workshop on Quality of Multimedia Experience. pp. 37–38 (2012). https://doi.org/10.1109/QoMEX.2012.6263880.

35. Kuznetsov A., Smirnov O., Kovalchuk D., Pastukhov M., Kuznetsova K., Prokopovych-Tkachenko D. Discrete Signals with Special Correlation Properties // Luengo D., Subbotin S., Arras P., Bodyanskiy Y., Henke K., Izonin

I., Levashenko V.G., Lytvynenko V., Parkhomenko A., Pester A., Shakhovska N., Sharpanskykh A., Tabunshchyk G., Wolff C., Wuttke H.-D., and Zaitseva E. (eds.) Proceedings of the Second International Workshop on Computer Modeling and Intelligent Systems (CMIS-2019), Zaporizhzhia, Ukraine, April 15-19, 2019. pp. 618–629. CEUR-WS.org (2019).

36. Kuznetsov A., Smirnov O., Reshetniak O., Ivko T., Kuznetsova T., Katkova T. Generators of Pseudorandom Sequence with Multilevel Function of Correlation // 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S T). pp. 517–522 (2019). https://doi.org/10.1109/PICST47496.2019.9061530.

37. Kuznetsov A., Kiian A., Kuznetsova K., Zub M., Zaburmekha Y., Lyshchenko E. Pseudorandom Sequences with Multi-Level Correlation Function for Direct Spectrum Spreading // 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT). pp. 232–237 (2019). https://doi.org/10.1109/ATIT49449.2019.9030436.

Поступила в редколлегию 23.09.2020

Сведения об авторах:

Кузнецов Александр Александрович – д-р техн. наук, профессор, профессор кафедры безопасности информационных систем и технологий, факультет компьютерных наук, Харьковский национальный университет имени В.Н. Каразина, Украина; e-mail: kuznetsov@karazin.ua, ORCID: https://orcid.org/0000-0003-2331-6326

Смирнов Алексей Анатольевич – д-р техн. наук, профессор, заведующий кафедрой кибербезопасности и программного обеспечения, Центральноукраинский национальный технический университет, м. Кропивницкий, Украина; e-mail: dr.smirnovoa@gmail.com, ORCID: https://orcid.org/0000-0001-9543-874X

Киян Анастасия Сергеевна – здобувач кафедры безопасности информационных систем и технологий, факультет компьютерных наук, Харьковский национальный университет имени В.Н. Каразина, Украина; e-mail: nastyak931@gmail.com, ORCID: https://orcid.org/0000-0003-2110-010X

Кузнецова Татьяна Юрьевна – научный сотрудник научно-исследовательской части, Харьковский национальный университет имени В.Н. Каразина, Украина; e-mail: kuznetsova.tatiana17@gmail.com, ORCID: https://orcid.org/0000-0001-6154-7139

УДК 621.391.15:519.7 **DOI:10.30837/rt.2020.4.203.05**

А.В. БЕССАЛОВ, д-р техн. наук, Л.В. КОВАЛЬЧУК, д-р техн. наук, Н.В. КУЧИНСКАЯ

ОЦЕНКА ЭФФЕКТИВНОСТИ ДИФФЕРЕНЦИАЛЬНОГО СЛОЖЕНИЯ ТОЧЕК КРИВЫХ В ОБОБЩЕННОЙ ФОРМЕ ЭДВАРДСА

Введение

Наряду с бесспорным приоритетом аспектов безопасности значимую роль в современных криптосистемах играет быстродействие. Если на заданном уровне безопасности удастся вдвое сократить время, например на вычисление цифровой подписи, следует ожидать и пропорционального снижения стоимости этой процедуры («время – деньги»). Потому временные затраты на вычисления – важная составляющая эффективности криптосистемы.

В большинстве алгоритмов криптосистем на эллиптических кривых основной и наиболее трудоемким является экспоненцирование точки P или скалярное произведение kP (где число $k < ordP = n$). Сегодня известно множество методов его вычисления [1, 2]. Мы остановились на одном из наиболее изящных – методе дифференциального сложения точек Монтгомери [3], обеспечивающем гарантированную защиту от некоторых атак побочного канала. Вместе с тем, недавно (2017) предложен новый метод реализации дифференциального сложения точек на кривых в форме Эдвардса [4], имеющий, как и для кривых в форме Монтгомери, рекордно низкую сложность вычислений. Прежние сравнительные оценки эффективности вычислений для кривых Эдвардса и других типов кривых [5 – 9] с учетом результатов работы [4] могут быть улучшены. Одной из целей данной статьи является сравнительная оценка скорости экспоненцирования точки на основе алгоритма Монтгомери для кривых в форме Эдвардса и Вейерштрасса. Последние получили наибольшее распространение в современных стандартах асимметричной криптографии, которые, очевидно, требуют обновления.

В разд. 1 даны определения и свойства трех классов кривых в обобщенной форме Эдвардса [7]. Во разд. 2 рассматривается алгоритм Монтгомери дифференциального сложения точек для кривой в форме Монтгомери [3] с оценкой стоимости вычислений на одном шаге рекуррентного цикла. В разд. 3 дан вывод новых формул дифференциального сложения-вычитания и удвоения точек для кривой в обобщенной форме Эдвардса, который не приведен в [4], с первой оценкой стоимости вычислений. В разд. 4 обсуждаются аспекты выбора и оптимизации параметров кривой в обобщенной форме Эдвардса для ее криптографических приложений и стандартизации. Здесь же приведены формулы сложения произвольной точки с одной из четырех особых точек, которые необходимы для построения завершенной арифметики кривых при неполном законе сложения точек. Наконец, в разд. 5 дан краткий сравнительный анализ трех полученных в [4] оценок стоимости вычислений и оценивается потенциальный выигрыш в скорости вычисления скалярного произведения kP на кривых Эдвардса по сравнению с кривыми в форме Вейерштрасса, равный 3,09.

1. Классификация кривых в обобщенной форме Эдвардса

Эллиптическая кривая *в обобщенной форме Эдвардса* [7] определяется уравнением

$$E_{a,d}: x^2 + ay^2 = 1 + dx^2y^2,\ a, d \in F_p^*,\ d \neq 1,\ a \neq d,\ p \neq 2. \quad (1)$$

В отличие от уравнения этой кривой в [6] здесь параметр a умножаем на y^2 вместо x^2. Если квадратичный характер $\chi(ad) = -1$, кривая (1) изоморфна *полной кривой* Эдвардса [5] с одним параметром d

$$E_d: x^2 + y^2 = 1 + dx^2y^2,\ \chi(d) = -1,\ d \neq 0,1. \quad (2)$$

При $\chi(ad)=\chi(a)=\chi(d)=1$ имеет место изоморфизм кривой (1) с *квадратичной кривой Эдвардса* [7]

$$E_d:\ x^2+y^2=1+dx^2y^2,\ \chi(d)=1,\ d\neq 0,1. \tag{3}$$

с одним параметром d, определенным, в отличие от (2), как квадрат. Это отличие ведет к кардинально различным свойствам кривых (2) и (3) [7], которые резюмируются ниже. Несмотря на это, в пионерской статье [6] эти классы кривых объединены общим термином *кривые Эдвардса.*

Наконец, при $\chi(a)=\chi(d)=-1$ кривая (1) попадает в класс *скрученных кривых Эдвардса*. Это единственный случай, оправдывающий введение нового параметра a в уравнение кривой (1) в работе [6].

В работе [7] модифицированный универсальный закон сложения точек кривой (1) имеет вид

$$(x_1,y_1)+(x_2,y_2)=\left(\frac{x_1x_2-ay_1y_2}{1-dx_1x_2y_1y_2},\frac{x_1y_2-x_2y_1}{1+dx_1x_2y_1y_2}\right) \tag{4}$$

При совпадении двух точек получим из (4) закон удвоения точек:

$$2(x_1,y_1)=\left(\frac{x_1^2-ay_1^2}{1-dx_1^2y_1^2},\frac{2x_1y_1}{1+dx_1^2y_1^2}\right) \tag{5}$$

Форма (4), (5) модифицированных законов сложения позволяет сохранить общепринятую горизонтальную симметрию (относительно оси x) обратных точек. Определяя обратную точку как $-P=(x_1,-y_1)$, получим согласно (4) координаты нейтрального элемента группы точек $O=(x_1,y_1)+(x_1,-y_1)=(1,0)$. Кроме нейтрального элемента О на оси x всегда лежит точка $D_0=(-1,0)$ второго порядка, для которой в соответствии с (5) $2D_0=(1,0)=O$. В зависимости от свойств параметров a и d из (1) можно получить еще 2 особые точки 2-го порядка и 2 точки 4-го порядка:

$$D_{1,2}=\left(\pm\sqrt{\frac{a}{d}},\infty\right),\ \pm F_1=\left(\infty,\pm\frac{1}{\sqrt{d}}\right) \tag{6}$$

где знак "∞" мы ставим при делении на 0. Они возникают при $\chi(ad)=1$ и $\chi(d)=1$ соответственно.

В зависимости от свойств параметров a и d кривые в обобщенной форме (1) разбиваются на три непересекающиеся (неизоморфных) класса [7]:

- *полные кривые Эдвардса* с условием С1: $\chi(ad)=-1$;
- *скрученные кривые Эдвардса* с условиями С2.1: $\chi(a)=\chi(d)=-1$;
- *квадратичные кривые Эдвардса* с условиями С2.2: $\chi(a)=\chi(d)=1$.

Перечислим основные свойства этих классов кривых.

1. Порядок N_E кривой (1) делится на 4. В отношении точек 2-го порядка первый класс полных кривых Эдвардса над простым полем является классом *циклических* кривых (с одной точкой 2-го порядка), скрученные же и квадратичные кривые Эдвардса образуют классы *нециклических* кривых (по 3 точки 2-го порядка). Максимальный порядок точек кривых двух последних классов равен $N_E/2$.

2. Класс полных кривых Эдвардса не содержит особых точек.

3. Скрученные и квадратичные кривые Эдвардса образуют пары квадратичного кручения на основе преобразования параметров: $\tilde{a}=ca,\ \tilde{d}=cd,\ \chi(c)=-1$.

4. Скрученные кривые Эдвардса содержат лишь две особые точки 2-го порядка $D_{1,2}=\left(\pm\sqrt{\frac{a}{d}},\infty\right)$, а квадратичные кривые Эдвардса, кроме них – еще две особые точки 4-го порядка $\pm F_1=\left(\infty,\pm\frac{1}{\sqrt{d}}\right)$.

5. В классах скрученных и квадратичных кривых Эдвардса замена $a\leftrightarrow d$ дает изоморфизм $E_{a,d}\sim E_{d,a}$

6. Полные и квадратичные кривые Эдвардса изоморфны кривым с параметром $a=1$: $E_{a,d}\sim E_{1,d/a}$.

7. Скрученные кривые Эдвардса при $p\equiv 1\bmod 4$ не имеют точек 4-го порядка и имеют порядок $N_E=4n$ (n – нечетное).

8. Для точек нечетного порядка закон сложения точек (4) кривой (1) полный (не образует особых точек).

Заметим, что в расширении F_{p^2} простого поля F_p все 3 класса кривых Эдвардса, заданных над простым полем, приобретают свойства квадратичных кривых (3).

2. Алгоритм Монтгомери вычисления скалярного произведения точки эллиптической кривой

Эффективный алгоритм Монтгомери [3] вычисления точки $Q=kP$ скалярного произведения успешно решает две задачи: противодействие атаке побочного канала типа «оценка парциальных вычислительных затрат» и повышение скорости экспоненцирования точки. Пусть число k представлено в двоичной форме $k=\left(k_{m-1},k_{m-2},...,k_0\right)_2$, где $k=\sum_{i=0}^{m-1}k_i 2^i$, $k_i\in\{0,1\}$, тогда классический алгоритм удвоений-сложений точек на каждом шаге (или одном бите m-битного числа k) последовательно удваивает предыдущий результат и, если $k_i=1$ складывает его с точкой P. Так как в среднем при числе m удвоений число сложений равно $m/2$, измерение времени вычислений на каждом шаге алгоритма позволяет мониторящему канал противнику организовать известную атаку побочного канала. Полезной для него информацией является также различие вычислительной сложности сложения и удвоения точки. В работе [3] Питер Монтгомери предложил алгоритм дифференциального сложения точек ($dADD$) в котором на каждом шаге алгоритма выполняются обе операции: сложения и удвоения точек. Очевидно, в этом случае атака подобного типа становится бессмысленной.

Алгоритм 1 Монтгомери (*dADD*)

Вход: $P_2\leftarrow O$ (O – нейтральный элемент группы точек);

$P_1\leftarrow P$ (P – базовая точка)

для $i\in m-1..0$

если $k_i=1$: $P_2\leftarrow P_1+P_2$,

$P_1\leftarrow 2P_1$;

если $k_i=0$: $P_1\leftarrow P_1+P_2$,

$P_2\leftarrow 2P_2$.

Выход: $Q=P_2$.

Идея этого алгоритма проста: на каждом шаге цикла разность точек $P_1 - P_2 = P$ остается фиксированной точкой P. В качестве простого примера примем значение $k = (10111)_2 = 23_{10}$. Тогда получим в цикле пары точек $\{P_1, P_2\}$: $\{2P, P\}$, $\{3P, 2P\}$, $\{6P, 5P\}$, $\{12P, 11P\}$, $\{24P, 23P\}$. На выходе – точка $Q = 23P$.

Далее Монтгомери для специфической кривой вида

$$M_{A,B} : By^2 = x^3 + Ax^2 + x, \tag{7}$$

получившей позже название кривой в форме Монтгомери, удалось получить лаконичные выражения для координат суммы точек при известной их разности, а также координат удвоенной точки.

Пусть $P_i = (x_i, y_i), i = \overline{0,4}$. Обозначим $P_0 = P_1 - P_2 = P$, $P_3 = P_1 + P_2$, $P_4 = 2P_1$. Для координат сложения, вычитания и удвоения точек кривой (7) в работе [3] получены выражения:

$$x_0 x_3 = \frac{(x_1 x_2 - 1)^2}{(x_1 - x_2)^2}, \tag{8}$$

$$x_4 = \frac{\left(x_1^{\,2} - 1\right)^2}{4x_1\left((x_1 + 1)^2 + ex_1\right)}, e = (A + 2). \tag{9}$$

Характерно, что x-координаты точек P_0, P_3, P_4 зависят лишь от x-координат складываемых точек. Поэтому в [3] введены проективные координаты $(X : Z)$ для рекуррентных вычислений без инверсий с восстановлением y-координаты на финальном шаге процедуры. Согласно (8) и (9) они имеют вид:

$$\begin{aligned} X_3 &= Z_0 (X_1 X_2 - Z_1 Z_2)^2, \\ Z_3 &= X_0 (X_1 Z_2 - X_2 Z_1)^2, \\ X_4 &= \left(X_1^2 - Z_1^2\right)^2 \\ Z_4 &= 4X_1 Z_1 \left((X_1 + Z_1)^2 + X_1 Z_1\right)^2. \end{aligned} \tag{10}$$

Если M – вычислительная стоимость умножения элементов поля, S – стоимость возведения в квадрат, U – стоимость умножения на константу e, то, игнорируя незначительные затраты на сложение в поле, получим из (10) стоимость сложения точек $C(P_1 + P_2) = 6M + 2S$, стоимость удвоения точек $C(2P_1) = 2M + 4S + 1U$ Поскольку базовая точка $P = P_0 = (X_0 : Z_0)$ является фиксированной, можно принять $Z_0 = 1$ (т.е. точка P является аффинной), при этом $C(P_1 + P_2) = 5M + 2S$, а суммарная стоимость равна $C(P_1 + P_2, 2P_1) = 7M + 6S + 1U$. Для минимизации вычислений Монтгомери представил формулы (10) в виде:

$$X_3 = \left[(X_1 - Z_1)(X_2 + Z_2) + (X_1 + Z_1)(X_2 - Z_2)\right]^2,$$

$$Z_3 = X_0\left[(X_1 - Z_1)(X_2 + Z_2) + (X_1 + Z_1)(X_2 - Z_2)\right]^2,$$

$$X_4 = (X_1 - Z_1)^2 (X_1 + Z_1)^2,$$

$$Z_4 = 4X_1Z_1\left((X_1 + Z_1)^2 + eX_1Z_1\right). \qquad (11)$$

При вычислении X_4 учтем бесплатный промежуточный результат, который используется при расчете Z_4:

$$4X_1Z_1 = (X_1 + Z_1)^2 - (X_1 - Z_1)^2.$$

Тогда $C(P_1 + P_2) = 3M + 2S$, $C(2P_1) = 2M + 2S + 1U$. Суммарная стоимость этих двух операций равна $C(P_1 + P_2, 2P_1) = 5M + 4S + 1U$. Этот результат для кривых в форме Монтгомери (7) и сегодня является рекордом минимальной вычислительной сложности выполнения двух операций – сложения и удвоения точек.

Примечание. Проективные координаты, использующие некоторые аффинные точки, называют смешанными проективными координатами (mixed projective coordinates).

3. Проективные координаты Фарашахи – Хоссейни для кривых в обобщенной форме Эдвардса

Поскольку эллиптические кривые в форме Монтгомери (7) и Эдвардса (1) бирационально эквивалентны [6], следует ожидать близких результатов оценки вычислительной сложности для кривых в форме (1). Если операции (4), (5) выполнять в классических проективных координатах $(X:Y:Z)$, то полученные в [6] оценки для кривых (1) составляют $C(P_1 + P_2) = 10M + 1S + 2U$, $C(2P_1) = 3M + 4S + 1U$. Суммарная стоимость этих двух операций при этом равна $C(P_1 + P_2, 2P_1) = 13M + 5S + 3U$, что более чем вдвое проигрывает кривым (7). Одной из очевидных причин этого является использование в расчетах обеих координат X и Y кривой (1) вместо одной X-координаты кривой (7) (Z-координаты во всех случаях заменяют инверсию).

Авторы работы [4] нашли эффективное решение этой проблемы. В уравнении (1) обе координаты представлены последним слагаемым $w(x, y) = dx^2y^2$, а это позволяет предположить, что по аналогии с методом дифференциального сложения точек Монтгомери (при $w(x, y) = x$)), можно выразить формулы сложения-вычитания и удвоения точек кривой Эдвардса с помощью одной интегральной координаты w. В основе такой идеи лежит бирациональная эквивалентность кривых (7) и (1) с рациональным преобразованием координат $\frac{x}{y} \to y$, $\frac{x-1}{x+1} \to x$ [6]. В разд. 4 работы [4] приводятся итоговые формулы дифференциального сложения точек для кривых в форме (1) без их выводов. В связи с их нетривиальностью ниже даем подробный вывод этих формул. Как отмечалось в разд. 1, мы используем формулы (4), (5) с заменой $x \leftrightarrow y$ в [4].

Сложение-вычитание точек

Пусть $P_i = (x_i, y_i)$, $w_i = w(P_i) = dx_i^2 y_i^2, i = \overline{0,3}$. Обозначим $P_0 = P_1 - P_2$, $P_3 = P_1 + P_2$, $w_0 = w(P_0)$, $w_3 = w(P_3)$. Тогда согласно (4)

$$P_0 = (x_0, y_0) = \left(\frac{x_1x_2 + ay_1y_2}{1 + dx_1x_2y_1y_2}, \frac{-x_1y_2 + x_2y_1}{1 - dx_1x_2y_1y_2}\right),$$

$$P_3 = (x_3, y_3) = \left(\frac{x_1 x_2 - a y_1 y_2}{1 - d x_1 x_2 y_1 y_2}, \frac{x_1 y_2 + x_2 y_1}{1 + d x_1 x_2 y_1 y_2} \right).$$

Отсюда

$$w_0 w_3 = (d x_0 y_0 x_3 y_3)^2 = d^2 \left[\left(\frac{(x_1 x_2)^2 - (a y_1 y_2)^2}{1 - w_1 w_2} \right) \left(\frac{(x_2 y_1)^2 - (x_1 y_2)^2}{1 - w_1 w_2} \right) \right]^2 \quad (12)$$

Сомножитель числителя преобразуем как

$$I = \left(\left((x_1 x_2)^2 - (a y_1 y_2)^2 \right) \left((x_2 y_1)^2 - (x_1 y_2)^2 \right) \right) =$$

$$= x_1^2 y_1^2 x_2^4 - a^2 x_2^2 y_2^2 y_1^4 - x_2^2 y_2^2 x_1^4 + a^2 x_1^2 y_1^2 y_2^4 =$$

$$= x_1^2 y_1^2 \left(x_2^4 + a^2 y_2^4 \right) - x_2^2 y_2^2 \left(x_1^4 + a^2 y_1^4 \right).$$

Так как

$$\left(x_i^2 + a y_i^2 \right) = 1 + w_i, \; i = 1, 2,$$

тогда

$$\left(x_i^4 + a y_i^4 \right) = (1 + w_i)^2 - 2 a d^{-1} w_i, \; i = 1, 2,$$

и можно получить

$$I = d^{-1} \left[w_1 \left((1 + w_2)^2 - 2 a d^{-1} w_2 \right) \right] - d^{-1} \left[w_2 \left((1 + w_1)^2 - 2 a d^{-1} w_1 \right) \right] =$$

$$= d^{-1} \left[w_1 + w_1 w_2^2 - w_2 - w_2 w_1^2 \right] = d^{-1} \left(w_1 - w_2 \right) \left(1 - w_1 w_2 \right).$$

С учетом этого равенство (6) принимает вид

$$w_0 w_3 = d^2 \frac{I^2}{(1 - w_1 w_2)^4} = \frac{(w_1 - w_2)^2}{(1 - w_1 w_2)^2}. \quad (13)$$

Удвоение точек

Пусть $P_1 = (x_1, y_1)$, $P_4 = 2P_1$, $w_1 = w(P_1)$, $w_4 = w(2P_1)$.

Согласно (5) и принятым обозначениям

$$2P_1 = \left(\frac{x_1^2 - a y_1^2}{1 - d x_1^2 y_1^2}, \frac{2 x_1 y_1}{1 + d x_1^2 y_1^2} \right) = \left(\frac{x_1^2 - a y_1^2}{1 - w_1}, \frac{2 x_1 y_1}{1 + w_1} \right),$$

$$w_4 = d \left(\left(\frac{x_1^2 - a y_1^2}{1 - w_1} \right) \left(\frac{2 x_1 y_1}{1 + w_1} \right) \right)^2 = 4 w_1 \left(\frac{\left(x_1^2 - a y_1^2 \right)^2}{\left(1 - w_1^2 \right)^2} \right).$$

В последней формуле сомножитель в числителе преобразуется к виду

$$\left(x_1^2 - ay_1^2\right)^2 = \left(x_1^2 + ay_1^2\right)^2 - 4ax_1^2y_1^2 = \left(1+w_1\right)^2 - 4ad^{-1}w_1.$$

В итоге

$$w_4 = \frac{4w_1\left(\left(1+w_1^2\right)^2 - cw_1\right)}{\left(1-w_1^2\right)^2}, c = 4ad^{-1} \tag{14}$$

Формулы (13) и (14) с целью вычисления инверсий Z представляются в проективных координатах $(W:Z)$ как:

$$W_3 = Z_0\left[\left(W_1 - Z_1\right)\left(W_2 + Z_2\right) - \left(W_1 + Z_1\right)\left(W_2 - Z_2\right)\right]^2,$$

$$Z_3 = W_0\left[\left(W_1 - Z_1\right)\left(W_2 + Z_2\right) + \left(W_1 + Z_1\right)\left(W_2 - Z_2\right)\right]^2,$$

$$W_4 = 4W_1Z_1\left(\left(W_1 + Z_1\right)^2 - cW_1Z_1\right), c = 4ad^{-1},$$

$$Z_4 = \left(W_1 - Z_1\right)^2\left(W_1 + Z_1\right)^2. \tag{15}$$

Нельзя не заметить, что они мало отличаются от формул (11) для координат $(X:Z)$ кривой в форме Монтгомери после обращения $X \leftrightarrow W^{-1}$. Как и для кривой (7), с учетом $Z_0 = 1$, стоимость вычислений сложения и удвоения точек на одном шаге алгоритма Монтгомери $dADD$ минимальна и равна $C\left(P_1 + P_2, 2P_1\right) = 5M + 4S + 1U$.

Следует отметить, что проективные координаты Фарашахи – Хоссейни для кривых (1) оказались также очень перспективными при вычислении изогений нечетных степеней в задачах постквантовой криптографии [10].

4. Специфические свойства приемлемых для криптосистем кривых в обобщенной форме Эдвардса

Из краткого обзора свойств кривых в форме (1) в разд. 1 следует, что кривые классов нециклических скрученных $\left(\chi(a) = \chi(d) = -1\right)$ и квадратичных $\left(\chi(a) = \chi(d) = 1\right)$ кривых Эдвардса содержат соответственно 2 и 4 особых точки 2-го и 4-го порядков (6). В литературе по эллиптической криптографии существует мнение, что это ограничивает применение этих кривых при необходимости выполнения групповых операций с точками четных порядков, так как бесконечная координата особой точки не лежит в конечном поле.

Один из авторов данной статьи в работе [7] ввел соответствующие групповые операции с особыми точками (6):

$$\left(x_1, y_1\right) + \left(\sqrt{\frac{a}{d}}, \infty\right) = \left(\sqrt{\frac{a}{d}} \cdot x_1^{-1}, \frac{1}{\sqrt{ad}} \cdot y_1^{-1}\right),$$

$$\left(x_1, y_1\right) + \left(-\sqrt{\frac{a}{d}}, \infty\right) = \left(-\sqrt{\frac{a}{d}} \cdot x_1^{-1}, -\frac{1}{\sqrt{ad}} \cdot y_1^{-1}\right)$$

$$\left(x_1, y_1\right) + \left(\infty, \frac{1}{\sqrt{d}}\right) = \left(-\frac{1}{\sqrt{d}} \cdot y_1^{-1}, \frac{1}{\sqrt{d}} \cdot x_1^{-1}\right),$$

$$(x_1, y_1)+\left(\infty,-\frac{1}{\sqrt{d}}\right)=\left(\frac{1}{\sqrt{d}}\cdot y_1^{-1},-\frac{1}{\sqrt{d}}\cdot x_1^{-1}\right).$$

Все найденные суммы, полученные с помощью правил предельного перехода, удовлетворяют уравнению (1) при подстановке, т.е. являются точками кривой. Эти формулы снимают теоретические ограничения в задаче построения арифметики группы точек в условиях неполноты закона сложения (4).

Вместе с тем, наличие особых точек (6) в криптоалгоритмах нежелательно в связи с проблемами программирования и снижением скорости выполнения алгоритмов. Однако в большинстве криптопримитивов точки четных порядков не используются. В их отсутствие закон сложения точек является полным (свойство 8 раздела 1).

Наиболее целесообразным следует считать выбор для криптосистемы кривой (1) порядка $N_E = 4n$ (n – простое) с минимальным кофактором 4. Такой кофактор при $p \equiv 1 mod 4$ имеет порядка половины всех полных кривых Эдвардса (2) и всех скрученных кривых Эдвардса (1) ($\chi(a) = \chi(d) = -1$) [7].

Циклические полные кривые (2) содержат точки порядков 2, 4, n, $2n$, $4n$. Подкласс нециклических скрученных кривых Эдвардса при $p \equiv 1 \bmod 4$ содержат точки порядков 2, n, $2n$. В криптосистеме базовой является точка $P, ordP = n$. Такая точка в подклассе скрученных кривых Эдвардса находится наиболее просто – с помощью единственной групповой операции удвоения случайной точки. Это существенно упрощает задачу нахождения генератора (базовой точки P) на этапе вычисления общесистемных параметров криптосистемы. Для точек циклической группы $\langle P \rangle$ закон сложения точек (4) кривой (1) является полным. Отмеченные преимущества (минимальный кофактор порядка кривой 4, минимальный набор порядков точек 2, n $2n$, простое вычисление базовой точки P) позволяют рекомендовать данный подкласс скрученных кривых Эдвардса при проектировании и стандартизации криптосистем. Это не исключает применение для этих целей и полных кривых Эдвардса с порядком $N_E = 4n$.

Операция скалярного произведения kP является основной в большинстве алгоритмов эллиптической криптографии. Наиболее безопасным к атакам побочного канала является алгоритм Монтгомери дифференциального сложения точек с рекордным быстродействием для кривых в форме Монтгомери и Эдвардса с использованием проективных координат Фарашахи – Хоссейни.

Дальнейшего снижения вычислительных затрат при вычислении скалярного произведения kP на скрученной кривой Эдвардса можно достичь минимизацией константы $c = 4ad^{-1}$ в формуле (15) для координаты W_4. Если принять $p \equiv 5 \bmod 8$, можно зафиксировать $d = 2$ как минимальный квадратичный невычет простого поля F_p, тогда $c = 2a$ После этого методом наращивания квадратичных невычетов a можно найти кривую приемлемого порядка $N_E = 4n$ (n – простое). Решение этой задачи позволяет получить минимальную оценку стоимости вычислений на одном шаге алгоритма Монтгомери $C(P_1 + P_2, 2P_1) = 5M + 4S$.

5. К оценке эффективности метода дифференциального сложения точек Монтгомери на кривых Эдвардса

В работе [4] получены 3 оценки стоимости вычислений для кривых (1)

$$C_1(P_1 + P_2, 2P_1) = 5M + 4S + 1U,$$

$$C_2(P_1 + P_2, 2P_1) = 3M + 7S + 1U,$$

$$C_3\left(P_1+P_2,2P_1\right)=3M+6S+3U\,.$$

Две последние оценки C_2 и C_3 получены из первой путем модификаций расчетных формул. Кроме того, оценка C_3 справедлива лишь для некоторого семейства класса полных кривых Эдвардса. Если воспользоваться известной оценкой $1S=2/3M$ [5], то получим $C_1=7.67M+1U$, $C_2=7.67M+1U$, $C_3=7M+3U$. При этом, мы видим, что две первые оценки равнозначны, а последняя может быть полезной для полных кривых Эдвардса лишь при очень малых значениях констант, для которых $U<0{,}17M$.

В предыдущих наших работах [7 – 9] проводился сравнительный анализ скорости вычисления скалярного произведения kP в проективних координатах $\left(X:Y:Z\right)$ для кривых в формах Эдвардса и Вейерштрасса. Использование классического метода последовательных удвоений и сложений точек обеспечивает максимальный выигрыш первых в быстродействии до 1,61 раза. Для кривых в форме Вейерштрасса стоимости вычислений составляют $C_W\left(P_1+P_2\right)=12M+2S$, $C_W\left(2P_1\right)=7M+5S$ [7]. Так как алгоритм сложений и удвоений точек Монтгомери можно реализовать для любого типа кривой, то для кривой в форме Вейерштрасса стоимость одного бита вычисления kP составит $C_W\left(P_1+P_2,2P_1\right)=19M+7S$. Тогда, с учетом оценки $1S=2/3M$, имеем $C_W\left(P_1+P_2,2P_1\right)=23.67M$. Если константой $c=4ad^{-1}$ в (15) можно пренебречь (это достигается методом, описанным в разд. 4), потенциальный выигрыш в скорости вычислений для кривой в форме Эдвардса (1) составит $\frac{C_W}{C_1}=\frac{23.67}{7.67}=3.09$.

Заключение

Проведенный анализ позволяет заключить, что алгоритм дифференциального сложения точек Монтгомери с его реализацией на скрученных кривых Эдвардса в проективных координатах Фарашахи – Хоссейни является на сегодня наиболее быстрым и безопасным к атакам побочного канала методом экспоненцирования точки кривой. Его можно рекомендовать при проектировании криптосистем и новых стандартов допостквантовой эллиптической криптографии.

Список литературы:

1. Menezes A., van Oorshot P.C., Vanstone S.A. Handbook of Applied Cryptography. CRC press, New York, 2006.
2. Washington L.C. Elliptic Curvres. Number Theory and Cryptography. Second Edition. CRC Press, 2008.
3. Montgomery, P.L. Speeding the Pollard and elliptic curve methods of factorization // Math. Comp. 48(177). P. 243–264 (1987).
4. Farashahi R.R., Hosseini S.G. Differential addition on twisted Edwards curves // Pieprzyk J., Suriadi S. (eds.) Information Security and Privacy. pp. 366-378. Springer International Publishing, Cham (2017).
5. Bernstein D.J., Lange T. Faster Addition and Doubling on Elliptic Curves // Advances in Cryptology – ASIACRYPT'2007 (Proc. 13th Int. Conf. on the Theory and Application of Cryptology and Information Security. Kuching, Malaysia. December 2–6, 2007). Lect. Notes Comp. Sci. V. 4833. Berlin: Springer, 2007. P. 29–50.
6. Bernstein Daniel J., Birkner Peter, Joye Marc, Lange Tanja, Peters Christiane. Twisted Edwards Curves // IST Programme under Contract IST–2002–507932 ECRYPT,and in part by the National Science Foundation under grant ITR–0716498, 2008. P. 1-17.
7. Бессалов А.В. Эллиптические кривые в форме Эдвардса и криптография : монография. Киев : Политехника, 2017. 272с.
8. Бессалов А.В., Дихтенко А.А., Третьяков Д.Б. Сравнительная оценка быстродействия канонических эллиптических кривых и кривых в форме Эдвардса над конечным полем // Сучасний захист інформації. 2011. №4. С.33-36.
9. Бессалов А.В., Цыганкова О.В. Производительность групповых операций на скрученной кривой Эдвардса над простым полем // Радиотехника. 2015. №181. С.58-63.

10. Suhri Kim, Kisoon Yoon, Young-Ho Park, and Seokhie Hong. Optimized Method for Computing Odd-Degree Isogenies on Edwards Curves. Center for Information Security Technologies (CIST), Korea University, Seoul,Republic of Korea, 2018.

Поступила в редколлегию 07.10.2020

Сведения об авторах:

Бессалов Анатолий Владимирович – д-р техн. наук, профессор, профессор кафедры информационной и кибернетической безопасности, Киевский Университет имени Бориса Гринченко, Украина; e-mail: a.bessalov@kubg.edu.ua, ORCID: https://orcid.org/0000-0002-6967-5001

Ковальчук Людмила Васильевна – д-р техн. наук, професор, профессор кафедры математических методов защиты информации, Национальный технический университет Украины "Киевский политехнический институт имени Игоря Сикорского", Украина; e-mail: lusi.kovalchuk@gmail.com, ORCID: https://orcid.org/0000-0003-2874-7950

Кучинская Наталия Викторовна – доцент кафедры математических методов защиты информации, Национальный технический университет Украины "Киевский политехнический институт имени Игоря Сикорского", Украина; e-mail: n.kuchinska@gmail.com, ORCID: https://orcid.org/0000-0002-6457-7525

УДК 004.056.55 **DOI:10.30837/rt.2020.4.203.06**

М.С. ЛУЦЕНКО

ПОСТКВАНТОВЫЙ АЛГОРИТМ ИНКАПСУЛЯЦИИ КЛЮЧЕЙ CLASSIC MCELIECE

Введение

В 2016 г. Национальный институт стандартов и технологий США (англ. The National Institute of Standards and Technology, NIST) объявил конкурс, целью которого было выбрать алгоритмы постквантовой криптографии (англ. Post-Quantum Cryptography, PQC). Среди алгоритмов шифрования с открытым ключом и алгоритмов инкапсуляции ключей представлены в качестве финалистов третьего раунда: Classic McEliece [1], CRYSTALS-KYBER, NTRU, SABER. В качестве альтернативных финалистов в этой же группе алгоритмов были выбраны: BIKE [13], FrodoKEM, HQC [14], NTRU Prime, SIKE.

Эта версия алгоритма Classic McEliece была представлена на третьем раунде конкурса постквантовой криптографии 10 октября 2020 г. [7] международной группой разработчиков из Великобритании, США, Швейцарии, Нидерландов, Дании, Германии.

Алгоритм Classic McEliece является вариацией алгоритма на основе кодов, который был предложен Робертом Мак-Элисом (англ. Robert J. McEliece). Первая криптосистема с открытым ключом на основе кода была представлена в 1978 г. математиком и инженером в Калифорнийском технологическом институте Робертом Мак-Элисом [2]. В такой системе открытый ключ определяется случайным двоичным кодом Гоппы [3 – 6] (англ. Binary Goppa code). Шифртекст является кодовым словом, объединенным с некоторым вектором ошибок. Личный ключ обеспечивает эффективное декодирование: извлечение кодового слова из зашифрованного текста, выявление и удаление ошибок.

Система Мак-Элиса была разработана как односторонняя (англ. one-wayness against chosen-plaintext attacks, OW-CPA) [3 – 11], что означает, что злоумышленник не может эффективно найти кодовое слово из зашифрованного текста и открытого ключа, когда кодовое слово выбирается случайным образом. Уровень безопасности системы Мак-Элиса оставался на удивление стабильным, несмотря на десятки документов об атаках за 40 лет. Первоначальные параметры криптосистемы Мак-Элиса были разработаны только для $\left(2^{64}\right)$ безопасности, но система легко масштабируется до «избыточных» параметров, которые обеспечивают достаточный запас безопасности по сравнению с достижениями в компьютерных технологиях, включая квантовые компьютеры.

Система Мак-Элиса по времени существования сравнима с алгоритмом RSA [3 – 11]. Как известно, алгоритм RSA не имеет необходимой стойкости против постквантового криптоанализа, в то время как криптосистема Мак-Элиса должна обеспечивать такую стойкость.

Система Мак-Элиса потребовала огромного количества дополнительных доработок спустя годы. Некоторые из них повышают эффективность при сохранении безопасности: это включает в себя «двойное» шифрование с открытым ключом (англ. public-key encryption, PKE), предложенное Нидеррайтером (англ. Harald G. Niederreiter), ускорение программного обеспечения и аппаратных составляющих системы.

Кроме того, теперь известно [3 – 11], как эффективно преобразовать OW-CPA алгоритмы шифрования с открытым ключом в алгоритмы инкапсуляции ключей (англ. key encapsulation mechanisms, KEM), защищенные от атак типа IND-CCA2 на основе модели случайного оракула (англ. random oracle model, ROM). Это преобразование является жестким, сохраняя уровень безопасности, при двух допущениях, которым удовлетворяет криптосистема Мак-Элиса: во-первых, шифрование с открытым ключом является детерминированным (т.е. дешифрование восстанавливает всю использованную случайность); во-вторых, алгоритм не имеет ошибок дешифрования действительных зашифрованных текстов. Более того,

внесенные авторами модификации классического алгоритм обеспечивают аналогичную степень защиты для более широкого класса атак, а именно – атак на основе модели квантового случайного оракула (англ. quantum random oracle model, QROM). Риск того, что атака, специфичная для хэш-функции, может быть быстрее, чем атака ROM или QROM, устраняется стандартной практикой выбора хорошо изученной, "неструктурированной" хэш-функции с высоким уровнем безопасности.

Classic McEliece [1] – это вариация алгоритма Мак-Элиса, которая объединяет все лучшие наработки предыдущих лет воедино. Она представляет собой алгоритм инкапсуляции ключей с обеспечением безопасности против IND-CCA2 на очень высоком уровне, даже против квантовых вычислений. Алгоритм инкапсуляции ключей построен консервативно на основе шифрования на открытом ключе, что позволяет обеспечивать безопасности OW-CPA. А именно – основан на двойной версии алгоритма шифрования на открытом ключе Мак-Элиса, созданной Нидеррайтером, с использованием двоичных кодов Гоппы. Каждый уровень конструкции разработан так, чтобы системы, в которых был внедрен данный алгоритм с высокой вероятностью, обеспечивали долгосрочную безопасность в постквантовый период.

Другая работа включает вариации алгоритма Мак-Элиса, безопасность которых еще не была изучена достаточно тщательно. Например, во многих предложенных вариациях двоичные коды Гоппа заменяются другими семействами кодов, а криптография на основе решеток заменяет понятие «кодовое слово плюс случайные ошибки» на «точку решетки плюс случайные ошибки». Криптография на основе кодов и криптография на основе решеток являются двумя основными типами кандидатов, указанных в требованиях NIST [7, 8] относительно стандартизации постквантовых алгоритмов. В этом документе основное внимание уделяется точности классической системы Мак-Элиса, поскольку она была тщательно изучена.

1. Базовые определения

1.1. Криптография с открытым ключом

Криптосистема с открытым ключом [3 – 11] использует одностороннюю функцию с потайным входом E, которая будет служить функцией шифрования. Вычисление обратной E^{-1}, называемой функцией дешифрования, возможно, только если известен секрет K. Эта концепция односторонней функции формирует основу криптографии с открытым ключом, в которой секретным ключом является K, а открытым ключом – E. Точнее, криптосистема шифрования с открытым ключом должна обеспечивать три алгоритма: $KeyGen$, $Encrypt$ и $Decrypt$. $KeyGen$ – это вероятностный алгоритм с полиномиальным временем, который на входе получает $\{0,1\}^k$, где $k \geq 0$ – параметр безопасности, а на выходе формирует пару открытого / личного ключа (pk, sk). $KeyGen$ также определяет конечное пространство сообщений M_{pk}. $Encrypt$ – это вероятностный алгоритм с полиномиальным временем, который из входных параметров $\{0,1\}^k$, открытого ключа pk и сообщения $x \in M_{pk}$ формирует на выходе шифртекст c. $Decrypt$ – это детерминированный алгоритм с полиномиальным временем, который на основе входных данных $\{0,1\}^k$, sk и шифртекст c восстанавливает сообщение x. Криптосистема должна удовлетворять свойству правильности, что означает, что дешифрование должно однозначно восстанавливать зашифрованное сообщение.

1.2. Двоичный код Гоппы

Двоичный код Гоппы [3 – 11], обозначаемый $\Gamma(g(z), L)$, где $g(z)$ – порождающий полином Гоппы степени t над расширением поля $GF(2^m)$, где m – порядок расширения, а L – диапазон значений код, где $L \subseteq GF\{2^m\}$

$$g(z)=\sum_{i=0}^{t} g_i z^i = g_0 + g_1 z + ... + g_t z^t \quad (1)$$

$$L=\left\{\forall \alpha_i \in GF\left(2^m\right) \setminus g(\alpha_i)=0\right\} \quad (2)$$

с вектором c над $GF(2)$ таким, что $c=(c_1,c_2,...,c_n)$ и

$$R_e(z)=\sum_{i=1}^{t}\frac{c_i}{z-\alpha_i} \quad (3)$$

Если $n=2^m$ – длина кодового слова c, ограниченная диапазоном L, k – размерность, ограниченная $k>n-mt$, и минимальное расстояние $d\geq 2t+1$. Тогда $[n,k,d]$ представляет параметры кода Гоппы $\Gamma(g(z),L)$.

Для двоичного кода Гоппы любой сгенерированный многочлен $g(z)$ называется разделимым, если многочлен не имеет корней с кратностью больше единицы (то есть не имеет повторяющихся корней). Коды Гоппы, состоящие из таких полиномов, называются разделимыми двоичными кодами Гоппы. Для таких кодов существует хотя бы одно значение α_i при котором $g(\alpha_i)=0$.

Для двоичного кода Гоппы любой сгенерированный многочлен $g(z)$ называется неприводимым, если для $\forall \alpha_i$ справедливо $g(\alpha_i)\neq 0$. Коды Гоппы, состоящие из таких полиномов, называются неприводимыми двоичными кодами Гоппы.

Оба типа имеют возможность исправлять максимальное количество ошибок по сравнению с другими семействами кодов.

Минимальное расстояние d кода Гоппы должно быть больше $d\geq 2t+1$. Исправляющая способность кода оценивается параметром t.

Порождающая матрица G двоичного кода Гоппы используется для кодирования и декодирования сообщения, а контрольная сумма с проверкой на четность важна для обнаружения и исправления ошибок.

Порождающая матрица G получается из матрицы проверки на четность H, пространство строк G – это векторы нулевого пространства H по модулю 2, такие, что $GH^T=0$. Матрица проверки на четность H определяется как

$$H_{di}=\sum_{\alpha_i\in L}\sum_{k=1}^{t-(d-1)} g_{t-(k-1)}\alpha_i^{\,t-d+(1-k)}h_i \quad (4)$$

где $1\leq d\leq t$. Причем должно удовлетворяться условие $cH^T=0$, где c – шифротекст.

Кодирование сообщения в двоичном коде Гоппы [6]. Сообщение можно закодировать, разбив его на блоки длиной k бит и умножив каждый блок на порождающую матрицу G:

$$(m_1,m_2,...,m_k)\cdot G=(c_1,c_2,...,c_k) \quad (5)$$

Полученное сообщение (y) будет иметь вид

$$y=mG+e \quad (6)$$

***Алгоритм исправления ошибок неприводимого кода Гоппы* [6].**

1) Рассчитать синдром $S(z)$:

$$S(z)=\sum_{i=1}^{n}\frac{y_i}{z-\alpha_i} \quad (7)$$

2) Вычислить $\sigma(z)$, как показано ниже:

– Использовать расширенный алгоритм Евклида для определения $h(z)$, такого что

$$\sigma(z)h(z) \equiv 1 \pmod{g(z)} \tag{8}$$

Если $h(z) = z$, то процесс завершен и $\sigma(z) = z$, в противном случае продолжить:

– вычислить $d(z)$ так, чтобы

$$d^2(z) \equiv h(z) + z \pmod{g(z)} \tag{9}$$

– определить $a(z)$ и $b(z)$ такое, что

$$d(z)b(z) \equiv a(z) \pmod{g(z)} \tag{10}$$

– вычислить

$$\sigma(z) = a^2(z) + zb(z) \tag{11}$$

3) Рассчитать набор местоположений ошибки:

$$B = \{i \mid \sigma(\alpha_i) = 0\} \tag{12}$$

4) Вектор ошибок $e = (e_1, e_2, ..., e_n)$ определяется $e_i = 1$ для $i \in B$ и нулями в противном случае.

5) Сформированный шифротекст c имеет вид

$$c = y - e \tag{13}$$

Расшифровка сообщения [6]. Когда ошибки исправлены, сообщение может быть декодировано; закодированное сообщение в уравнении (6) можно представить в виде матрицы:

$$G^T \cdot \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_k \end{pmatrix} = \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix} \tag{14}$$

Для вычисления сообщения можно применить метод Гаусса, чтобы удалить порождающую матрицу $\lceil n/8 \rceil$:

$$\left(G^T \left| \begin{matrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{matrix} \right. \right) \square \ldots \square \cdot \left(\begin{array}{c|c} I_k & \begin{matrix} m_1 \\ \vdots \\ m_k \end{matrix} \\ \hline P & \end{array} \right) \tag{15}$$

где I_k _ это единичная матрица с размером $k \times k$, а p – это матрица с размером $(n-k) \times (k+1)$.

1.3. Свойство неразличимости шифротекста

К криптосистемам шифрования и инкапсуляции ключей с открытым ключом выдвигаются следующие требования [3 – 5, 8, 9]:

– семантическая безопасность (также известная как полиномиальная безопасность / неразличимость шифров): если злоумышленник имеет некоторую информацию об открытом тексте, он не может получить на основе этих знаний дополнительный данные о параметрах криптосистемы из шифротекста. Вычислительно невозможно различить два сообщения, одно из которых было зашифровано. Это означает, что схемы шифрования должны быть вероятностными;

– отсутствие гибкости. Из любого заданного зашифрованного текста злоумышленник не может получить новый зашифрованный текст таким образом, чтобы открытые тексты, лежащие в основе двух зашифрованных текстов, были значимо связаны. С другой стороны, злоумышленник может использовать множество видов атак: он может просто получить доступ к общедоступным данным, а затем зашифровать любой открытый текст по своему выбору (атаки на основе подобранного открытого текста) или, кроме того, использовать алгоритм дешифрования (атаки на основе неадаптивно / адаптивно подобранного шифротекста).

Криптосистема может быть семантически защищенной от атак с подобранным открытым текстом или даже атак с неадаптивным подобранным зашифрованным текстом (CCA1), при этом оставаясь гибкой. Однако защита от атак с адаптивно подобранным шифротекстом (CCA2) эквивалентна отсутствию гибкости.

Свойство неразличимости шифротекста определяет криптостойкость алгоритма к атаке на основе подобранного открытого текста. Обеспечение такого свойства неразличимости на основе открытого теста (IND-CPA) считается основным требованием для большинства доказуемо защищенных криптосистем с открытым ключом [3 – 5, 8, 9], хотя некоторые схемы также обеспечивают криптографическую стойкость против атак на основе подобранного шифротекста и адаптивных атак на основе подобранного шифротекста. Такие свойства неразличимости обозначаются, как IND-CCA1 и IND-CCA2 соответственно [3 – 5, 8, 9].

Для оценки уровня криптостойкости в классической и постквантовой криптографии для каждого алгоритма и его вариации используется обеспечиваемый уровень криптостойкости и соответствующие основные параметры преобразований. При описании требований к алгоритмам, подаваемым на конкурс, были определены три уровня криптографической стойкости [7, 8]:

– Уровень 1: любая атака, которая взламывает IND-CCA-стойкий алгоритм, должна требовать вычислительных ресурсов, сравнимых или превышающих требуемые для поиска ключа на блочном шифре с 128-битным ключом (например, AES-128);

– Уровень 3: если существует атака на IND-CCA-криптостойкий алгоритм, то для проведения такой атаки должны обеспечиваться вычислительные ресурсы, соизмеримые или превышающие требуемые для поиска ключа на блочном шифре с 192-битным ключом (например, AES-192);

– Уровень 5: любая атака, которая нарушает криптостойкость IND-CCA-стойкой схемы, должна требовать вычислительных ресурсов, сравнимых или превышающих требуемые для поиска ключа на блочном шифре с 256-битным ключом (AES-256).

1.4. Классическая и квантовая случайная модель оракула

За последние несколько лет, после многочисленных атак доказанная безопасность стала представлять наибольший интерес. Такое доказательство проводится в рамках теории сложности: предпринимаются попытки полиноминально свести хорошо установленную сложно решаемую проблему к атаке. Следовательно, эффективный злоумышленник не сможет решить сложную проблему: иначе это приведет к противоречию. Очень мало доказано схем с использованием только таких полиномиальных редукций без каких-либо других предположений. Кроме того, они с трудом достигают эффективности. В последние годы так называемая «случайная модель оракула» активизировала исследования, предоставив интересный инструмент для доказательства безопасности очень эффективных схем. Действительно, эта модель, в которой идеализированы некоторые конкретные криптографические объекты,

а именно хеш-функции, которые считаются действительно случайными, помогли обеспечить доказательства безопасности для многих схем шифрования и схем цифровой подписи.

Криптографическая хеш-функция – это функция $h:\{0,1\}^m \to \{0,1\}^n$ (где обычно $n<m$), которую трудно проанализировать. Интуитивно понятно, что желательно, чтобы единственный способ узнать информацию об $h(x)$ для любого конкретного $x \in \{0,1\}^n$ _ это фактически вычислить $h(x)$ и для каждого x, для которого h еще не вычислено, $h(x)$ должен выглядеть как новое случайное значение в $\{0,1\}^n$.

Модель случайного оракула – это способ формального моделирования этих интуитивных требований при анализе безопасности криптографических схем (таких как схемы шифрования или цифровой подписи), которые используют криптографическую хеш-функцию h как составную часть внутренней структуры. В модели случайного оракула хэш-функция h моделируется оракул, который необходимо запросить об $x \in \{0,1\}^m$, чтобы объект узнал хэш-значение $h(x)$, а случайный ответ оракула $h(x)$ относится к равномерно случайной функции $h:\{0,1\}^m \to \{0,1\}^n$.

Эта модель оказывается очень полезной для анализа безопасности криптографических схем. Например, это позволяет вести учет вычислительных возможностей злоумышленников, и поэтому возможно точно определить хеш-значения, которые доступны злоумышленнику. Тогда есть вероятность, что криптографическая схема, которая доказано безопасна в модели случайного оракула, будет доказуемо безопасна в принципе.

Оказывается, что модель случайного оракула необходимо пересмотреть в контексте квантовых атак, то есть когда рассматриваются злоумышленники, которые имеют в своем распоряжении неограниченные возможности проведения квантовых вычислений. Такая гипотетическая возможность позволила бы злоумышленнику вычислить суперпозиции хеш-функции h по нескольким x, то есть он мог бы создавать состояния, которые зависят от $\sum_x \alpha_x |x\rangle|h(x)\rangle$ для разных x, вычисляя h только один раз. Однако возможности злоумышленника относительно квантового криптоанализа ограничены рядом теорем о запрете (например, теоремой о запрете клонирования).

1.5. Криптосистема McEliece (1978)

Используя тот факт, что алгоритм быстрого декодирования существует для общего кода Гоппы, в то время как его не существует для общего линейного кода, в 1978 г. Робертом Мак-Элисом [2] было предложено создать криптосистему с открытым ключом, которая была бы достаточно безопасной, но в то же время обеспечивала чрезвычайно высокую скорость передачи данных. По мнению автора, такая криптосистема идеально подходит для использования в многопользовательских коммуникационных сетях, таких как те, которые предусмотрены НАСА для распространения данных, полученных из космоса, для передачи данных по незащищенным каналам передачи данных.

Криптосистема Мак-Элиса – это асимметричная криптосистема с открытым ключом, основанная на теории алгебраического кодирования. Криптосистема Мак-Элиса использует неприводимый двоичный код Гоппы, который до сих пор считался криптоустойчивым, особенно с параметром [1024, 524, 101], предложенным Мак-Элисом. Криптосистема с таким набором параметров страдает от большой матрицы открытых ключей, что затрудняет ее применение.

Криптосистема Мак-Элиса – одна из самых многообещающих криптосистем с открытым ключом, способная противостоять атакам на основе квантовых вычислений. Фактически, в отличие от криптосистем, использующих целочисленную факторизацию или дискретные логарифмы, криптостойкость данного алгоритма полагается на сложность декодирования полных линейных кодов (общая задача декодирования является NP-сложной).

После того, как Диффи и Хейлман ввели понятие криптосистемы с открытым ключом, в которой безопасность связи достигается без необходимости периодического распространения личного ключа отправителю и получателю. Это свойство делает такие системы идеально подходящими для использования в многопользовательских сетях связи.

Криптосистема Мак-Элиса состоит из трех основных алгоритмов:

– случайной генерации открытого и личного ключей;
– случайного шифрования открытого текста;
– детерминированного алгоритма расшифрования шифротекста.

Общесистемными параметрами для всех алгоритмов являются длина кода n, длина битовой последовательности открытого текста k, исправляющая способность кода t.

Каждому неприводимому многочлену степени t над $GF\left(2^m\right)$ соответствует двоичный неприводимый код Гоппы длины $n=2^m$, размерности $k \geq n-tm$ способный исправить любую комбинацию t ошибок или меньше. Более того, существует быстрый алгоритм декодирования этих кодов (алгоритм, предложенный Паттерсоном, время работы $\mathrm{O}(nt)$).

Предположим, что изначально в системе уже выбраны общесистемные параметры, а именно n и t, а также случайным образом выбран неприводимый полином степени t над $GF\left(2^m\right)$. Поскольку вероятность того, что случайно выбранный многочлен степени t является неприводимым, составляет около $1/t$, и поскольку существует быстрый алгоритм проверки неприводимости, предложенный Берлекампом, этот выбор будет легко сделать.

Генерация ключей

Входные параметры:

отсутствуют

Выходные параметры:

открытый ключ $\left(G', t\right)$,

личный ключ $\left(S, G, P\right)$

Алгоритм:

1) Сформировать $k \times n$ порождающую матрицу G для кода, которая может быть в канонической (например, приведённого ступенчатого вида), форме.
2) Сформировать случайную $k \times k$ невырожденную матрицу S.
3) Сформировать случайную $n \times n$ матрицу перестановок P.
4) Вычислить матрицу G' размером $k \times n$: $G' = SGP$, которая будет генерировать линейный код с той же скоростью и минимальным расстоянием, что и матрица G. Матрица G' будет общедоступной порождающей матрицей.
5) Сформировать наборы параметров в качестве открытого ключа $\left(G', t\right)$ и личного ключа $\left(S, G, P\right)$.

Схематически данный алгоритм представлен на рис. 1.

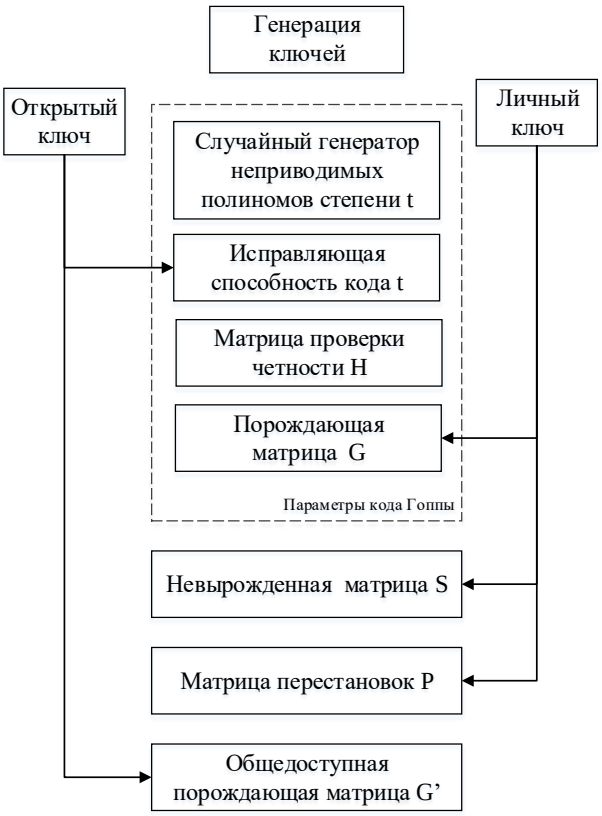


Рис. 1. Схема алгоритма случайной генерации открытого и личного ключей

Шифрование открытого текста

Входные параметры:

открытый текст m, общедоступная порождающая матрица G'.

Выходные параметры:

шифротекст c.

Алгоритм:

1) Представить открытый текст m в виде битовых последовательностей длины k.

2) Сформировать так называемый вектор ошибок – случайный вектор z длины n и веса t.

3) Вычислить шифротекст $c = mG' + z$.

Схематически данный алгоритм представлен на рис. 2.

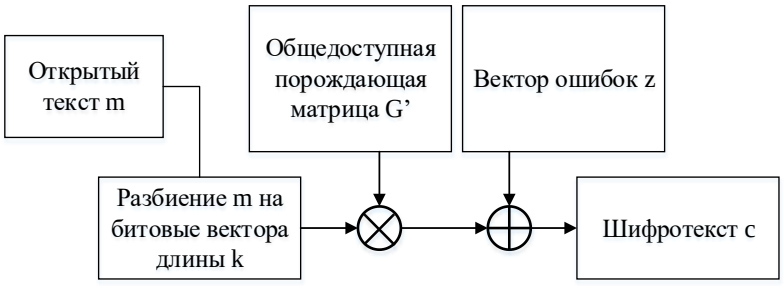


Рис. 2. Схема алгоритма шифрования открытого текста

Алгоритм расшифрования шифротекста

Входные параметры:

шифротекст c'.

Выходные параметры:

открытый текст m.

Алгоритм:

1) Вычислить обратную матрицу перестановок P^{-1}.
2) Вычислить $c' = cP^{-1}$.
3) Использовать алгоритм декодирования кодов Гоппы для восстановления m' из полученного c'.
4) Вычислить обратную матрицу S^{-1}, которая используется в алгоритме Паттерсона.
5) Вычислить открытый текст $m = m'S^{-1}$.

Схематически данный алгоритм представлен на Рис. 3.

Автором доказана корректность системы, т.е. правильность восстановления открытого текста после расшифрования $Decrypt\left(Encrypt\left(m\right)\right) = m$. Сформированный шифротекст имеет вид

$$c = mG' + z = mSGP + z \tag{16}$$

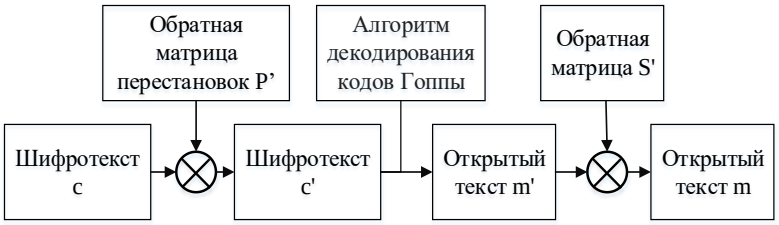


Рис. 3. Схема алгоритма расшифрования шифротекста

При расшифровывании формируется

$$c' = cP^{-1} = mSG + zP^{-1} \tag{17}$$

Как указывалось ранее, z имеет вес t, соответственно вес произведения zP^{-1} будет не более t.

Следовательно, при помощи кода Гоппы будет исправлено t ошибок. Расстояние Хемминга для составляющих шифротекста не превышает t, т.е. $d\left(mSG,\ cP^{-1}\right) \le t$, что доказывает соответствие исходного и расшифрованного текстов $m = m'S^{-1} = mSS^{-1}$.

2. Общая спецификация алгоритма Classic McEliece

2.1. Обозначения и параметры

Общесистемные параметры

n — Длина кода, $n \le q, n \in \mathbb{N}$

k — Размер кода, $k = n - mt$

t — Гарантируется возможность коррекции ошибок, $t \ge 2, mt < n$

q — Размер используемого конечного поля

m — $\log_2 q$, $m > 0, m \in \mathbb{N}$

μ — Неотрицательное целое число $\nu \ge \mu \ge 0,\ \nu \le k + \mu$

ν — Неотрицательное целое число

$f\left(z\right)$ — Неприводимый полином степени m, $f\left(z\right) \in F_2[z]$. Это определяет представление $F_2[z]/\ f\left(z\right)$ поля F_q

$F\left(y\right)$ — Неприводимый полином степени t, $F\left(y\right) \in F_q[y]$. Это определяет представление $F_q[y]/\ F\left(y\right)$ поля $F_{q^t} = F_{2^{mt}}$

Параметры симметричной криптографии

H — Криптографическая хеш-функция

l — Длина выхода криптографической хеш-функции, $l > 0$

σ_1 — Неотрицательное целое число, $\sigma_1 \geq m$

σ_2 — Неотрицательное целое число, $\sigma_2 \geq 2m$

G — Генератор псевдослучайных бит, который отображает строку из l бит в строку из $\left(n+\sigma_2 q+\sigma_1 t+l\right)$ бит

Параметры личного ключа

g — Многочлен в поле $F_q[x]$

α_i — Элемент конечного поля F_q

Γ — $\left(g,\alpha_1,...,\alpha_n\right)$

s — Битовая строка длины n

Параметры открытого ключа

T — Матрица из $\left(n-k\right)\times k$ элементов над полем F_2

Параметры шифротекста

e — Битовая строка длины n и веса Хэмминга t

C — Зашифрованный текст, содержащий сеансовый ключ

C_0 — Битовая строка длины $n-k$

C_1 — Битовая строка длины l

Элементы поля F_2^n, такие как кодовые слова и векторы ошибок, всегда рассматриваются как векторы-столбцы.

2.2. Выбор типа и размера параметров

Выбор параметров симметричной криптографии:

- l-битовая строка $H\left(x\right)$ определяется как первые l битов вывода $SHAKE256\left(x\right)$. Байтовые строки здесь рассматриваются как битовые строки с прямым порядком байтов.
- Длина битовой строки $l = 256$.
- Целое число σ_1 равно 16. (Во всех наборах параметров $m \leq 16$, поэтому $\sigma_1 \geq m$).
- Целое число σ_2 равно 32.
- $\left(n+\sigma_2 q+\sigma_1 t+l\right)$-битовая строка $G\left(\delta\right)$ определяется как первые $\left(n+\sigma_2 q+\sigma_1 t+l\right)$ вывода $SHAKE256\left(64,\delta\right)$. Здесь $64,\delta$ означает 33-байтовую строку, которая начинается с байта 64 и продолжается δ.

Все входы $H\left(x\right)$, используемые в криптосистеме Classic McEliece, начинаются с байта 0, 1 или 2 и, таким образом, не перекрывают входы $SHAKE256\left(x\right)$, используемые в G.

2.3. Представление параметров в виде байтовых строк

Векторы над полем F_2**.** Если r кратно 8, то r-битовый вектор $\upsilon = \left(\upsilon_0,\upsilon_1,...,\upsilon_{r-1}\right) \in F_2^r$ представляется в виде следующей последовательности из $r/8$ байтов:

$$\begin{pmatrix} \upsilon_0 + 2\upsilon_1 + 4\upsilon_2 + ... + 128\upsilon_7,\ \upsilon_8 + 2\upsilon_9 + 4\upsilon_{10} + ... \\ \qquad\qquad + 128\upsilon_{15},\ \upsilon_{r-8} + 2\upsilon_{r-7} + 4\upsilon_{r-6} + ... + 128\upsilon_{r-1} \end{pmatrix} \tag{18}$$

Если r не кратно 8, то r-битный вектор $\upsilon = \left(\upsilon_0,\upsilon_1,...,\upsilon_{r-1}\right) \in F_2^r$ дополняется 0 справа до длины между $r+1$ и $r+7$, в таком случае r станет кратно 8.

Сеансовые ключи. Сеансовый ключ K элемент поля F_2^l, представляется $\lceil l/8 \rceil$ байтовой строкой.

Шифротекст. Шифротекст C состоит из двух компонентов: $C_0 \in F_2^{n-k}$ и $C_1 \in F_2^l$. Шифротекст представлен как конкатенация $\lceil mt/8 \rceil$-байтовой строки, представляющей C_0 и $\lceil l/8 \rceil$-байтовой строки, представляющей C_1.

Хеш-входы. В алгоритме присутствуют три типа хеш-входов: $(2, \upsilon)$, $(1, \upsilon, C)$ и $(0, \upsilon, C)$. Здесь $\upsilon \in F_2^n$ и C представляет шифротекст.

Первые 0, 1 и 2 параметры представляются как байты. Вектор υ представляет собой следующие $\lceil n/8 \rceil$ байт. Если шифротекст присутствует, то он представляется как следующие $\lceil mt/8 \rceil + \lceil l/8 \rceil$ байт.

Открытые ключи. Открытый ключ T, который является матрицей $mt \times k$, представлен в виде строк. Каждая строка T представляется как $\lceil k/8 \rceil$-байтовая строка, и открытый ключ представлен как $mt\lceil k/8 \rceil$-байтовая конкатенация этих строк.

Элемент поля. Каждый элемент поля $F_q \cong F_2[z]/\, f(z)$ имеет форму $\sum_{i=0}^{m-1} c_i z^i$, где $c_i \in F_2$. Представление вектора поля это вектор $(c_0, c_1, ..., c_{m-1}) \in F_2^m$.

Неприводимые полиномы. Неприводимые полиномы $g = g_0 + g_1 x + ... + g_{t-1} x^{t-1} + x^t$ степени t представлены $t\lceil m/8 \rceil$ байтами, конкатенацией элементов поля $g_0, g_1, ..., g_{t-1}$.

Упорядоченное поле. Представление последовательности $(\alpha_1, ..., \alpha_q)$ из q различных элементов поля F_q будет последовательность q элементов поля.

Авторы описывают представление, которое упрощает быстрые алгоритмы декодирования с постоянным временем.

«Локальная сеть Бенеша» (англ. in-place Benes network) представляет собой серию из $2m-1$ этапов замены, применяемых к массиву из $q = 2^m$ объектов $(\alpha_0, \alpha_1, ..., \alpha_{q-1})$. Первый этап меняет местами α_0 и α_1, меняет местами α_2 и α_3 меняет местами α_4 и α_5 и т. д., как указано последовательностью из $q/2$ управляющих бит (1 означает замену мест, 0 означает отсутствие необходимости в замене). Второй этап меняет местами α_0 и α_2, меняет местами α_1 и α_3, меняет местами α_4 и α_6, и т.д., как указано следующими $q/2$ управляющими битами. Это продолжается до стадии m, на которой меняются α_0 и $\alpha_{q/2}$, меняются на α_1 и $\alpha_{q/2+1}$, и т.д. На $(m+1)$ этапе точно все происходит так же как и на $(m-1)$ этапе (с новыми управляющими битами), $(m+2)$-й этап аналогичен $(m-2)$-му этапу, и так далее вплоть до $(2m-1)$ этапа.

Определим π как перестановку $\{0,1,...,q-1\}$ такую, что $a_{i+1} = \sum_{j=0}^{m-1} \pi(i)_i \cdot z^{m-1-j}$ для всех $i \in \{0,1,...,q-1\}$. Порядок $(\alpha_1, ..., \alpha_q)$ представлен как последовательность из $(2m-1)2^{m-1}$ управляющих бит для локальной сети Бенеша для π. Этот вектор представлен в виде $\lceil (2m-1)2^{m-4} \rceil$ байт, как описано выше. Каждая перестановка имеет несколько вариантов управляющих битовых векторов. Чтобы упростить тестирование, требуется, чтобы переста-

новка π была преобразована конкретно в управляющие биты, определенные для π. Программные биты управления считыванием не проверяют уникальность.

В качестве простой защиты от ошибок при вычислении управляющих битов для π авторы рекомендуют разработчикам после вычисления проверять, что применение сети Бенеша дает π, и перезапускать генерацию ключа, если этот тест не прошел.

Выбор столбца. Часть личного ключа, сгенерированного функцией *KeyGen*, представляет собой последовательность $c=\left(c_{n-k-\mu+1},...,c_{n-k}\right)$ из μ целых чисел в порядке возрастания от $n-k-\mu+1$ до $n-k-\mu+\nu$. Эта последовательность c представлена как строка размером $\lceil \nu/8 \rceil$ байт, формат представления в порядке от младшего к старшему (обратном порядке байт):

$$\sum_{i=0}^{\mu-1} 2^{c_{n-k-\mu+1}-(n-k-\mu+1)} \tag{19}$$

Однако для $(\mu,\nu)=(0,0)$ последовательность c вместо этого представлена как 8 байтовая строка, которая является обратным порядком байтов $2^{32}-1$, т. е. 4 байта значения 255, за которыми следуют 4 байты значения 0.

Специальная обработка $(\mu,\nu)=(0,0)$ разработана таким образом, чтобы личный ключ, использующий $(\mu,\nu)=(0,0)$, был совместим с программным обеспечением декапсуляции, использующим $(\mu,\nu)=(32,64)$, когда все остальные параметры совпадают.

Личный ключ. Личный ключ (δ,c,g,α,s) представляет собой конкатенацию пяти частей:

- $\lceil l/8 \rceil$- байтовая строка $\delta \in F_2^l$.
- строка, представляющая выбор столбцов c. Эта строка имеет $\lceil \nu/8 \rceil$ байтов или 8 байтов, если $(\mu,\nu)=(0,0)$.
- $t\lceil m/8 \rceil$- байтовая строка полинома g.
- $\lceil (2m-1)2^{m-4} \rceil$ байт, представляющие поле порядка α.
- $\lceil n/8 \rceil$- байтовая строка $s \in F_2^n$.

3. Classic McEliece: алгоритм инкапсуляции ключей

3.1. Генерация неприводимого полинома

Входные параметры:

строка $d_{0,}d_{1,},...,d_{\sigma_1 t-1}$ из $\sigma_1 t$ бит.

Выходные параметры:

неприводимый полином $g \in F_q[x]$ степени t.

Алгоритм:

1) Определить $\beta_j=\sum_{i=0}^{m-1} d_{\sigma_1 j+iz^i}$ для каждого $j \in \{0,1,...,t-1\}$. В каждой группе σ_1 входных бит, используются только m первых бит. Алгоритм игнорирует оставшиеся биты строки.
2) Определить $\beta=\beta_0+\beta_1 y+...+\beta_{t-1}y^{t-1} \in F_q[y]/F(y)$.
3) Вычислить минимальный полином g из β над полем F_q. По определению g неприводимый полином, такой что $g(\beta)=0$.
4) Вернуть g если g имеет степень t. В противном случае вернуть ошибку выполнения.

3.2. Генерация упорядоченных полей

Входные параметры:

строка $\sigma_2 q$.

Выходные параметры:

последовательность $(\alpha_1, \alpha_2, ..., \alpha_q)$ из q различных элементов в поле F_q.

Алгоритм:

1) Берутся первые α_2 входных битов $b_0, b_1, ..., b_{\sigma_2 - 1}$ как σ_2-разрядное целое число $a_0 = b_0 + 2b_1 + ... + 2^{\sigma_2 - 1} b_{\sigma_2 - 1}$, затем берутся следующие σ_2 бит как σ_2-разрядное целое число a_1 и так далее до a_{q-1}.
2) Если $a_0, a_1, ..., a_{q-1}$ не различны, возвращается ошибка,
3) Сортируются пары (a_i, i) в лексикографическом порядке, чтобы получить пары $\left(a_{\pi(i),} \pi(i)\right)$, где π – перестановка $\{0,1,...,q-1\}$.
4) Определить $\alpha_{i+1} = \sum_{j=0}^{m-1} \pi(i)_j \cdot z^{m-1-j}$, где $\pi(i)$ определяет j наименее значащий бит в $\pi(i)$. Следует отметить, что конечное поле F_q построено как $F_2[z] / f(z)$.
5) Вернуть $(\alpha_1, \alpha_2, ..., \alpha_q)$.

3.3. Генерация ключей

Входные параметры:

не принимает никаких входных данных (помимо параметров).

Выходные параметры:

открытый ключ и личный ключ.

Алгоритм:

1) Генерируется строка δ с нормальным распределением длиной l бит, т.н. порождающее значение.
2) Вычисляется $E = F(\delta)$, строка длиной $(n + \sigma_2 q + \sigma_1 t + l)$ бит.
3) Определяется строка δ' как последние l бит от E.
4) Определяется s как первые n бит от E.
5) Вычисляется $\alpha_1, ..., \alpha_q$ из $\sigma_2 q$ последующих бит от E используя описанный выше алгоритм генерации упорядоченных полей. Если генерация завершается ошибкой, устанавливается $\delta \leftarrow \delta'$ и алгоритм выполняется заново.
6) Вычисляется g из следующих $\sigma_1 t$ от E используя описанный выше алгоритм генерации неприводимого полинома. Если генерация завершается ошибкой устанавливается $\delta \leftarrow \delta'$ и алгоритм выполняется заново.
7) Определяется $\Gamma = (g, \alpha_1, \alpha_2, ..., \alpha_n)$ (следует отметить, что $\alpha_{n+1}, ..., \alpha_q$ не используется здесь).
8) Вычисляется $(T, c_{n-k-\mu+1}, ..., c_{n-k}, \Gamma') \leftarrow MATGEN(\Gamma)$. Если генерация завершается ошибкой устанавливается $\delta \leftarrow \delta'$ и алгоритм выполняется заново.
9) Определяется Γ' как $(g, \alpha'_1, \alpha'_2, ..., \alpha'_n)$.
10) Формируется T как открытый ключ и как $(\delta, c, g, \alpha, s)$ личный ключ, где $c = (c_{n-k-\mu+1}, ..., c_{n-k})$ и $\alpha = (\alpha'_1, ..., \alpha'_n, \alpha_{n+1}, ..., \alpha_q)$.

3.4. Генерация вектора фиксированного веса

Входные параметры:

не принимает никаких входных данных.

Выходные параметры:

вектор $e \in F_2^n$ веса t. Алгоритм использует предварительно вычисленное целое число $\tau \geq t$.

Алгоритм:

1) Сгенерировать $\sigma_1 \tau$ случайных бит $b_0, b_1, ..., b_{\sigma_1 \tau - 1}$.

2) Определить $d_j = \sum_{i=0}^{m-1} b_{\sigma_1 j + i} 2^i$ для каждого $j \in \{0,1,...,\tau - 1\}$.

3) Определить $a_{0,} a_1, ..., a_{t-1}$ как первые t записей в $d_{0,} d_1, ..., d_{\tau - 1}$ в диапазоне $\{0,1,...,n-1\}$. Если получается определить менее чем t таких последовательностей, алгоритм выполняется заново.

4) Если $a_{0,} a_1, ..., a_{t-1}$ не все различны, алгоритм выполняется заново.

5) Определить $e = (e_{0,} e_1, ..., e_{n-1}) \in F_2^n$ как вектор веса t, такой, что $e_{a_i} = 1$ для каждого i.

6) Результатом является e.

Целое число τ определяется как t, если $n = q$; как $2t$, если $q/2 \leq n \leq q$; как $4t$, если $q/4 \leq n \leq q/2$; и т.д. Все выбранные параметры имеют $q/2 \leq n \leq q$, поэтому $\tau \in \{t, 2t\}$.

3.5. Инкапсуляция

Входные параметры:

открытый ключ T.

Выходные параметры:

шифротекст C и сеансовый ключ K.

Алгоритм:

1) Используя алгоритм генерации вектора фиксированного веса сгенерировать вектор $e \in F_2^n$ веса t.

2) Вычислить $C_0 = ENCODE(e, T)$.

3) Вычислить $C_1 = H(2, e)$.

4) Сформировать $C = (C_0, C_1)$.

5) Вычислить $K = H(1, e, C)$.

6) Сформировать шифротекст C и сеансовый ключ K.

3.6. Алгоритм кодирования

Входные параметры:

вектор-столбец $e \in F_2^n$ с весом t; и открытый ключ T, то есть матрица $(n-k) \times k$.

Выходные параметры:

вектор $C_0 \in F_2^{n-k}$.

Алгоритм:

1) Определить $H = (I_{n-k} \mid T)$.

2) Вычислить $C_0 = He \in F_2^{n-k}$.

3.7. Алгоритм декодирования

Входные параметры:

вектор $C_0 \in F_2^{n-k}$, набор параметров Γ'.

Выходные параметры:

вектор-столбец e, $C_0 = He$.

Существует два возможных исхода алгоритма:

– Если $C_0 = ENCODE(e,T)$, то $DECODE(C_0,\Gamma') = e$. Другими словами, если существует вектор $e \in F_2^n$ весом t, такой что выполняется $C_0 = He \in F_2^{n-k}$ с $H = (I_{n-k} \mid T)$, то алгоритм декодирования завершится успешно.

– Если C_0 не имеет формы He для любого вектора $e \in F_2^n$ весом t, то алгоритм декодирования завершится ошибкой.

Алгоритм:

1) Расширить C_0 до $\nu = (C_0, 0, ..., 0) \in F_2^n$ добавлением k нулей.
2) Найти уникальное кодовое слово c в коде Гоппы определенное Γ' с расстоянием $\le t$ от ν, если такого кодового слова нет, вернуть ошибку.
3) Установить $e = \nu + c$.
4) Если $wt(e) = t$ и $C_0 = He$ вернуть e, в обратном случае вернуть ошибку.

4. Параметры Classic McEliece

Существует пять предлагаемых наборов параметров в систематической форме: mceliece348864, mceliece460896, mceliece6960119, mceliece6688128 и mceliece8192128. Также авторами было предложено пять наборов параметров, использующих полусистематическую форму: mceliece348864f, mceliece460896f, mceliece6960119f, mceliece6688128f и mceliece8192128f.

В табл. 1 приведены общесистемные параметры вариаций криптосистемы Classic McEliece. В табл. 2 приведены фактические размеры входных и выходных параметров для вариаций алгоритма. Все данные приведены в байтах.

Таблица 1

Основные параметры криптосистемы Classic McEliece

Алгоритм	m	n	t	Полиномы
mceliece348864	12	3488	64	$f(z) = z^{12} + z^3 + 1,\ F(y) = y^{64} + y^3 + y + z$
mceliece348864f	12	3488	64	$f(z) = z^{12} + z^3 + 1,\ F(y) = y^{64} + y^3 + y + z,\ (\mu,\nu) = (32,64)$
mceliece460896	13	4608	96	$f(z) = z^{13} + z^4 + z^3 + 1,\ F(y) = y^{96} + y^{10} + y^9 + y^6 + 1$
mceliece460896f	13	4608	96	$f(z) = z^{13} + z^4 + z^3 + 1,\ F(y) = y^{96} + y^{10} + y^9 + y^6 + 1,\ (\mu,\nu) = (32,64)$
mceliece6688128	13	6688	128	$f(z) = z^{13} + z^4 + z^3 + z + 1,\ F(y) = y^{128} + y^7 + y^2 + y + 1$
mceliece6688128f	13	6688	128	$f(z) = z^{13} + z^4 + z^3 + z + 1,\ F(y) = y^{128} + y^7 + y^2 + y + 1,\ (\mu,\nu) = (32,64)$
mceliece6960119	13	6960	119	$f(z) = z^{13} + z^4 + z^3 + z + 1,\ F(y) = y^{119} + y^8 + 1$
mceliece6960119f	13	6960	119	$f(z) = z^{13} + z^4 + z^3 + z + 1,\ F(y) = y^{119} + y^8 + 1,\ (\mu,\nu) = (32,64)$
mceliece8192128	13	8192	128	$f(z) = z^{13} + z^4 + z^3 + 1,\ F(y) = y^{128} + y^7 + y^2 + y + 1$
mceliece8192128f	13	8192	128	$f(z) = z^{13} + z^4 + z^3 + 1,\ F(y) = y^{128} + y^7 + y^2 + y + 1,\ (\mu,\nu) = (32,64)$

Каждый из этих десяти наборов параметров имеет эталонную реализацию; реализацию с использованием 64-битной векторизации; реализацию с использованием 128-битных векторных инструкций Intel / AMD); и реализацию с использованием 256-битных векторных инструкций Intel / AMD). Эти четыре реализации являются интероперабельными и формируют идентичные тестовые векторы.

Таблица 2

Размеры входных и выходных параметров для криптографических функций криптосистемы Classic McEliece. Все размеры представлены в байтах

Алгоритм	Категория	Открытый ключ	Личный ключ	Шифртекст	Сессионный ключ
mceliece348864	1	261120	6492	128	32
mceliece348864f	1	261120	6492	128	32
mceliece460896	3	524160	13608	188	32
mceliece460896f	3	524160	13608	188	32
mceliece6688128	5	1044992	13932	240	32
mceliece6688128f	5	1044992	13932	240	32
mceliece6960119	5	1047319	13948	226	32
mceliece6960119f	5	1047319	13948	226	32
mceliece8192128	5	1357824	14120	240	32
mceliece8192128f	5	1357824	14120	240	32

Для наглядности на гистограмме (рис. 4) приведены размеры входных и выходных параметров. Так как значения параметров разнятся на несколько порядков, для наглядного представления на гистограммах данные длины личных и открытых ключей, а также длины соответствующих шифротекстов представлены в логарифмическом масштабе. Суть использования такого масштабирования заключается в преобразовании длин данных следующим образом: $x = \log_{10} X$, где X – параметр, такой как длина открытого или личного ключа, длина шифротекста, который подлежит масштабированию; x – результат вычисления десятичного логарифма над масштабируемым значением.

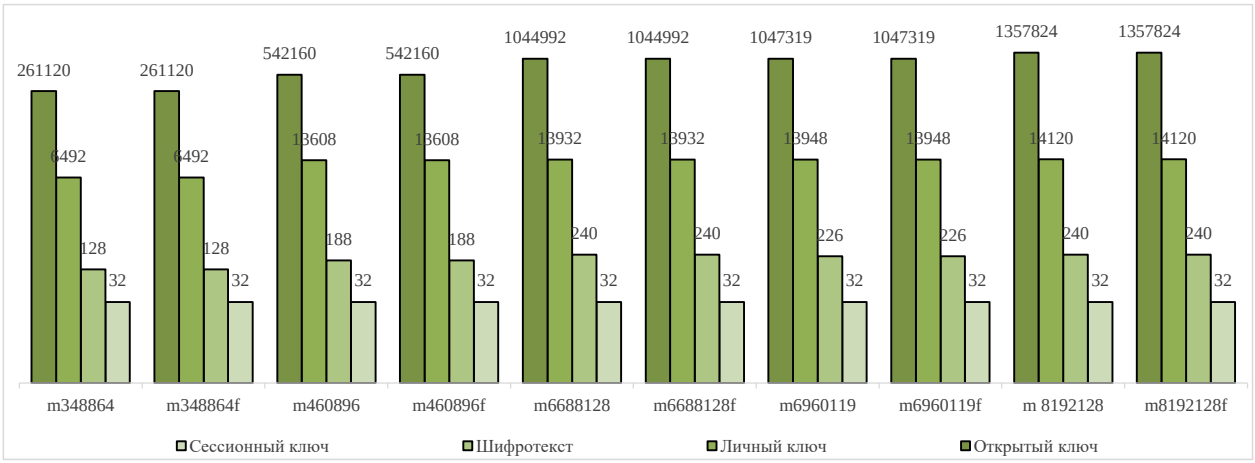


Рис. 4. Размеры входных и выходных параметров для криптографических функций криптосистемы Classic McEliece. Все размеры представлены в байтах

5. Анализ показателей быстродействия

Влияние выбора основных параметров на производительность. Размер зашифрованного текста составляет $n-k$ бит. Обычно соотношение $R = k/n$ выбирается около 0.8, поэтому размер зашифрованного текста составляет около $0.2n$ бит, то есть $n/40$ байтов, плюс 32 байта для подтверждения.

Размер открытого ключа составляет $k(n-k)$ бит. Для $R \approx 0.8$ это, примерно, $0.16n^2$ бит, то есть $n^2/50$ байтов. Для генерации открытого ключа используется $n^{3+o(1)}$ операций со стандартным методом Гаусса. Существуют асимптотически более быстрые

матричные алгоритмы. В операциях с личным ключом используется всего $n^{1+o(1)}$ операций со стандартными алгоритмами.

Сравнительный анализ показателей быстродействия. Данная оценка показателей быстродействия представлена в формате количества циклов процессора, затраченных на выполнение операции формирования ключей, инкапсуляции и деинкапсуляции ключей. Все измерения происходили без применения каких-либо технологий оптимизации производительности.

В частности, приводится оценка быстродействия, которая была проведена самими авторами при подаче алгоритма на всех трех раундах конкурса постквантовой криптографии. Программные измерения были выполнены с использованием пакета SUPERCOP на платформе Intel Xeon E3-1275 v3 (Haswell) с тактовой частотой 3,50 ГГц [1]. Объем оперативной памяти платформы 32 ГБ и работает под управлением Ubuntu 16.04. Для вариаций с полусистематической формой скорость выполнения операций инкапсуляции и деинкапсуляции не указана.

Приведенные оценки быстродействия сравнимы при условии игнорирования остальных (помимо приведенных показателей используемого центрального процессора) характеристик используемых вычислительных систем. Такая оценка носит исключительно первичный ознакомительный анализ возможностей производительности перечисленных выше алгоритмов. Как указывают сами авторы показатели производительности представленных ими оптимизированных реализаций алгоритма возможно еще улучшить.

В табл. 3 приведены показатели производительности для вариаций алгоритма инкапсуляции ключей Classic McElice, представленном на втором раунде конкурса. В табл. 4 приведены показатели производительности для Classic McElice, представленном на третьем раунде конкурса [1]. Данные приведены в циклах процессора, которые требуется выполнить для проведения каждой операции.

Как упоминалось ранее, каждая попытка генерации ключа (для систематических вариантов) успешна с вероятностью около 29 %, поэтому общее время генерации ключа варьируется. Однако окончательная успешная генерация ключей требует постоянного времени, и она использует отдельные случайные числа из неудачных попыток генерации ключей.

Для наглядности ниже на рис. 5 – 8 приведены гистограммы параметров быстродействия для всех вариаций алгоритма.

Таблица 3

Показатели производительности для вариаций алгоритма Classic McElice (раунд 2)

Название	Формирование ключей	Инкапсуляция	Деинкапсуляция
mceliece348864	208145574	46895	137503
mceliece348864f	82258215	-	-
mceliece460896	612458270	85410	274759
mceliece460896f	283980350	-	-
mceliece6688128	1344459257	156750	321536
mceliece6688128f	625501207	-	-
mceliece6960119	1202081992	156826	303207
mceliece6960119f	565430070	-	-
mceliece8192128	1277898472	185146	324803
mceliece8192128f	678901745	-	-

Таблица 4

Показатели производительности для вариаций алгоритма Classic McElice (раунд 3)

Название	Формирование ключевых данных	Инкапсуляция	Деинкапсуляция
mceliece348864	58034411	44350	134745
mceliece348864f	36641040	-	-
mceliece460896	215785433	117782	271694
mceliece460896f	117067765	-	-
mceliece6688128	556495649	151721	323957
mceliece6688128f	284584602	-	-
mceliece6960119	438217685	161224	301480
mceliece6960119f	246508730	-	-
mceliece8192128	514489441	178093	326531
mceliece8192128f	316202817	-	-

Чтобы адекватно продемонстрировать эти показатели, все данные на гистограммах приведены с использованием логарифмического масштаба, так как параметры разнятся на несколько порядков. Следует отметить, что меньшие значения циклов, затрачиваемых на выполнение одной операции, являются предпочтительными. В то же время, большие значения количества затрачиваемых циклов указывают на низкую скорость выполнения операции.

На рис. 5 приведена сводная гистограмма всех показателей быстродействия, показывающая общее соотношение скорости выполнения трех операций (формирование ключей, инкапсуляция и деинкапсуляция ключей) для каждого из вариаций алгоритмов, представленных на третьем раунде. Все данные указаны в затраченных на выполнение операции циклах.

Примерно сравнимую скорость выполнения операций инкапсулиции и деинкапсуляции имеют все вариации. Однако стоит отметить достаточно большой разрыв в производительности между формированием ключей и инкапсуляцией (деинкапсуляцией).

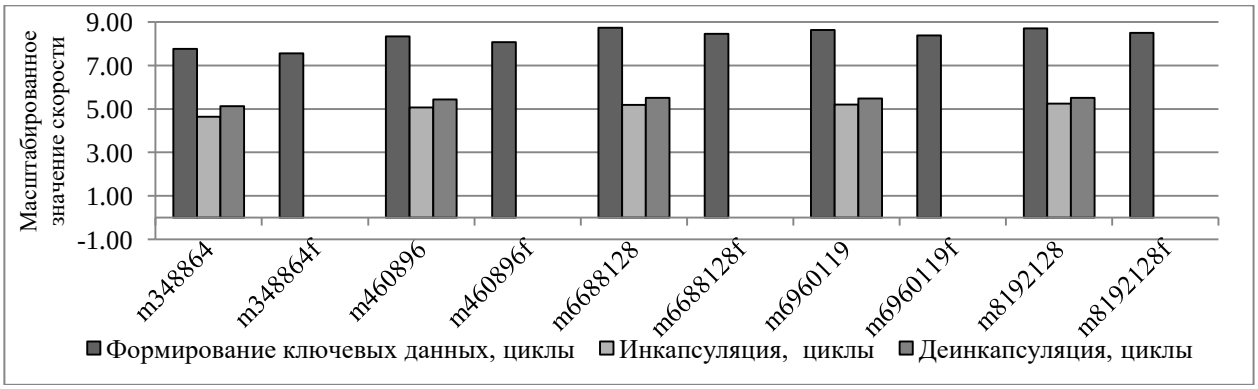


Рис. 5. Гистограмма показателей быстродействия (в логарифмическом масштабе)

Как указывалось, авторы для каждого из трех раундов представляли эталонные и оптимизированные версии алгоритма. Однако если прирост производительности в сравнении с первым раундом, по мнению авторов, был почти двойной. Прирост производительности же для реализации третьего раунда по сравнению со вторым менее значителен. Небольшого ускорения удалось добиться для операции формирования ключей, для остальных же операций скорость сравнима, а для вариации mceliece460896 из третьего раунда скорость инкапсуляции уменьшилась почти на треть. На рис. 6 и 7 приведена сводная гистограмма показателей быстродействия, показывающая общее соотношение скорости выполнения реализаций, представленных на втором и третьем раунде конкурса.

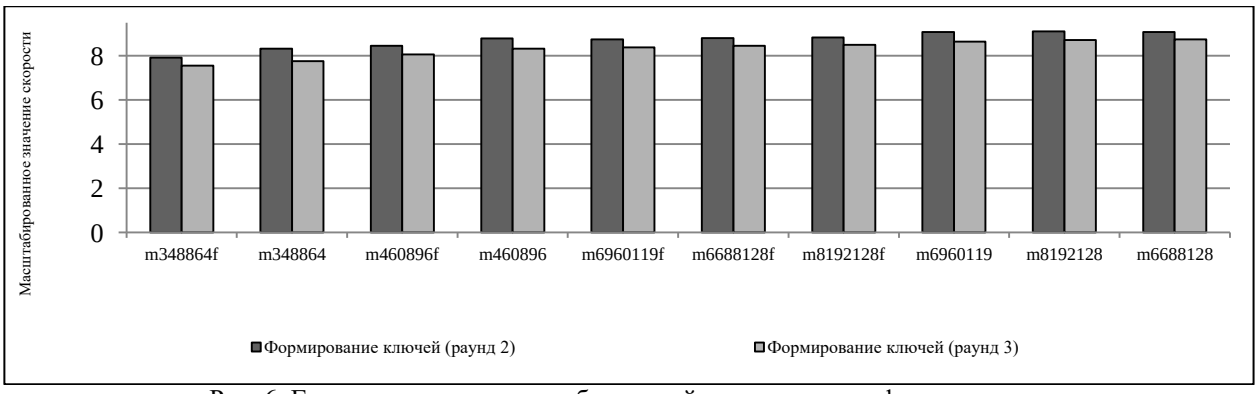


Рис. 6. Гистограмма показателя быстродействия: скорость формирования ключевых данных (раунд 2 и 3), в циклах (в логарифмическом масштабе)

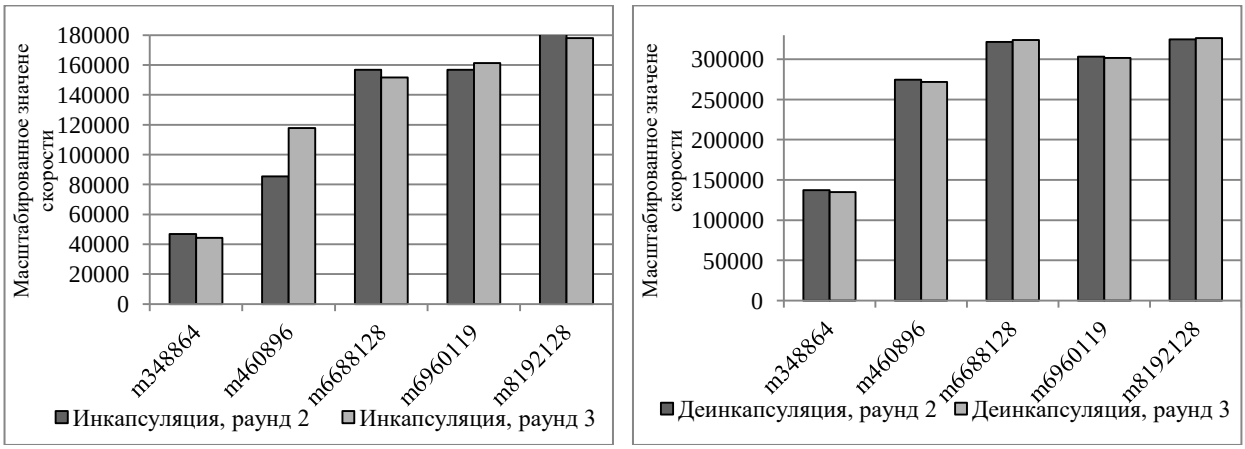


Рис. 7. Гистограмма показателей быстродействия: скорость инкапсуляции (раунд 2 и 3) и скорость деинкапсуляции (раунд 2 и 3), в циклах (в логарифмическом масштабе)

В рамках данного исследования проведен сравнительный анализ с алгоритмами BIKE и HQC. Для всех трех алгоритмов программные измерения были выполнены с использованием пакета SUPERCOP на платформе Intel Xeon E-2124 (CoffeeLake) с тактовой частотой 3,3 ГГц. На рис. 8 приведена гистограмма показателей быстродействия алгоритмов Classic McElice (раунд 3), BIKE и HQC.

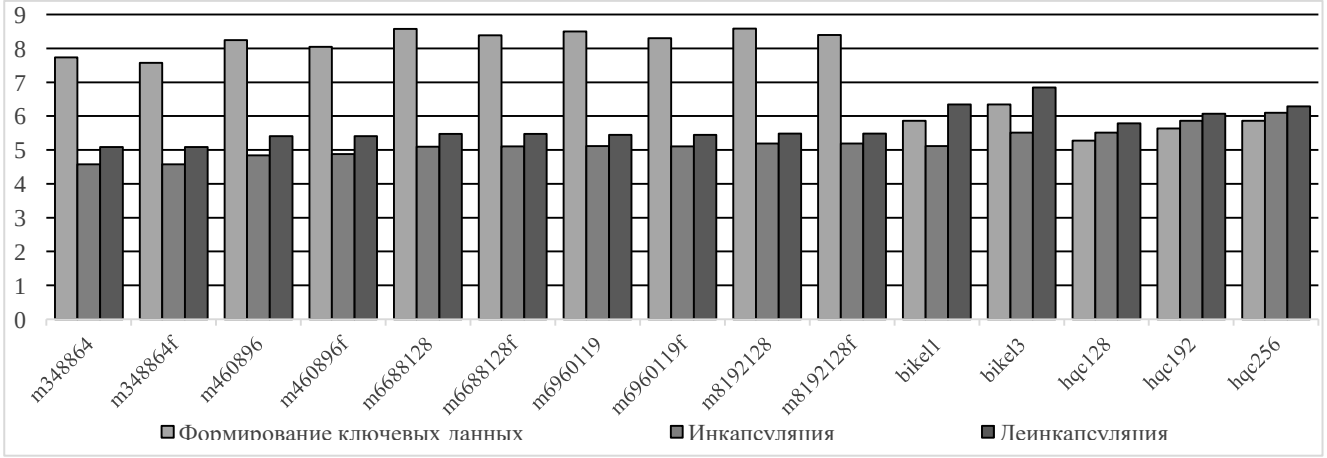


Рис. 8. Гистограмма показателей быстродействия алгоритмов Classic McElice, BIKE и HQC, в циклах (в логарифмическом масштабе)

Схема инкапсуляции ключей BIKE (BIt Flipping Key Encapsulation) представлена группой ученых из университетов стран Франции, США, Израиля, Германии [13]. Схема основана на квазициклических кодах с проверкой на четность (QC-MDPC) с умеренной плотно-

стью. Алгоритм обладает IND-CPA криптостойкостью. В третьем раунде авторами подана модификация алгоритма BIKE-2, представленного на предыдущих раундах. В основе алгоритма BIKE-2 лежит криптосистема Нидеррайтера с проверочной матрицей на четность. Алгоритм обеспечивает все три уровня безопасности.

Схема HQC (Hamming Quasi-Cyclic) подана на конкурс группой ученых из университетов стран Франции, США, Израиля, Германии [14]. Алгоритм обладает IND-CCA2 криптостойкостью. Основными особенностями HQC являются маленький размер открытого ключа и эффективные реализации на основе классических алгоритмов декодирования.

Стоит отметить, что, несмотря на медленную операцию формирования ключей для Classic McElice по сравнению с BIKE и HQC, скорость инкапсуляции и деинкапсулиции у рассматриваемого алгоритма меньше.

В требованиях указано, что алгоритм должен быть интероперабельным и масштабируемым. Поэтому в данном исследовании был проведен анализ производительности для довольно слабой вычислительной платформы. Измерения были выполнены с использованием пакета SUPERCOP на четырехядерной платформе Cortex-A9 с тактовой частотой 1,2 ГГц. Ожидаемо, скорость выполнения всех операций упала, для формирования ключей потребовалась на четверть больше операция процессора, остальным операциям требовалось на 1/5. Авторы отмечают, что совершенствование производительности для малоресурсных платформ является перспективным направлением исследований. На рис. 9 приведена гистограмма показателей быстродействия полученных при измерениях.

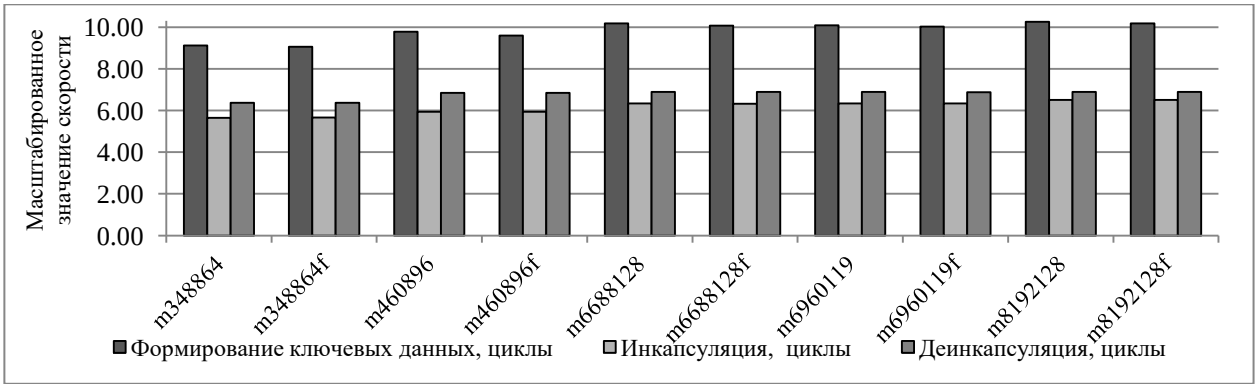


Рис. 9. Гистограмма показателей быстродействия алгоритма Classic McElice для вычислительной платформы Cortex-A9, в циклах (в логарифмическом масштабе)

6. Внесенные изменения

В алгоритм по мере продвижения конкурса постквантовой криптографии Classic McEliece вносились изменения. В частности, перед началом второго раунда конкурса NIST (30 марта 2019 г.) был существенно список наборов параметров m для поддержки необходимых уровней безопасности. Список параметров расширили следующим образом [1]:

- $(8192, 6528, 128)$, шифротексты длиной 240 байт: принимают как n, так и t как степени двойки; как и в первом раунде.
- $(6960, 5413, 119)$, шифротексты длиной 226 байт: оптимальная безопасность в пределах 2^{20} байт для открытого ключа; как и в первом раунде.
- $(6688, 5024, 128)$, шифротексты длиной 240 байт: оптимальная безопасность в пределах 2^{20} байт, если требуется, чтобы n и t были кратны 32.
- $(4608, 3360, 96)$, шифротексты длиной 188 байт: оптимальная безопасность в пределах 2^{19} байт, если требуется, чтобы n и t были кратны 32.

– $(3488,\ 2720,\ 64)$, шифротексты длиной 128 байт: оптимальная безопасность в пределах 2^{18} байтов, если требуется, чтобы n и t были кратны 32.

Поскольку Classic McEliece имеет такие маленькие зашифрованные тексты, можно было бы значительно сэкономить от изменения преобразования CCA, чтобы исключить подтверждение открытого текста (32 байта). Однако подтверждение в виде открытого текста имеет преимущества в плане безопасности: например, оно останавливает атаки с выбранным зашифрованным текстом на более раннем этапе, чем неявное отклонение, что упрощает защиту побочных каналов. Поэтому авторы решили сохранить существующее преобразование CCA.

Также возможно изменить параметры для дальнейшего уменьшения размеров зашифрованного текста на каждом уровне безопасности за счет использования более длинных ключей.

Был изменен формат случайного формирования пары ключей так, чтобы при необходимости можно было дополнительно сжимать ключи до 256 битной строки. Также был описан в качестве возможного будущего предложения альтернативный метод генерации ключей, который является более сложным (и требует больших сжатых личных ключей), но производительность которого значительно выше.

При подаче документации (от 10 октября 2020 г.) к третьему раунду наборы параметров для полусистематической формы алгоритма были задокументированы и реализованы в качестве возможных вариаций алгоритма.

Как и во 2-м раунде генерация ключа определяется с использованием различных случайных объектов, таких как случайный неприводимый многочлен g над F_q степени t. В 3-м раунде указывается явное отображение из случайной строки байтов в пары ключей с помощью явных отображений из случайных байтовых строк к случайным объектам, таким как g. Это оставляет открытой возможность указания дополнительных способов отображений в будущем с проверкой безопасности.

Отображение пар ключей начинается с 32 байтов случайности, что позволяет сжать личный ключ до 32-байтового порождающего значения. Порождающее значение расширяется с помощью $SHAKE256$ [12]. Выборка отклонения при генерации ключей обрабатывается путем детерминированного сопоставления каждого порождающего значения с новым порождающего значения. Личный ключ теперь имеет следующий формат: 256 бит (окончательного) порождающего значения, генерирующего ключ (а не ранее отклоненных порождающих значений); 64-битная строка веса 32, определяющая столбцы, используемые для полусистематической формы (или совместимая константа для систематической формы); многочлен g; управляющие биты для $(\alpha_1,...,\alpha_n)$; и n-битная строка s, используемая для неявного отклонения. Это оставляет открытой возможность указания других форматов личных ключей в будущем, таких как сжатые форматы (порядок объектов в этом формате разработан, чтобы обеспечить сжатие посредством простого усечения с эффективной декомпрессией) или список $(\alpha_1,...,\alpha_n)$ вместо управляющих битов для сред, где перестановка через RAM не является проблемой. Любой другой формат личного ключа с эффективными алгоритмами преобразования в этот формат личного ключа и обратно будет иметь такую же математическую безопасность.

Выводы

Проведен анализ финалиста конкурса постквантовой криптографии NIST PQC алгоритма инкапсуляции ключей Classic McEliece. Рассмотрены математические модели алгоритма Мак-Элиса и его современной вариации Classic McEliece. Рассмотрены характеристики входных и выходных параметров, а также основные показатели криптографической стойкости и быстродействия. Оценка быстродействия формировалась на основе эталонных реали-

заций на нескольких вычислительных платформах. Также проведен анализ изменений, внесенных на протяжении трех раундов конкурса. На основе этого проведен сравнительный анализ показателей быстродействия для вариаций алгоритма, представленных на трех раундах.

В ходе исследований установлено, что схема удовлетворяет формальным требованиям к кандидатам на постквантовые схемы инкапсуляции ключей, т.е. имеет различные варианты алгоритма, которые обеспечивают все три уровня крипто стойкости (1-й, 3-й и 5-й). Алгоритму свойственны длинные открытые ключи вследствие того, что вероятность успешного исполнения отдельных функций формирования ключа достаточно низка, формирование ключей – наиболее медленная и ресурсоемкая операция. Несмотря на это, операции инкапсуляции и деинкапсуляции по сравнению с остальными конкурсантами более производительны.

Перспективным направлением исследования является улучшение свойств масштабируемости без потери показателей производительности и криптографической стойкости.

Список литературы:

1. Classic McEliece: conservative code-based cryptography [Электронный ресурс]. Режим доступа: https://classic.mceliece.org/nist/mceliece-20201010.pdf
2. McEliece R.J. A public-key cryptosystem based on algebraic coding theory // Prog. Rep., Jet Prop. Lab., California Inst. Technol, 1978. P. 114 – 116.
3. Горбенко І.Д. Прикладна криптологія. Теорія. Практика. Застосування: монографія / І.Д. Горбенко, Ю.І. Горбенко. Харків : Форт, 2012. 870 с.
4. Есин В.І. Безпека інформаційних систем і технологій / В.І. Есин, О.О. Кузнецов, Л.С. Сорока. Харків : ХНУ ім. В.Н. Каразіна, 2013. 632 с.
5. Горбенко І. Д. Постквантова криптографія та механізми її реалізації / І. Д. Горбенко, О. О. Кузнєцов, О. В. Потій, Ю. І. Горбенко, Р. С. Ганзя, В. А. Пономар // Радіотехніка. 2016. Вип. 186. С. 32-52.
6. Гоппа В. Д.. Введение в алгебраическую теорию информации. Москва : Наука, Физматлит, 1995. 112 с.
7. Post-Quantum Cryptography [Электронный ресурс]. Режим доступа: https://csrc.nist.gov/Projects/post-quantum-cryptography/round-3-submissions
8. Report on Post-Quantum Cryptography [Электронный ресурс]. https://csrc.nist.gov/publications/detail/nistir/8105/final
9. Daniel J. Bernstein Johannes Buchmann Erik Dahmen. Post-Quantum Cryptography. [Электронный ресурс]. Режим доступа: https://www.researchgate.net/profile/Nicolas_Sendrier/publication/226115302_Code -Based_ Cryptography/links/540d62d50cf2df04e7549388/Code-Based-Cryptography.pdf.
10. Menezes J., van Oorschot P. C., Vanstone S. A. Handbook of Applied Cryptography. Boca Raton, Florida. CRC Press. 1997. 816 p.
11. Katz, Jonathan; Lindell, Yehuda. Introduction to Modern Cryptography: Principles and Protocols // Chapman and Hall/CRC, 2007. 552 pages.
12. FIPS PUB 180-4, Secure Hash Standard (SHS) [Электронный ресурс]. Режим доступа: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf
13. BIKE: Bit Flipping Key Encapsulation [Электронный ресурс]. Режим доступа: https://bikesuite.org/files/v4.1/BIKE_Spec.2020.10.22.1.pdf
14. Hamming Quasi-Cyclic (HQC) [Электронный ресурс]. Режим доступа: http://pqc-hqc.org/doc/hqc-specification_2020-10-01.pdf
15. SUPERCOP [Электронный ресурс]. Режим доступа: https://bench.cr.yp.to/supercop.html

Поступила в редколлегию 00.00.2020

Сведения об авторах:

Луценко Мария Сергеевна – аспирант кафедры безопасности информационных систем и технологий, Харьковский национальный университет имени В. Н. Каразина, Украина; e-mail: lutsenko.maria.kh@gmail.com, ORCID: https://orcid.org/0000-0003-2075-5796

УДК 003.026:004.056 **DOI:10.30837/rt.2020.4.203.07**

Д.В. ГАРМАШ, Г.А. МАЛЄЄВА, С.О. КАНДІЙ

ПРОЕКТ СТАНДАРТУ ЕЛЕКТРОННОГО ПІДПИСУ RAINBOW ТА ЙОГО ОСНОВНІ ВЛАСТИВОСТІ І МОЖЛИВОСТІ ЩОДО ЗАСТОСУВАННЯ

Вступ

За результатами другого етапу міжнародного конкурсу щодо проведення досліджень та розробки стандартів асиметричних криптографічних перетворень постквантового періоду позитивну оцінку та визнання фіналістом отримав механізм електронного підпису (ЕП) Rainbow [1]. Його важливими перевагами, у порівнянні з іншими постквантовими ЕП, це менша складність прямого та зворотного перетворень – вироблення та перевірки підпису, а також суттєво зменшена довжина підпису. Разом з тим довжина відкритого ключа у нього достатньо велика. Тому є думка, що Rainbow не підходить, як алгоритм ЕП загального призначення для заміни алгоритмів, які наразі визначені у FIPS 186-4. Зокрема, великі відкриті ключі роблять ланцюги сертифікатів надзвичайно великими. Однак є додатки, яким не потрібно надто часто надсилати ключі, тому цей недолік у цих випадках може бути несуттєвим. За цих умов механізм ЕП Rainbow може знайти застосування, в тому числі збільшуючи різноманітність постквантових ЕП. Також, суттєво проблемним є обмеження рівнів безпеки ЕП Rainbow 256 біт проти класичного та 128 біт проти квантового криптоаналізу.

Предметом статті є аналіз та узагальнення конструкцій механізму Oil-Vinegar систем автентифікації з відкритим ключем на основі застосування ЕП Rainbow. Це важливий напрямок щодо створення безпечних та ефективних систем автентифікації для практичних застосувань з використанням відкритих ключів, наприклад недорогих смарт-карт, коли потрібна швидкодія при виробленні та перевірці ЕП. Особливістю такого механізму автентифікації є реалізація ідеї багаторівневої системи Oil-Vinegar [2]. Вважається, що система автентифікації на основі ЕП повинна бути більш безпечною у змісті криптографічної стійкості та більш ефективною у змісті широкого застосування у малопотужних тощо додатках. Важливість вирішення цієї проблемної задачі полягає у потенційному застосуванні механізму Rainbow, як надійно безпечної та дуже ефективної системи автентифікації з відкритим ключем на основі ЕП.

Загальні положення щодо схеми ЕП RAINBOW

Криптосистеми, що засновані на квадратичних поліномах, пройшли за останні 10 років суттєвий розвиток та визнання. Теоретичною основою конструкцій Oil-Vinegar є доведена теорема, згідно з якою вирішення (визначення) набору багатоваріантних поліноміальних рівнянь над кінцевим полем є експоненційно складною проблемою, хоча це є у загальному випадку як необхідною так і достатньою умовами [2].

Цей напрямок досліджень пов'язаний з появою конструкції Мацумото та Імаї [MI88], в тому числі використовуючи рівняння лінеаризації [1]. Далі Патарін та його співробітники доклали великих зусиль для розробки безпечних багатоваріантних криптосистем. Один з конкретних напрямків, яким займались Патарін та його співробітники, пов'язаний з рівняннями лінеаризації Dragon, Oil and Vinegar, Unbalanced Oil-Vinegar [1]. Побудова механізму ЕП Rainbow на основі Oil and Vinegar, Unbalanced Oil-Vinegar грунтується на тому, що певні квадратичні рівняння можна легко розв’язати, якщо є можливість вгадувати декілька варіантів [1].

Нехай k буде кінцевим полем. Ключовою конструкцією є відображення (карта) F від k^{o+v} до k^{o}:

$$F(x_1,...,x_0,x_1^{'},...,x_v^{'}) = F(x_1,...,x_0,x_1^{'},...,x_v^{'}),...,F_0(x_1,...,x_0,x_1^{'},...,x_v^{'}) \quad (1)$$

і кожна F_l у формі:

$$F(x_1,...,x_0,x_1^{'},...,x_v^{'}) = \sum a_{l,i,j}x_i x_j + \sum b_{l,i,j}x_i^{'}x_j^{'} + \sum c_{l,i}x_i + \sum d_{l,i}x_j^{'} + c_l \quad , \tag{2}$$

де x_i, $i = 1,...,o$ це Oil значення та $x_j^{'}$, $j = 1,...,v$ значення Vinegar у кінцевому полі k.

Потрібно звернути увагу на схожість наведеної вище формули з рівняннями лінеаризації. Такий тип поліномів називається „поліномом Oil-Vinegar“. Причина, по якій вона називається схема "Oil-Vinegar", пов'язана з тим, що в квадратичному вимірі змінні Oil та Vinegar не змішуються повністю. Це дозволяє легко знайти одне рішення для будь-якого рівняння виду

$$F(x_1,...,x_0,x_1^{'},...,x_v^{'}) = (y_1,...,y_o), \tag{3}$$

коли $(y_1,...,y_o)$ дано. Щоб знайти одне рішення, потрібно лише випадковим чином вибрати значення для Vinegar змінних та підключити їх до рівнянь вище, що дасть набір o лінійних рівнянь з o змінними. Це має, з імовірністю, близькою до 1, дати рішення. Якщо цього не сталося, можна спробувати ще раз, вибравши різні значення для Vinegar змінних, поки не вдасться знайти рішення [4].

Це сімейство криптосистем розроблено спеціально для схем підписів, де потрібно лише знайти одне рішення для даного набору рівнянь, а не унікальне рішення. Застосовуючи відображення (карту F), ми «приховуємо» її, складаючи її з лівої та правої сторін за двома оборотними афінними лінійними відображеннями L_1 та L_2. Оскільки L_1 знаходиться на k^o, а L_2 на k^{o+v}, це генерує квадратичне відображення (карту)

$$F^{-} = L_1 \circ F \circ L_2 \tag{4}$$

від k^{o+v} до k^o.

Сбалансована схема Oil-Vinegar характеризується тим, що $o = v$, але її удосконалили Кіпніс та Шамір [KS99], використовуючи матриці, що відносяться до білінійних форм, визначених квадратичними поліномами [3].

Для незбалансованої схеми Oil-Vinegar, $v > o$, показано, що конкретна атака має складність приблизно $q^{v-o-1}o^4$, коли $v \approx o$. Це означає, що якщо o не надто велике (меньше ніж 100) і дане фіксоване поле розміром q, тоді $v - o$ має бути досить великим, але також не надто великим, щоб забезпечити безпеку схеми.

Однак слід зауважити, що в цій схемі документ, що підписується, є вектором у k^o, а підпис – вектором у k^{o+v}. Це означає, що підпис має принаймні вдвічі більший розмір документа, і при великому $v + o$ система стає менш ефективною.

В рамках статті пропонується конструкція, яка використовує конструкцію Oil-Vinegar кілька разів, так що в підсумку підпис буде лише трохи довшим за документ. Отже, ця схема набагато ефективніша. Її називають схемою Rainbow.

Сутність та властивості схеми підпису RAINBOW

Загальна конструкція Rainbow.

Нехай S – множина $\{1, 2, 3, ..., n\}$. Нехай $v_1,...,v_u$ – цілі числа, такі що попадають в умову $0 < v_1 < v_2 < \cdots < v_u = n$ і визначимо декілька наборів цілих чисел $S_l = \{1, 2, ..., v_l\}$ для $l = 1,...,u$, так що ми маємо $S1 \subset S2 \subset \cdots \subset Su = S$

Нехай O_i є такою множиною, що $O_i = S_{i+1} - S_i$, $fori = 1,...,u-1$.

Нехай P_l – лінійний простір квадратних многочленів, що задаються поліномами

$$\sum_{i \in O_{l,j} \in S_l} \alpha_{i,j}x_i x_j + \sum_{i \in O_{l,j} \in S_l} \beta_{i,j}x_i x_j + \sum_{i \in O_{l,j} \in S_l} \gamma_i x_i + \eta \tag{5}$$

Видно, що це багаточлени типу Oil-Vinegar, такі що x_i, $i \in O_l$ – змінні Oil наряду з x_i, $i \in S_l$ – змінні Vinegar. x_i, $i \in O_l$ називаються l-м рівнем Oil змінної, а x_i, $i \in S_l$ являються l-м рівнем Vinegar змінної.

Будь-який поліном у P_l називається l-м рівнем поліном Oil та Vinegar. З цього маємо, що

$$P_i \subset P_j \text{ для } i < j.$$

Таким чином, кожен $P_l, l = 1,...,u-1$ є набором багаточленів Oil та Vinegar. Кожен поліном у P_l має x_i, $i \in O_l$ як змінні Oil і x_i, $i \in S_l$ як змінні Vinegar. Поліноми Oil та Vinegar у P_i можна визначити як поліноми так, що $x_i \in O_l$ – змінні Oil, а x_i, $i \in S_l$ – Vinegar змінні. Це можна проілюструвати тим, що $S_i + 1 = \{S_i, O_i\}$.

Тепер ми визначимо відображення (карту) F схеми підпису Rainbow. Це карта F від k^n до k^{n-v1} така, що

$$F(x_1,...,x_n) = (\tilde{F}_1(x_1,...,x_n),...,\tilde{F}_{u-1}(x_1,...,x_n)) = (F_1(x_1,...,x_n),...,F_{n-v_1}(x_1,...,x_n)), \quad (6)$$

кожен $\tilde{F}_i$ складається з o_i випадково обраних квадратичних многочленів з P_i. Під випадково обраним поліномом маємо на увазі, що ми вибираємо його коефіцієнти випадковим чином [4].

Таким чином, можна зазначити, що F насправді має $u-1$ рівні Oil-Vinegar конструкцій. Перший рівень складається з поліномів o_1 $F_1,...,F_{o1}$, таких що x_j, $j \in O_1$ – змінні Oil, а x_j, $j \in S_1$ – змінні Vinegar. I-й рівень складається з поліномів o_i, $F_{vi}+1,...,F_{vi+1}$, так що x_j, $j \in O_i$ – змінні Oil, а x_j, $j \in S_i$ – змінні Vinegar. З цього ми можемо побудувати «веселку» з наших змінних:

$$[x_1,...,x_{v1}];\{x_{v1}+1,...,x_{v2}\}\ [x_1,...,x_{v1},x_{v1}+1,...,x_{v2}];\{x_{v2}+1,...,x_{v3}\}$$
$$[x_1,...,x_{v1},x_{v1}+1,...,x_{v2},x_{v2}+1,...,x_{v3}];\{x_{v3}+1,...,x_{v4}\}\ [x_1,...,...,x_{vu-}1];\{x_{vu-}1+1,...,x_n\} \quad (7)$$

Кожен рядок вгорі представляє рівень Rainbow. Для l-го рівня, наведеного вище, є змінні Vinegar, у { } – змінні Oil, а змінні Vinegar кожного рівня складаються з усіх змінних попереднього рівня.

F можна назвати поліноміальною картою Rainbow з рівнями $u-1$.

Нехай L_1 і L_2 є двома випадковими обраними аффінними лінійними картами, L_1 знаходиться на $kn-v1$ і L_2 на kn.

$\bar{F}(x_1,...,x_n) = L_1 \circ F \circ L_2(x_1,...,x_n)$ який складається з $n-v_1$ квадратних многочленів з n змінними.

Тепер можна використати вищезазначене для побудови схеми підпису Rainbow із відкритим ключем.

Публічний ключ – для схеми підпису Rainbow відкритий ключ складається з $n-v_1$ поліноміальних компонентів F та структури поля k. Приватний ключ складається з карт L_1, L_2 та F.

Підписати документ, який є елементом $Y' = (y_1',...,y_{n-v_1}')k^{n-v_1}$ потрібно знайти рішення рівняння

$$L_1 \circ F \circ L_2(x_1,...,x_n) = F(x_1,...,x_n) = Y^l \quad (8)$$

Для цього спочатку можна застосувати обернену до L_1, а потім виявляється

$$F \circ L_2(x_1,...,x_n) = L_1^{-1}Y^l = Y^l \tag{9}$$

Далі потрібно інвертувати F . У цьому випадку потрібно вирішити рівняння

$$F(x_1,...,x_n) = Y^l = (y_1^{-l},...,y_{n-v_1}^{-l}) \tag{10}$$

Спочатку необхідно випадково вибрати значення $x_1,...,x_{v1}$ і підключити їх до першого рівня o_1, заданих

$$F_1 = (y_1,...,y_{o_1}^{-l}) \tag{11}$$

Це дає набір лінійних рівнянь o_1 зі змінними o_1, $x_{o1}+1,...,x_{v2}$, які вирішуються, щоб знайти значення $x_{o1}+1,...,x_{v2}$. Тоді отримуються всі значення x_i, $i \in S_2$ [1]. Потім ми підключаємо ці значення до другого рівня багаточленів, який знову дасть o_2 число лінійних рівнянь, яке потім дасть значення всіх x_i, $i \in S_3$ Процедура повторюється, поки не буде знайдено рішення. Якщо в будь-який час набір лінійних рівнянь не має рішення, все починається з початку, вибравши інший набір значень для $x_1,...,x_{v1}$. Це буде продовжуватись, поки не буде знайдено рішення. З [Pat96] відомо, що з дуже великою ймовірністю можна розраховувати на успіх, якщо кількість рівнів не надто велика.

Потім ми застосовуємо обернену до L_2, яка дає нам підпис Y, який позначається

$$X^l = (x_n^l,...,x_n^l). \tag{12}$$

Щоб перевірити підпис, потрібно лише перевірити, чи справді

$$F(X^l) = Y^l. \tag{13}$$

Для того щоб підписати великий документ, можна пройти ту саму процедуру для Flash, що і в [PCG01], застосувавши спочатку хеш-функцію, а потім підписати хеш-значення документа.[4]

Практична реалізація схеми Rainbow.

Для практичної реалізації ми вибрали k кінцевим полем розміром $q = 2^8$.

Нехай $n = 33$ і S – множина $\{1,2,3, ..., 33\}$.

Нехай $u = 5$ і $v_1 = 6$, $v_2 = 12$, $v_3 = 17$, $v_4 = 22$, $v_5 = 33$.

Маємо $o_1 = 6$, $o_2 = 5$, $o_3 = 5$, $o_4 = 11$

У цьому випадку і F^{-}, і F є картами від k^{33} до k^{27}.

Відкритий ключ складається з 27 квадратних многочленів із 33 змінними. Загальна кількість коефіцієнтів для відкритого ключа становить $27 \times 34 \times 35/2 = 16\,065$, або близько 15 КБ пам'яті.

Приватний ключ складається з 11 багаточленів з 22 змінами Vinegar та 11 змінних Oil, 5 поліномів з 17 змінами Vinegar та 5 Oil, 5 поліномів з 12 змінними Vinegar та 5 Oil, та 6 поліномів з 6 змінними Vinegar та 6 Oil плюс дві афінні лінійні перетворення L_1 і L_2. Загальний розмір – близько 10 КБ.[5]

Ця схема підпису підписує документ розміром $8 \times 27 = 216$ біт із підписом $8 \times 33 = 264$ біт.

Криптоаналіз схеми підпису RAINBOW

Представляється короткий криптоаналіз схеми підпису Rainbow, розглянувши його для наведеного вище прикладу. Є кілька способів атак, з якими будуть мати справу користувачі алгоритму. Для тих методів, де використовуються квадратні форми, слід пам'ятати, що

теорія квадратних форм над скінченними полями відрізняється, коли характеристика дорівнює 2, у порівнянні з випадком, коли характеристика є непарною [D09] [6].

Метод зниження рангу

Метод зниження рангу використовується для розбиття схеми підпису біраціональної перестановки Шаміра. Причина, по якій ця атака може спрацювати, полягає в тому, що простір, що охоплюється поліноміальними компонентами шифру схеми Шаміра, складається з прапора пробілів:

$$V1 \subset V2 \subset \cdots \subset Vt,$$

де V_t – простір, охоплений поліноміальними компонентами шифру, кожна V_i є власною підмножиною V_{t+1}, а ранг відповідної білінійної форми, що відповідає елементам у $V_{t+1} - V_i$ занадто більший, ніж у V_i, а різниця розмірів між V_i та V_{t+1} рівно 1. Завдяки цим властивостям, зокрема останньому, це дозволяє легко знайти цей прапор просторів, а саме всі V_i, спочатку знайшовши V_{n-1}, потім V_{n-2} і так далі шляхом зменшення рангу [8]. Але цей метод атаки вже не може працювати проти цієї схеми. Причиною цього є те, що, в нашому випадку, існує також такий прапор просторів, що кількість компонентів – це точно кількість рівнів, розмірність кожного компонента прапора точно відповідає розміру V_{i+1}, $i = 1,...,u-1$, але різниця в розмірах останніх двох великих просторів – це точно $O_u - 1$, яка була обрана спеціально для досить великого числа 11, на відміну від випадку Шаміра, коли воно дорівнює 1.

Властивість, наведена вище, якраз і є причиною того, що атака більше не може працювати. Тут не можна використовувати метод зниження рангу через те, що $O_u - 1 = 11$і більше не 1. „Останній товстий рівень Oil" дозволяє схемі протистояти атаці зниження рангу [7].

Метод атаки на Oil-Vinegar схеми.

Аналіз показав, шо, дія L_1 полягає у змішуванні всіх поліноміальних компонентів F. Отже, кожен компонент шифру *F* тепер належить до верхнього рівня поліномів Oil-Vinegar, а саме всі вони є елементами P_4. Це багаточлени Oil-Vinegar з 22 змінними Vinegar та 11 змінними Oil [1]. Для цього випадку можна застосувати метод для незбалансованої схеми підпису Oil-Vinegar, щоб спробувати атакувати систему, що дозволить відокремити змінні верхнього шару Oil-Vinegar. Для цього нам потрібно розділити верхній (або кінцевий) рівень з 11 змінних Oil та 22 змінних Vinegar. Відповідно до криптоаналізу, складність атаки цього першого кроку становить $q^{22-11-1} \times 11^4 > 2^{90}$.

Метод MinRank

Існує два абсолютно різних способи використання методу MinRank. Перший – пошук полінома, асоційована матриця якого має найнижчий ранг серед усіх можливих варіантів. Цей набір поліномів із 6 змінними Vinegar та 6 Oil належить до першого рівня, тобто $P1$, і позначався $\tilde{F}_1$. Для цього спочатку ми прив'язуємо до кожного полінома білінійну форму, яка має матрицю розміром 33×33. Потім ми можемо використовувати лінійні комбінації матриць, пов'язаних із компонентами F, для виведення полінома, пов'язана з яким матриця має ранг 12 [3]. В цьому випадку, щоб атакувати систему, проблемою стає пошук матриці рангу 12 серед групи з 27 матриць розміром 33×33. З методу MinRank ми знаємо, що складність пошуку такої матриці становить $q^{12} \times 27^3$, що набагато більше, ніж 2100.

Інша можливість це пошук поліномів, що відповідають поліномам у другому останньому рівні, а саме той, який належить P_3 і походить від лінійних комбінацій $\tilde{F}_i$, $i < 4$. У цьому випадку метод MinRank однозначно не може бути використаний , оскільки вони взагалі мають ранг 22. Одним із шляхів, безсумнівно, є випадковий пошук. Оскільки розмірність P_3 дорівнює 16, це стає проблемою пошуку елемента в підпросторі розмірності 16 в загальному

просторі розмірності 27. Отже, такий випадковий пошук потребує щонайменше q^{11} пошуків, щоб знайти його, але нам також потрібно визначити, чи дійсно рейтинг нижче 22 для кожного пошуку. У цьому випадку загальна складність повинна бути не менше $q^{11} \times (22 \times 33^2 / 3) > 2^{100}$. Ця ідея атаки насправді пов'язана з іншим методом атаки, і наведений вище аргумент пояснює, чому цей метод більше не може працювати [8].

З останніх результатів електронного друку в цьому напрямку, де вивчаються дуже загальна система, яка називається STS, ми знаємо, що їх метод може бути застосований і до нашого випадку. Відповідно до їх оцінки, безпека нашої системи становить принаймні $27 \times 33^3 \times (2^8)^{12} \times 5 > 2^{100}$.

Атака за допомогою структури багатошаровості

Для випадку криптосистеми Мацумото-Імай Патарін зрозумів, що якщо шифр складається з декількох незалежних паралельних «гілок», можна виконати поділ змінних таким чином, що всі поліноми в шифрі виведені як лінійні комбінації поліномів над кожною групою змінних. Ця властивість насправді може бути використана для атаки на систему. На перший погляд, можна подумати, що рівні виглядають як різні «гілки». Тим не менше, слід усвідомити, що рівні жодним чином не є «незалежними», оскільки кожен з них будується на попередньому. Тобто, можна сказати, що всі рівні злипаються, і ми ніяк не можемо зробити будь-якого розділення змінних. Це зрозуміло при розгляданні поліномів останнього рівня P_4. Тому атака з використанням властивості паралельних незалежних гілок у [Pat95] тут не може працювати. Подібним чином можна стверджувати, що атака з використанням системних систем також не може працювати тут, оскільки немає гілок і все насправді «склеєно» [2].

Загальні методи

Іншими методами, які можуть бути використані для атаки на нашу схему підписів, є такі, які безпосередньо вирішують поліноміальні рівняння, наприклад метод XL та різні його узагальнення, або такі, що використовують основи Гробнера. Безумовно, дуже складно вирішити набір з 27 рівнянь із 33 змінними, оскільки для цього набору рівнянь існує надто багато рішень. Загалом, набагато краще розв'язувати рівняння лише з однією змінною. Через характер проектування системи можна здогадатися про значення для будь-якого набору змінних $v_1 = 6$, і ми маємо ймовірність $1 / e < 1 / 2.71828 < 0.37$ отримати унікальне рішення. Тепер задача стає проблемою вирішення набору з 27 квадратних рівнянь із 33 змінними. Ми повинні думати про це так, ніби це сукупність випадково вибраних квадратних рівнянь. Відповідно до того, що прийнято вважати, для вирішення цього набору рівнянь складність становить щонайменше $23 \times 27 > 281$.

З цього ми робимо висновок, що загальна складність атаки на наш приклад становить принаймні 280 [3].

Загальний аналіз безпеки

На основі цього можна побачити, що для атаки на систему можна підійти до неї або з верхнього рівню, або сформувати нижній рівень. Безпека нижнього рівню залежить від того, наскільки ефективно можна використовувати метод Minrank. Загалом складність атаки дорівнює $q^{(v2-1)} o^3{}_u - 1 if v_1 > o_1$, якщо $v_1 > o_1$, або $q^{2v1} o_u{}^3 - 1$, якщо $v_1 \le o_1$. З цього можна отримати, що не можна дозволити $v_2 = o_1 + v_1$ бути занадто малим. З останніх результатів електронного друку [WBP], безпека системи становить принаймні $(n - v_1) \times n^3 \times (q)^{o1+v1} \times u$, що, безсумнівно, вимагає, щоб $o_1 + v_1$ не був малим.

Що стосується випадку атаки зверху, метод атаки для незбалансованого методу Oil-Vinegar говорить, що $v_u - 1 - o_u - 1$ не може бути занадто малим. Також щоб уникнути випадкових атак пошуку $o_u - 1$ не повинно бути занадто малим [4].

Порівняння з іншими схемами багатоваріантних підписів

Порівняння з незбалансованою Oil-Vinegar

По-перше, система, що розглядається, є узагальненням оригінальної конструкції Oil-Vinegar, і оригінальну схему можна трактувати як просто однорівневу схему Rainbow, де $u = 2$. Припустимо, що ми хочемо створити незбалансовану схему Oil-Vinegar, яка має однакову довжину для документа, який може бути підписаний, як наш практичний приклад вище. У цьому випадку ми знову вибираємо k як кінцеве поле розміром $q = 28$, і ми знаємо, що кількість змінних Oil має бути 27. Через атаку на дисбаланс схем Oil-Vinegar [KPG99], ми знаємо, що число змін Vinegar має бути не менше $27 + 11 = 38$, щоб мати однаковий рівень безпеки [1]. Далі, відкритий ключ складається з 27 поліномів із $38 + 27 = 65$ змінними. Отже, розмір відкритого ключа становить $27 \times (67 \times 66/2)$ байт, що становить приблизно 116 КБ, що приблизно в 10 разів перевищує наш практичний приклад. Це означає, що публічне обчислення перевірки підпису триватиме щонайменше в 10 разів довше.

Приватний ключ для незбалансованої схеми Oil-Vinegar складається з одного афінного лінійного перетворення на k^{27} та іншого на k^{65} та набору з 27 поліномів Oil та Vinegar з 27 змінними Oil та 38 змінними Vinegar. Це означає, що закритий ключ становить близько 40 КБ. Також, що приватний розрахунок для підписання документа займе приблизно у чотири рази довше порівняно з нашим прикладом. Довжина підпису становить $65 \times 8 = 520$ біт, що також приблизно вдвічі перевищує розмір підпису нашого прикладу [2]. З цього ми робимо висновок, що наша схема має бути набагато кращим вибором загалом як з точки зору безпеки, так і ефективності.

Порівняння з Sflash

NESSIE, «Нові європейські схеми підписів, цілісності та шифрування» – це проект в рамках Програми Європейської комісії з технологій інформаційного суспільства. Він зробив остаточний вибір крипто алгоритму після більш ніж 2-річного процесу. Sflashv2, швидку багатоваріантну схему підпису було обрано консорціумом Nessie і рекомендовано для недорогих смарт-карт. Однак, з погляду безпеки, дизайнер Sflash одного разу рекомендував не використовувати Slashv2, натомість рекомендується нова версія Sflashv3. Це просте розширення Sflashv2 за рахунок збільшення довжини підпису. Sflashv3 має довжину підпису 469 біт і відкритий ключ 112 Кбайт. Але нещодавно Sflashv2 знову визнали безпечним, і ми порівняли нашу реалізацію із Sflashv2. Sflashv2 має підпис довжиною $37 \times 7 = 259$ для документа $26 \times 7 = 182$ біт. Наш приклад має підпис довжиною $33 \times 8 = 264$ для документа розміром $27 \times 8 = 216$ біт. З точки зору ефективності на біти ці два фактично однакові [3].

Для порівняння часу роботи було застосовано Sflashv2, як описано в [ACDG03]. Генерація підпису приблизно вдвічі швидша для нашого прикладу з Rainbow у порівнянні з Sflash. Час перевірки підпису, звичайно, майже однаковий. З цього можна зробити висновок, що схема має бути хорошим вибором як з точки зору безпеки, так і ефективності.

Також можна порівняти цю систему з новими схемами TTS, але ці схеми атаковані, як це було показано в презентації в IWAP'04 [DY04]. Слід також побачити, що Tractable Rational Map Signature, як представлено в [WHLCY], дуже схожий на TTS і може розглядатися як дуже особливий приклад нашої схеми [5].

Побудова системних параметрів для RAINBOW для 384 біт безпеки

Аналіз показав, що для схеми Rainbow актуальною є задача побудови системних параметрів для рівня безпеки 384 біт. В цьому розділі наводяться результати попередніх досліджень щодо вирішення вказаної задачі.

До загальносистемних параметрів Rainbow належать поле $GF(q)$, над яким задані поліноми, кількість «oil» змінних o_1, o_2 (в Rainbow використовується 2 рівня), кількість «vinegar» змінних v_1.

Загальна кількість рівнянь є $n = o_1 + o_2 + v_1$

Загальна кількість змінних є $m = o_1 + o_2$

Всі ефективні атаки на Rainbow полягають в використанні лінеаризації рівнянь.

До основних атак належать:

1) Прямі алгебраїчні атаки. Полягають у безпосередньому застосуванні алгоритмів вирішення квадратичних рівнянь над полями Галуа. Автори Rainbow зазначають, що алгоритм XL (та його модифікації) дає найкращі результати. Час роботи алгоритму залежить від константи d_{reg} – степені регуляризації системи.

2) MinRank атаки. Атаки цього класу полягають у пошуку лінійної комбінації мінімального рангу поліномів. Аналіз, що приведений в специфікації Rainbow є спрощеним. Повну методику обчислення параметрів автори виклали у [1].

3) HighRank атаки. Полягають у пошуку «oil» змінних в останньому рівні. Оцінити складність атаки можливо за формулою

$$C_{HighRank} = q^{o_2} * \frac{n^3}{6}. \tag{14}$$

При застосуванні алгоритму Гровера можливо пришвидшити пошук:

$$C_{HighRank(quantum)} = q^{o_2/2} * \frac{n^3}{6}. \tag{15}$$

4) UOV атаки. Оскільки Rainbow є узагальненням OUV, то атаки на цю схему можливо також узагальнити. Оцінити складність атаки можливо за формулою

$$C_{HighRank} = q^{n-2o_2-1} * o_2^4. \tag{16}$$

При застосуванні алгоритму Гровера можливо пришвидшити пошук:

$$C_{HighRank} = q^{\frac{n-2o_2-1}{2}} * o_2^4. \tag{17}$$

5) Rainbow-Band-Separation атаки. Полягає у пошуку маскуючих афінних перетворень *S* і *T*.

Загальні зауваження щодо атак:

1) Атаки HighRank і атаки на UOV сильно залежать від поля.

2) Атаки Rainbow-Band-Separation і прямі атаки сильно залежать від кількості невідомих змінних m, кількості рівнянь n і кількості «oil» змінних на останньому рівні o_2.

3) Від кількості «oil» змінних на першому рівні o_1 безпека залежить значено менше, ніж від кількості «oil» змінних на останньому рівні o_2.

Параметри для 384 біт наведені в таблиці:

Рівень	Параметри	прямі	MR	HR	UOV	RBS
384	$(o_1 = 108, o_2 = 96, v_1 = 134, GF(256))$	?	533	406	602	?

Також наведемо проблемні (невирішені) питання.

Прямі атаки та RBS атаки потребують детальнішого вивчення для оцінки.

Автори Rainbow використовують поле $GF(2^x)$. Чи є доцільним використовувати поле іншої форми?

Висновки

1. Постквантова криптографія – частина криптографії, яка залишається актуальною і при появі квантових комп'ютерів і квантових атак. Так як по швидкості обчислення тради-

ційних криптографічних алгоритмів квантові комп'ютери значно перевершують класичні комп'ютерні архітектури, сучасні криптографічні системи стають потенційно вразливими до криптографічних атак. Більшість традиційних криптосистем спирається на проблеми факторизації цілих чисел або завдання дискретного логарифмування, які будуть легко розв'язуватись на досить великих квантових комп'ютерах, що використовують алгоритм Шора.

2. Багато криптографів ведуть розробку алгоритмів, незалежних від квантових обчислень, тобто стійких до квантовим атакам. Ці задачі розглянуті на 2-му етапі конкурсу NIST США.

3. У зв’язку з можливістю появи потужного квантового комп’ютера актуальними є завдання створення постквантових алгоритмів ЕП. В цьому напрямі вже розпочаті дослідження, в певній мірі визначено математичні основи, на яких можуть бути побудовані постквантові алгоритми ЕП. Для цього можна застосувати схему Rainbow.

4. Реалізація квантовозахищених алгоритмів вимагає великих матеріально-технічних ресурсів. Вказане пов’язане з великими довжинами ключів і та загальних параметрів. Сучасний рівень розвитку техніки дозволяє оптимістично ставитися до можливості ефективної реалізації квантовозахищених алгоритмів.

5. Мультиваріативні квадратичні перетворення можуть бути застосованими для розроблення постквантового стандарту ЕП. Вони вже були використані для побудови схем підпису, але всі спроби побудувати надійну схему досі не увінчалися успіхом. Попередній аналіз показав, що мультиваріативні квадратичні перетворення можуть вирішити проблему захищеності від атак на основі квантових комп’ютерів, але для цього ще потрібно провести величезний обсяг досліджень та робіт, а також вкласти значні ресурси.

6. Попередній аналіз показує, що розміри загальних параметрів та ключів не викликають сумнівів відносно криптографічної стійкості стандарту, розробленого на основі мультиваріативного квадратичного перетворення. Але залишається проблема просторової складності, яка пов’язана зі значними довжинами загальних параметрів та відкритих ключів.

Список літератури:

1. Lili Chen, Stephen Jordan, Yi-Kai-Liu, Dustin Moody, Rene Peralta, Ray Perlner, Daniel Smith-Tone. Report on Post – Quatum Cryptography. Nistir 8105 (draft). https://www.google.com.ua/search?

2. Інтернет-ресурс. Режим доступу http://www.nkj.ru/archive/articles/5309/

3. Інтернет-ресурс. Режим доступу http://www.win.tue.nl/diamant/symposium05/abstracts/wolf.pdf

4. Горбенко І.Д. Аналіз проблем криптографічного захисту інформації у постквантовий період та можливі шляхи їх вирішення / І.Д. Горбенко, О.О. Кузнєцов, Р.В. Олійников, О.В. Потій, Ю.І. Горбенко, Р.С. Ганзя, В.І. Пономар // Матеріали V-ї міжнар. наук.-техн. конф. «Захист інформації і безпеки інформаційних систем». Львів, 2016 (02.06 – 03.06). С. 52.

5. Reinier Broker. Constructing supersingular elliptic curves // J. Comb. Number Theory. (3): pp. 269–273, 2009.

6. McGrew D., Curcio M. Hash-Based Signatures draft-mcgrew-hash-sigs-00 [Электронный ресурс]. Режим доступа: https://tools.ietf.org/html/draft-mcgrew-hash-sigs-00

7. Daniel J. Bernstein, Chitchanok Chuengsatiansup, Tanja Lange, and Christine van Vredendaal. NTRU Prime

8. D. J. Bernstein. Grover vs. McEliece // N. Sendrier, editor, Post-Quantum Cryptography, Third International Workshop, PQCrypto 2010, Darmstadt, Germany, May 25-28, 2010. Proceedings, volume 6061 of Lecture Notes in Computer Science, pages 73–80. Springer, 2010.

Надійшла до редколегії 06.09.2020

Відомості про авторів:

Гармаш Дмитро Васильович – аспірант кафедри кібербезпеки, Харківський національний університет імені В.Н. Каразіна; Україна, e-mail: donni.dima@gmail.com

Малєєва Ганна Андріївна – аспірант кафедри безпеки інформаційних технологій, Харківський національний університет радіоелектроніки, Україна; e-mail: hanna.malieieva@nure.ua

Кандій Сергій Олегович – технік-конструктор, АТ "ІІТ", Україна; e-mail: sergeykandy@gmail.com

МЕТОДИ ТА МЕХАНІЗМИ ЗАХИСТУ ІНФОРМАЦІЇ

УДК 004.056.52 **DOI:10.30837/rt.2020.4.203.08**

Р.Ю. ГВОЗДЬОВ, Р.В. ОЛІЙНИКОВ, д-р техн. наук

МЕТОД І МЕТОДИКА ФОРМАЛЬНОГО ПРОЕКТУВАННЯ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

Вступ

Нормативними документами (далі – НД) в сфері технічного захисту інформації (далі – ТЗІ) визначено сім ієрархічних критеріїв гарантій від Г-1 до Г-7 включно, які визначають ступінь впевненості в тому, що кожна з функціональних вимог безпеки здатна протистояти певним загрозам. НД ТЗІ 2.5-004.99 висуває вимоги до процесу проектування КСЗІ, де стиль формалізованої (частково формалізованої) специфікації є обов'язковим для отримання рівня гарантій Г-4 та вище.

На даний момент не існує методик для формального проектування КСЗІ в інформаційно-телекомунікаційних системах (далі – ІТС).

Метою статті є аналіз існуючих мов формального опису системи, які в перспективі можуть використовуватися для проектування КСЗІ в ІТС та створення наукового підґрунтя для подальших досліджень в цій сфері.

Поняття формального проектування

Під терміном формалізованої специфікації слід розуміти таке представлення, яке базується на чітко визначених математичних концепціях. В свою чергу, математичні концепції визначають синтаксис і семантику подання, що дозволяє унеможливити неоднозначність розуміння моделі.

Процес проектування (або послідовність розробки) включає в себе модель політики безпеки та проект архітектури комплексу засобів захисту (далі – КЗЗ).

Методика формального проектування повинна включати:

- формалізоване моделювання політики безпеки;
- формалізований опис ІТС та процесів обробки інформації;
- алгоритм формування комплексу засобів захисту у ІТС з формальної моделі політики безпеки та з формалізованого опису ІТС та процесів обробки інформації

Задача формального проектування

Основна задача формального проектування полягає у виборі методу формалізованого моделювання політики безпеки, методу формалізованого опису ІТС та процесів обробки інформації та формування алгоритму формування комплексу засобів захисту у ІТС з формальної моделі політики безпеки та з формалізованого опису ІТС та процесів обробки інформації.

Вимоги при розробці формальних описів КСЗІ

Можна виділити такі основні вимоги щодо складу та подання проекту архітектури комплексу засобів захисту:

1) опис усіх базових апаратних, програмно-апаратних та/або програмних засобів, що реалізують комплекс заходів захисту (далі – КЗЗ) з визначенням функцій механізмів захисту;

2) визначення взаємозв'язків між всіма компонентами на рівнях зовнішніх інтерфейсів, підсистем, потоків даних, керування тощо;

3) опис порядку захищеного функціонування кожного компонента КЗЗ – опис будь-яких операцій функціонального компонента КЗЗ, дії якого можуть спричинити зміну захищеного стану об'єкту, у вигляді послідовності дій, які виконуються в кожній підсистемі КЗЗ, як результат впливу на відповідний інтерфейс;

4) опис використовуваних зовнішніх послуг безпеки, що не входять до складу КЗЗ.

Для подання проекту архітектури у формалізованому вигляді (для заявлених рівнів гарантій Г-6 або Г-7), опис порядку захищеного функціонування компонентів КЗЗ має бути викладений згідно з попередньо-визначеними математичними поняттями. Пояснення математичних понять та використана нотація мають бути описані в неформалізованому вигляді. Мають бути визначені критичні властивості безпеки та виконувані над ними операції.

Для перевірки відповідності проекту архітектури та моделлю політики безпеки необхідно формально довести відповідність між захищеним функціонуванням компонентами КЗЗ та правилами політик реалізованих функціональних послуг безпеки (далі – ФПБ).

Критерії методів формалізованого моделювання політики безпеки

Критерії для методу формалізованого моделювання політики безпеки:

- складність реалізації моделі політики безпеки;
- наявність інструментальної підтримки.

Критерії методу формалізованого опису ІТС та процесів обробки інформації

Для проектування систем використовують різні мови, різні підходи, тому необхідно ввести критерії та показники для відбору найкращих кандидатів з ухилом на опис процесів безпеки та виконання вимог НД ТЗІ. Пропонується наступний перелік:

1) Складність. Показник складності характеризує, в першу чергу, здатність до адекватного опису потрібного параметру чи операції. Необхідність введення показника зумовлена тим, що при оцінюванні коректності реалізації рівня гарантій експерт може неправильно зрозуміти формальну модель, її формалізований вигляд або ж математичні концепції.

2) Орієнтованість на опис процесів обробки інформації. Під процесами обробки інформації найкраще тлумачення можна надати з [1] – виконання однієї або кількох операцій, зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації, приймання, отримання, передавання, які здійснюються в системі за допомогою технічних і програмних засобів.

3) Орієнтованість на опис процесів безпеки. Опис процесів безпеки можна поділити на чотири типи:

- конфіденційності;
- цілісності;
- доступності;
- спостереженості.

Кожна з чотирьох властивостей забезпечує захист від певної множини загроз.

4) Повнота вирішення задачі. Під критерієм мається на увазі здатність в повній мірі описати кожну ФПБ з [2]. Структура ФПБ та їх скорочення наведено в табл. 1.

5) Наявність інструментальної підтримки. Наявність готових програмних пакетів значно спрощує та прискорює процес розробки методики формального проектування. З іншого боку, готові інструменти для роботи можуть бути застарілі на даний момент, не підтримуватися розробниками чи багато коштувати.

Таблиця 1

Критерії				
Критерії конфіденційності	Критерії цілісності	Критерії доступності	Критерії спостережності	
Довірча конфіденційність (КД)	Довірча цілісність (ЦД)	Використання ресурсів (ДР)	Реєстрація (НР)	Розподіл обов'язків (НО)
Адміністративна конфіденційність (КА)	Адміністративна цілісність (ЦА)	Стійкість до відмов (ДС)	Достовірний канал (НК)	Автентифікація при обміні (НО)
Повторне використання об'єктів (КО)	Відкат (ЦО)	Гаряча заміна (ДЗ)	Ідентифікація та автентифікація (НИ)	Автентифікація відправника (НВ)
Аналіз прихованих каналів (КК)	Цілісність при обміні (ЦВ)	Відновлення після збоїв (ДВ)	Цілісність КЗЗ (НЦ)	Автентифікація отримувача (НП)
Конфіденційність при обміні (КВ)			Самотестування (НТ)	

Вибір методу формалізованого моделювання політики безпеки

Існують наступні методи формалізованого моделювання політики безпеки:

- UMLSec;
- Ponder2.

При виборі методу формалізованого моделювання політики безпеки далі наведено властивості методів UMLsec, Ponder2 та надано їх порівняльну характеристику за визначеними вище критеріями.

Проектування з використанням нотації UMLsec

Основа ідея UMLsec – розширення існуючої моделі UMLsec, шляхом додавання спеціальних міток – стереотипів, які додають відомості щодо безпеки. Відомості можуть бути наступного типу [3]:

- припущення щодо безпеки на фізичному рівні, наприклад як стереотип $||Internet||$;
- вимоги щодо безпеки на логічному рівні системи, наприклад як стереотип $||secrecy||$ (конфіденційність);
- вимоги політики безпеки, які накладаються на систему, наприклад як стереотипи $||secure\ links||$ (захищені зв'язки), $||no\ down\ flow||$ (керування потоком) .

Стереотип визначає новий тип елементів моделювання, розширюючи семантику вже існуючого типу або класу в моделі UML. Нотація стереотипу складається з імені стереотипу, взяті в подвійні прямі дужки || ||. Перелік стереотипів UMLsec наведено в табл. 2.

Таблиця 2

Стереотип	Базовий клас	Тег	Обмеження	Опис
fair exchange	subsystem	start, stop, adversary	Після старту з часом досягне зупинки	Реалізація чесного обміну
provable	subsystem	action, cert, adversary	Незаперечна дія	Вимоги до відмов
rbac	subsystem	protected, role, right	Виконується тільки для дозволених дій	Реалізація контролю доступу на основі ролей
Internet	link			Інтернет
encrypted	link			Зашифроване з'єднання
LAN	link, node			Локальна мережа
wire	link			кабель
smart card	node			Взуол смарт карти
POS device	node			POS-термінал

Продовження табл. 2

issuer node	node			Вузол постачальника
secrecy	dependency			Конфіденційність
integrity	dependency			Цілісність
high	dependency			Висока чутливість
critical	object, subsystem	Secrecy, integrity, authenticity, high, fresh		Критичний об’єкт
secure links	subsystem	adversary	Безпека залежностей відповідає посиланням «call», «send» відносно безпеки даних	Реалізація захищених ліній зв’язку
secure dependency	subsystem			Структурна взаємодія безпеки даних
data security	subsystem	adversary, integrity, authenticity	Забезпечує конфіденційність, цілісніть, автентичність, свіжість (новизна)	Базові вимоги до безпеки даних
no-down flow	subsystem	(data, origin)		Стан потоку інформації
no-up flow	subsystem	object name		Стан потоку інформації
guarded access	subsystem		Доступ до захищених об’єктів через механізми захисту	Контроль доступу з використанням захищених об’єктів
guarded	object	guard		Захищений об’єкт

Розширити модель можна значенням тегів елементу моделі. Теги можуть розширити можливості при описі властивостей даних. Перелік тегів UMLsec наведено в табл. 3.

Таблиця 3

Тег	Стереотип	Тип	Опис
start	fair exchange	state	Стан старту
stop	fair exchange	state	Стан зупинки
adversary	fair exchange	adversary model	Тип порушника
action	provable	state	Операція/дія, що потребує підтвердження
cert	provable	expression	Сертифікат
adversary	provable	adversary model	Тип порушника
protected	rbac	state	Захищені ресурси
role	rbac	(actor, role)	Призначення ролі
right	rbac	(role, right)	Призначення прав до ролі
secrecy	critical	data	Конфіденційність даних
integrity	critical	(variable, expression)	Цілісність даних
authenticity	critical	(data, origin)	Автентичність даних
high	critical	message	Повідомлення високого рівня
fresh	critical	data	Нові дані
adversary	secure links	adversary model	Тип порушника
adversary	data security	adversary model	Тип порушника
integrity	data security	(variable, expression)	Цілісність даних
authenticity	data security	(data, origin)	Автентичність даних
guard	guarded	object name	Захищений об’єкт

Таким чином, використання нотації UMLsec дозволяє доповнити вже існуючу модель UML за допомогою надбудов безпеки. До реалізованих в UML нотацій, додаються параметри безпеки, які дозволяють реалізувати вимоги політики безпеки та встановити відповідність між проектом архітектури та моделлю політики безпеки.

Використання нотацій Ponder2

Ponder2 поєднує в собі розподілену систему управління об'єктами загального призначення із службою домену, інтерпретатора зобов'язальної політики, інтерпретатора команд та застосування дотримання авторизації.

Ponder2 – це назва мови специфікації політики. Розробниками мови було розроблено набір інструментів та послуг для специфікації, аналізу та забезпечення застосування політик. Таким чином, Ponder – не тільки мова, а й набір інструментів.

Мова Ponder2 забезпечує загальний засіб визначення політик безпеки, які відображаються на різних механізмах реалізації контролю доступу для брандмауерів, операційних систем, баз даних тощо. Підтримуються, в першу чергу, два типи політик: політики авторизації, що визначає, які дії дозволені за певних обставин та політики зобов'язань, що визначає, які дії слід виконувати у відповідь на подію, що відбувається при виконанні конкретних умов.

Ponder2 визначає політики у форматі "предмет-дія-ціль" (subject-action-target, SAT). Ponder2 надає два типи політики авторизації, а саме позитивну авторизацію auth + та негативну авторизацію auth-. У Ponder2 зазначено лише один тип політики зобов'язань, в якому зазначено, що суб'єкт зобов'язаний виконати певні дії щодо цієї цілі. Політика зобов'язань може бути застосована лише за умови, що відповідна політика авторизації була вказана в системі. Поле події визначає активатор зобов'язання. Необов'язкові обмеження можуть застосовуватися до обох типів політик. Ці обмеження оцінюються щодо стану системи.

Порівняння методів формалізованого моделювання політики безпеки

1) Порівняння методів формалізованого моделювання політики безпеки виконано за двома основними критеріями – наявність програмного забезпечення методу розробки та складність реалізації:UMLsec та Ponder мають в своєму складі готове програмне забезпечення для розробки;

2) реалізація вимог політики безпеки, які будуть засновані на логіці методу Ponder2, не є інтуїтивно-зрозумілими і, як наслідок, їх нелегко відобразити механізмами мови. В свою чергу, UMLsec використовує базові механізми з відомого методу UML, що робить UMLsec більш привабливим методом формалізованого моделювання політики безпеки.

Отже, за критерієм складності UMLsec був обраний як метод для формалізованого моделювання політики безпеки, бо має більш зрозумілу та чітку нотацію.

Вибір методу формалізованого опису ІТС та процесів обробки інформації

Існує один промислово розповсюджений метод опису – UML. Інформаційна система в моделі UML зображується за допомогою основних елементів – компонентів, інтерфейсів та залежностей між ними. Формалізований опис ІТС подається у вигляді діаграми компонентів UML.

Діаграми UML доволі прості для розуміння після ознайомлення з його синтаксисом. Також існує можливість додавати власні текстові та графічні стереотипи, що значно розширює можливості застосування UML.

Завдяки розповсюдженості методу існує багато програмних середовищ для розробки UML-діаграм.

Алгоритм формування КЗЗ в ІТС з формальної моделі політики безпеки та з формалізованого опису ІТС та процесів обробки інформації

Вхідні дані алгоритму:

- діаграма компонентів UML (формалізований опис ІТС та процесів обробки інформації);
- формальний опис політики безпеки.

Діаграмою компонентів UML визначено вузли та інтерфейси системи. Усі інтерфейси кожного вузла перевіряються та висуваються необхідні вимоги політики безпеки. Проект архітектури КЗЗ, в підсумку, містить усі інтерфейси, правила їх взаємодії та вимоги політики безпеки.

Висновки

В ході досліджень було запропоновано методику формального проектування КСЗІ в ІТС, що включає в себе формальний опис ІТС та процесів обробки інформації, формальну модель політики безпеки та алгоритм формування комплексу засобів захисту в ІТС.

Були обрані метод формального опису ІТС та метод формального опису моделі політики безпеки, що можуть бути застосовані в алгоритмі формування КЗЗ в ІТС з формальної моделі політики безпеки та з формалізованого опису ІТС та процесів обробки інформації.

Список літератури:

1. J. J¨urjens Secure Systems Development with UML. Springer – Verlag, 2005.
2. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»
3. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Київ: Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, 1999. 61с.

Надійшла до редколегії 10.09.2020

Відомості про авторів:

Олійников Роман Васильович – д-р техн. наук, професор, професор кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук, Харківський національний університет імені В.Н. Каразіна, Україна; e-mail: roman.oliinykov@nure.ua, ORCID: https://orcid.org/0000-0002-3494-0493

Гвоздьов Роман Юрійович – магістрант, кафедра безпеки інформаційних технологій, факультет комп'ютерної інженерії та управління, Харківський національний університет радіоелектроніки, Україна; e-mail: roman.hvozdov@nure.ua

УДК 681.3.06:519.248.681 **DOI:10.30837/rt.2020.4.203.09**

І.Д. ГОРБЕНКО, д-р техн. наук, Д.О. ФЕСЕНКО

ВИКОРИСТАННЯ BLOCKCHAIN В АВТОМОБІЛЬНІЙ БЕЗПЕЦІ (AUTOMOTIVE SECURITY)

Вступ

Сучасними системами захисту автомобілів все більше цікавляться зловмисники, автомобілі стають більш технологічними, це в свою чергу відкриває нові можливості компрометації роботи вузлів та систем автомобіля, тому до систем безпеки пред'являються все більш жорсткі вимоги щодо забезпечення ефективності та безпечності їх функціонування. Сучасні системи захисту від незаконного заволодіння автотранспортом, більш відомі як «сигналізація», намагаються стримувати атаки зловмисників, але в свою чергу можуть привносити додаткові бекдори для зловмисників зовсім ненавмисно, наприклад додаючи цікаву функцію в систему автомобіля, а згодом ця функція може мати двояке значення через проблеми з системою автентифікації. Тож, системи безпеки автомобіля повинні мати найвищий рівень безпеки автентифікації, для реалізації якого пропонується використання децентралізованої мережі блокчейн з вузлами для кожного автомобіля, що автентифікують користувача групово, це дозволить відійти від стандартної клієнт-серверної архітектури, що є недостатньо захищеною. Основними шляхами вирішення зазначеної проблеми є побудування комплексної системи безпеки, що, в свою чергу, включає покращений та надійний захід автентифікації на основі децентралізованої мережі блокчейн та двох комплексних схем оновлення системи передачі критичних даних автомобіля – мережі CAN. Використання даних систем дозволить поліпшити показники захищеності системи автентифікації та інформації, що курсує між блоками критичної важливості, що покращить безпечність автомобіля як від угонів, так і від можливостей створення зловмисниками аварійних ситуацій дистанційно.

Мета статті – розгляд існуючих систем автентифікації для системи безпеки автомобіля та можливостей з інтеграції децентралізованих технологій для систем безпеки автомобіля на прикладі системи автентифікації.

1. Дослідження проблем сучасних автомобільних систем безпеки

Зараз існує багато брендів, що випускають продукцію для захисту безпеки автомобілів за допомогою різноманітних видів сигналізації. В описах своїх продуктів вони пропонують дуже гарну захищеність майже від всіх атак, але чи насправді це так? Цікавим є те, що всі розробки побудовані на добре відомій клієнт-серверній архітектурі.

Розглянемо дослідження різних команд, що займаються проблемами безпеки транспортних засобів, які були оприлюднені за результатами тестування безпечності найбільш використовуваних систем сигналізації.

Першою системою є рішення, при детальному розгляді якого виявилося, що в бекенд частині системи безпеки є небезпечні прямі посилання, що знаходяться прямо в головному API, тобто, використовуючи спеціально підготовлені параметри, можна без авторизації змінити критичні дані користувача, обновити пароль для доступу до акаунту та усі пов’язані з цим дані. Таким чином, зловмисник повністю отримує доступ до системи безпеки автомобіля, може додати свій ключ доступу до автомобіля. Повну процедуру розглянемо далі. Керування автоматичною трансмісією складається з кількох підсистем, що взаємопов’язані між собою та виконують свої функції, що в сукупності і дозволяє компонентам системи синхронізовано та правильно між собою працювати.

Підсистема обробки інформації забезпечує створення, зберігання, актуалізацію інформації про стан блоків транспортного засобу та можливості керування ними і складається із засобів обробки інформації, системного та функціонального ПЗ.

До засобів обробки інформації належать бортовий комп'ютер та встановлена кількість блоків керування для забезпечення всіх функцій щодо роботи, супроводження транспортного засобу та захисту інформації. Підсистема взаємодії з користувачами АС забезпечує моніторинг, керування даними блоків транспортного засобу, з використанням мереж передачі даних та стандартних CAN та LIN-протоколів.

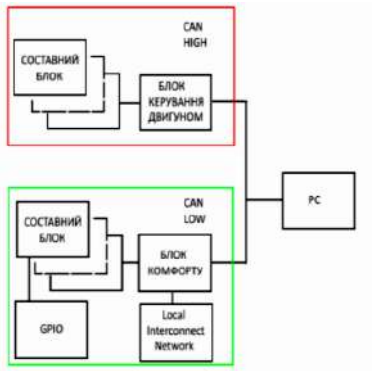


Рис. 1. Склад робочої станції

Технічні засоби, що встановлені на даному транспортному засобі та цікавлять нас при проведенні даного типу огляду, взаємопов'язані в мережу CAN, або контактують з нею.

Мережа CAN ділиться на два рівні абстракції: CAN High, в колі якого взаємодіють надзвичайно важливі для правильної роботи механізмів транспортного засобу блоки. Наприклад, в блок керування двигуном можна було б відправляти заготовлені зловмисником повідомлення для атаки інших блоків. Розглянемо приклади таких атак.

Перший вид атак – атаки на мережі, які підтримуються даним транспортним засобом, – це мережа Bluetooth, вектор атаки якого використовує помилки реалізації протоколу та дозволяє виконати атаку спарювання пристрою атакуючого з пристроєм, встановленим на авто.

Інший напрям – це мережа Wi-Fi, яка найчастіше буде використовуватися для доступу до мережі інтернет з метою серфінга інтернет-сторінок, оновлення навігаційних карт. Тут атаки можуть бути різноманітні: від реалізації атаки на стек до можливостей проведення Fake AP/MITM атаки.

В авто також встановлена система навігації GPS – ще один можливий напрям атаки, який, наприклад, може реалізовувати спуфінг координат або ж використовувати атаку на реалізацію самої системи.

Кожен автовиробник використовує спеціальну протиугонну систему – імобілайзер, що встановлюється в електронну систему керування та блокує роботу двигуна, якщо не знайдено спеціального ідентифікатора, що знаходиться в ключі автомобіля. Основна проблема в тому, що штатний імобілайзер не дозволяє підключень інших пристроїв до себе і подальшого їх використання. Для керування системами двигуна з використанням сторонніх систем безпеки виробники цих систем пропонують пристрої обходу імобілайзеру, що несе ще більше загроз. Розглянемо їх детальніше. Під час розгляду іншою командою дослідників було знайдено вразливість, яка використовує атаку на саме таку систему обходу імобілайзера. Як було вказано, система імобілайзеру повинна блокувати роботу двигуна і у випадку, коли був використаний варіант з обходу штатного імобілайзера, відкривалась можливість керувати системою імобілайзера через інтерфейси системи безпеки. Це з боку виробника подається в якості додаткової системи захисту, що начебто дозволить зупинити машину, якщо її вкрали і переганяють, але чином вся система через одну вразливість в серверній частині дозволяє зловмиснику зупинити двигун, коли це потрібно, що може привести до трагічних наслідків. Також виробники систем захисту використовують мережу CAN(Controller Area Network) для інтеграції своїх систем, що спрощує встановлення такої системи в авто, оскільки, використовуючи цю мережу, система безпеки може самостійно визначити дані про транспортний засіб

та на основі цих даних налаштувати систему та ввести її в дію. Але і в цьому плюсі є великий мінус: частіше за все пристрій системи безпеки доданий до мережі у гілку важливих частин автомобільних систем і таким чином скомпрометований пристрій може керувати іншими пристроями, пов'язаними з цими мережами таким самим чином, що і дозволяє системі безпеки отримувати дані про автомобільні системи. Цей канал зв'язку можна назвати дуплексним, він дозволяє як читати дані, так і записувати, тобто передавати команди пристроям, що знаходяться на одному рівні з системою безпеки. Пристрої – це електронні блоки, що керують важливими електронними системами автомобіля, а які саме – залежить від того, де встановлена скомпрометована система безпеки. Через відсутність автентифікації в протоколі CAN стає можливим маскувати ECU або замінити легальний ECU зловмисним за допомогою апаратного пристрою. До CAN-шини також може бути приєднаний пристрій зловмисника, який може не завжди спеціально представляти собою закладний пристрій, а може бути пристрій, який просто має в собі вразливості через їх недостатню захищеність, або й встановлений саме зловмисниками, наприклад під час ремонтних робіт, оскільки мережеві дроти більшості транспортних засобів легко виявити та використовувати для з'єднання.

Розглянемо два сценарії нападу, які використовують підмінні повідомлення на CAN-шині. Перший сценарій ілюструє атаку, коли оригінальна програма ECU замінюється шкідливою. Другий сценарій являє собою атаку, коли неавторизований пристрій підключено до CAN-шини. За безпеку в мережах та інформації в ЄС відповідає Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA), воно має сприяти та захищати передові практики щодо безпеки та стійкість критичного систем. Останнім часом агентство опублікувало звіт, в якому описує відсутність безпеки в поточних мережах автомобілів і представляє ряд можливих загроз і моделей нападу, які можуть бути виконані в мережі для виявлення стану кібербезпеки та стійкості систем автомобілів. Серед іншого, у доповіді згадується, що атака типу man-in-the-middle можлива шляхом підключення несанкціонованого пристрою безпосередньо до шини CAN. Також у звіті зазначено, що атаки відтворення дозволяють зловмисникам виявляти команди, які контролюють критичні системи безпеки, а також вказує на вразливість до атак відмови в обслуговуванні. Сучасні автомобілі мають спеціальний діагностичний порт, який називається портом OBD-II (бортовий діагностичний пристрій), який знаходиться під приладовою панеллю автомобіля. Цей інтерфейс дозволяє технікам виконувати діагностику засобів в мережі, перевіряти контроль викидів і повідомляти про будь-які несправності. Реалізація цього порту в автомобілях стала обов'язковою як у США з 1996 р. і в ЄС з 2001 р. Відомо, що за результатами дослідження, що були проведені незалежними експертами щодо автомобільної безпеки деяких автомобілів, є можливість ввести підроблені повідомлення на CAN шину Toyota Prius та Ford Escape. Ця атака була успішно проведена через те, що протокол CAN не надає жодної форми автентифікації, а повідомлення передаються по всій мережі у режимі широкомовної передачі. Опублікований звіт містить докладний опис того, як було здійснено атаку і на яких машинах було проведено атаку. Звіт також включає в себе архітектуру CAN, реалізовану в обох автомобілях, і їхні відповідні схеми підключення, код, який використовується для виконання атаки, і ідентифікатори повідомлень CAN обох автомобілів разом з відповідними функціями. Налаштування цієї атаки складалося з ноутбука, підключеного до порту OBD-II. Через те, що вдалося прочитати та записати в CAN-шину дані, ідентифікатори повідомлень були успішно ідентифіковані та була успішно виконана атака відтворення. Результати цього експерименту показали, що можливо відправляти підроблені повідомлення до важливих блоків для обох розглянутих в доповіді транспортних засобів, що призвело до відключення або примусового застосування гальм, вимкнення двигуна, відображення підроблених значень на панелі приладів, блокування та розблокування дверей і втручання як в внутрішні, так і в зовнішні вогні. В загальному вигляді пристрій, навіть якщо він не скомпрометований, буде підключений, тому для мережі при правильному налаштуванні компрометуючого пристрою (вірно проставлених ідентифікаторів пристрою та інше) буде виглядати як нескомпрометований пристрій, що готовий до робо-

ти. У випадку компрометації пристрою атака буде виконана в декілька етапів. По перше, треба вибрати пристрій для компрометації, наприклад розглянемо як такий пристрій ECU2, що є яким-небудь легкодоступним пристроєм, визначимо, що ECU2 буде видавати себе за пристрій ECU4, який буде пов'язаний з ECU двигуна. Для того щоб ECU2(NEW ECU4) став повністю працюючим скомпрометованим пристроєм, необхідно щоб пристрій не був дублікатом, тому його необхідно вимкнути. Для того щоб вимкнути пристрій з мережі, можна використати DOS атаку. Данні атаки мають багато варіантів реалізації, розглянемо деякі з них: DoS всієї шини дозволяє повністю запобігти комунікації CAN, генеруючи в шині безперервні з'єднання; цей стан не дозволить будь-якому вузлу надсилати повідомлення. Для проведення атаки необхідно згенерувати постійний рівень «0» в лінії приймача CAN. Багато реалізацій CAN мають вбудовані механізми запобігання таким порушенням. Але цей варіант не підходить для даного виду атаки, оскільки так вся мережа стане недоступною. Направлена DoS атака «DoS ACK» може бути направлена на один пристрій в мережі, вводячи домінуючі біти тільки в повідомленнях, надісланих на цільовий вузол. Для цього атакуючий повинен мати точні дані про ідентифікатори повідомлень, відправлених певним вузлом. Контролюючи шину для цільових ідентифікаторів, вона повинна вводити необхідні біти після фази арбітражу. Така заміна призводять до втрати цільових даних, лічильник помилок зростає, мережа відкидає пристрій з пріоритетності передачі і, тим самим, пристрій можна вважати вимкненим. Цей варіант повністю підходить для даного виду атаки, оскільки в цьому випадку стає недоступним лише пристрій, що атакується, а вся мережа працює в звичайному режимі. Після компрометації блоку відкривається можливість для проведення атак від імені скомпрометованого блоку. Шина CAN має послідовну схему з'єднання, тобто біти передаються один за одним від старшого біта до молодшого. Поняття байт до CAN зазвичай не вживається, тому в основному оперують терміном «поле». Довжина поля не повинна бути кратна байту (8 бітам). Протокол обміну даними проводиться фреймами. Фрейм складається з чотирьох основних полів: кода відправника, він же є основою арбітражу передачі даних; керуючого поле; даних; контрольної суми. Особливістю цього інтерфейсу є те, що біт, який передається, приймається приймачем CAN. Це допомагає проконтролювати правильність передачі даних та вести арбітраж на лінії між бажаючими передати дані. Передача йде «зліва направо», тобто першим піде ідентифікатор. При передачі ідентифікатора вузол вивчає стан лінії. Якщо необхідно передати 1, а на лінії раптом опинився 0, то це буде означати, що який-небудь більш пріоритетний ECU намагається передати свої дані. У цій ситуації передавач, який впіймав 0 замість переданого 1, не передає дані. Таким чином, чим менший ідентифікатор у передавального вузла, тим вище у нього пріоритет. Оскільки сучасний автомобіль практично всім керує за допомогою контролерів, тому і необхідно захищати з'єднання між блоками. Для цього необхідно розглянути декілька видів архітектури, що дозволила б надійно контролювати цілісність та відповідність даних, що передаються.

2. Захищеність мережі блокчейн

Багато відомих брендів автовиробників хочуть встановлювати на свої автомобілі власні системи безпеки з різними ідентифікаторами доступу для ідентифікації користувачів з їх транспортними засобами, але все одно всі ці сучасні розробки використовують систему з центральним сервером, який обробляє все запити. Розглянемо детальніше можливі сценарії, що можуть трапитися через такі вразливості. В системі такого типу встановлюється система глобального позиціювання, що відправляє на сервер дані про місце розташування автомобіля, тобто, отримавши доступ до аканту користувача, зловмисник може легко дізнатися, де знаходиться автомобіль, та вкрасти його, не докладаючи великих зусиль на пошук чи відстеження автомобіля. Якщо розглядати даний випадок з можливістю зміни чи отримання будь-яких даних, то будь-який більш-менш досвідчений розробник програмного забезпечення може зробити парсер для пошуку в базі автомобілів за маркою, роком випуску, місцем знаходження та іншими визначними параметрами, що зберігаються в акаунтах користувачів, та

можуть надаватися іншим зловмисникам за плату з метою знаходження бажаного автомобіля під замовлення. Це робить систему з централізованим доступом зберігання даних дуже небезпечним. Останнім часом з'являються нові проекти на основі децентралізованої системи блокчейн, що дозволяє вирішити питання автентифікації найбільш ефективно. Блокчейн – це система регістрів, які являють собою розподілену систему та не мають центрального органу, що складається з реєстрів обліку криптографічно підписаних транзакцій, згрупованих в блоки, де кожен блок пов'язується з попереднім після перевірки. На базовому рівні вони дозволяють спільноті користувачів записувати транзакції в загальнодоступному реєстрі групи користувачів цієї системи таким чином, щоб ніяка транзакція не могла би бути змінена після опублікування. Завдяки цим можливостям блокчейн успішно використовується для розробки рішень для різних сфер застосування, в першу чергу – в сфері електронної валюти. Після додавання нових блоків попередні блоки все важче модифікувати, оскільки вони копіюються по всіх реєстрах обліку всередині мережі та будь-які конфлікти вирішуються автоматично за допомогою встановлених правил.

Розглянемо можливі атаки, що можуть бути проведені для отримання неправомірного доступу до автомобілю зловмисниками. Ці атаки витікають з загальновідомих атак на будь-яку систему, що використовує в собі мережу блокчейн:

1) Атака Сібілли – тип атаки, що можливий в однорангових мережах, в яких вузол в мережі працює одночасно з декількома ідентичностями і підриває авторитет/владу в репутаційних системах. Основна мета цієї атаки – отримати більшість впливу в мережі для здійснення незаконних (стосовно правил і законів, встановлених у мережі) дій у системі;

2) DDoS (Distributed Denial of Service) – тип атак, ідея якої полягає в пересиланні великої кількості схожих запитів на один конкретний сервер або цілу мережу серверів з метою виходу з ладу частини мережі;

3) Зламування криптоалгоритмів. Злам алгоритмів, що використовуються для криптографічного захисту даних, що передаються та зберігаються, наприклад обчислення гешфункцій SHA-256 і ECDSA, вважаються досить стійкими при існуючих обчислювальних потужностях. Однак поява високопродуктивних квантових комп'ютерів збільшить ризик злому цих криптографічних функцій.

4) Пошук помилок та «бекдорів» у коді протоколів. На сьогодні це найбільша загроза для проектів, що будуються на базі блокчейн. Оскільки ця сфера є досить новою та складною навіть для досвідчених розробників, то час від часу знаходяться нові помилки у коді, що можуть завдати суттєвої шкоди усій системі;

5) (MITM) – атака типу людина посередині, це атака, яка більш за все нас цікавить при проектуванні системи безпеки автомобіля. В загальному випадку розглянемо в ролі вузлу, що буде атакуватися «Вузол 1», якому ми привласнимо ім'я Аліси (А), вузлу, що буде працювати з Алісою («Вузол 2») привласнимо ім'я Боб (В), також маємо зловмисника, який поставив собі за мету скомпрометувати, якого будемо називати Мелорі (Е).

Аліса відправляє Бобу повідомлення про запит на отримання блоку для синхронізації, яке перехоплює Мелорі:

$$A \overset{E}{\nrightarrow} B : \text{BLOCK REQ}$$

Розглянемо випадок, коли не буде використовуватися шифрування, а лише гешування блоків в вузлах, таким чином, не потрібно отримувати ключі шифрування.

Мелорі передає повідомлення Бобу, Боб на даному етапі не розуміє, що це повідомлення не від Аліси:

$$E \rightarrow B : \text{mod data}$$

Мелорі перехоплює блок Боба та модифікує його:

$$A \overset{E}{\nleftarrow} B : \text{BLOCK DATA}$$

Мелорі відправляє Алісі модифікований блок:

$$A \leftarrow E : \text{MOD BLOCK}$$

Аліса, отримавши повідомлення, намагається додати дані до ланцюгу блоків, але через використання механізму зберігання попередніх блоків виявляється факт підміни геш-значення пов'язаного блоку, і атака стає неможливою, а якщо цей блок ще не фігурував в блокчейні, то ця атака можлива. Для унеможливлення цієї атаки необхідно використовувати захищене з'єднання, що використовується далеко не завжди.

Ці атаки стають неможливими через те, що платформа, що планується до використання, вже має достатню кількість користувачів та надійне зберігання даних, що підтверджене роками використання платформи iOS, яка постійно оновлюється. Ця децентралізована система підходить для створення системи безпеки автомобіля наступного покоління, що забезпечила б гарний рівень гарантії для автентифікації користувачів.

Розглянувши детальніше принципи побудування системи на основі такої технології та потенційні атаки, можна зрозуміти, що рівень гарантій буде залежати від наявності достатньої кількості учасників. Будувати систему самостійно не є правильним рішенням. Необхідно використовувати платформи, в яких все достатньо користувачів та розповсюдженість буде найбільша.

3. Прототип системи CARKEY для автентифікації за допомогою мобільних пристроїв

Електронні коді доступу ключів CarKey зберігаються у додатку Wallet на iPhone користувача, функція CarKey нещодавно з'явилася у iOS 13.4. Спільний доступ до CarKey з кимось дозволить цій особі використовувати свій iPhone або Apple Watch для доступу до автомобіля, тримаючи пристрій біля зчитувача NFC, розташованого всередині транспортного засобу. Ключі можуть бути постійними (для подружжя) або тимчасовими (для водія або механіка). Функція CarKey дозволяє використовувати ваші iPhone та Apple Watch для розблокування/блокування автомобіля, запуску двигуна та керування автомобілем. Доступ до CarKey також як до Apple Pay та Apple Cash, засвідчується біометрично, використовуючи Face ID або Touch ID, щоб переконатися, що особа, яка тримає iPhone, є особою, яка має дозвіл на доступ до автомобіля.

Apple буде співпрацювати з виробниками автомобілів для CarKey, що вказує на те, що це може бути заводський варіант, подібний до CarPlay. CarKey вимагає транспортного засобу з NFC, тому виробники транспортних засобів повинні реалізовувати так, як це було «CarPlay» – мультимедійна система для автомобілів, що була розроблена Apple та активно використовується в даний час.

Apple є членом консорціуму автомобільної зв'язку (CCC), який розробив специфікацію Digital Key 2.0 на базі NFC, яка була доступна наприкінці 2019 року. Нова специфікація встановлює безпечний зв'язок між мобільними пристроями та транспортними засобами через NFC.

Консорціум CCC також працює над специфікацією Digital Key 3.0, заснованою на Bluetooth Le та Ultra Wideband, що дозволяє пасивний доступ до безключового ключа. IPhone 11, 11 Pro та 11 Pro Max від Apple підтримують ультраширокополосний діапазон, тому це функція CarKey, яку ми могли б побачити в майбутньому. Можливості отриманого програмно-апаратного комплексу із застосуванням додаткового відповідного математичного апарату дозволяють здійснювати синтез та аналіз безлічі класів сигналів, у тому числі й тих, які наведено у даній публікації.

4. Вразливості системи передачі даних NFC

NFC працює на дистанції до 10 см на частоті 13,56 МГц. Технологія потребує обов'язкової наявності відправника і отримувача. Пристрій відправника генерує активне поле, а пристрій отримувача зчитує його в пасивному режимі. Цікавим для зловмисників є

можливість отримання доступу до даних, що передаються по каналу передачі даних NFC, та методи захисту від такого виду атак. Над цими питаннями вже працюють вчені та хакери з усього світу, та вже є деякі успіхи в цьому, дослідникам вдалося отримати дані тестових NFC-приладів, що перебували на відстані 45 см від одержувача інформації. Відомий також вірус, що використовував relay-атаку та був створений з метою атакувати операційні системи смартфонів, що ініціював використання NFC смартфоном, що в свою чергу надсилав дані банківської карти зловмисникам, які, в свою чергу оплачували покупку карткою, використовуючи ретрансльовану транзакцію. Ще однією атакою на мережу NFC можна вважати використання засобами радіоелектронної боротьби або RFID-джаммерів. При їх використанні порушується робота ініціатора відправлення і система перестає працювати.

Розглянемо захист від атак на мережі, що використовують NFC. Безконтактна технологія, зручна, але як і кожна система має вразливі місця. Щоб забезпечити передачу даних NFC, при проектуванні системи важливо врахувати ризики, що пов'язані з можливістю елевації прав суперкористувача сторонніми додатками на смартфоні, якщо пристрій підтримує Root-доступ. Бажано налаштування, при якому система з Root-доступом на пристрої не буде працювати, або в такому випадку буде додатково використаний рівень абстракції з надійним шифруванням, оскільки отримання елевації прав дозволить з більшою вірогідністю встановити зловмисне програмне забезпечення.

Розглянемо втрату або крадіжку смартфону, на якому не встановлене блокування по пінкоду або відбитку пальця, та що зберігає NFC ідентифікатор.

5. Вибір платформи для зберігання ідентифікатору користувача

Компанія Apple на світовому ринку досить довгий час та продала вже приблизно два мільярди тільки лише iPhone, таким чином, використовувати таку платформу для цієї розробки дуже ефективно. Схема використання технології CarPlay є використання цієї платформи як основи для проміжного слою для інтеграції блокчейн-автентифікації, в якій CarPlay буде виконувати функції зв’язку з автомобілем та зберігання проміжних даних у захищеному сховищі, що в архітектурі Apple відомо як Wallet. На початковому етапі для використання системи користувачу необхідно завантажити додаток з офіційного магазину Apple – AppStore, що й буде основою керування доступу до автомобіля. Додаток являє собою повноправний вузол мережі блокчейн, що буде використовувати для зберігання критичних даних пристрій користувача. Після реєстрації, виконання усіх налаштувань та тестування роботи налаштувань пристрій буде доданий до мережі блокчейн та буде використовуватися для захисту автомобіля. В специфікаціях CarKey вказано, що є можливість передачі повноважень з доступу до автомобілю іншим особам. В рамках цієї блокчейн системи для цих цілей за необхідності будуть видані тимчасові токени для доступу стороннім особам. Для автентифікації в додатку необхідно буде вибрати дію, яку необхідно виконати з автомобілем (відкрити/закрити, дозволити запуск двигуна, чи інші дії, що доступні в залежності від встановленої комплектації засобів захисту), також, при наявності смарт-годинника Apple Watch буде можливість використовувати його як мітку для автентифікації, доступ до додатку також буде доступний з екрану Apple Watch. Після створення запиту на виконання дії з транспортним засобом він буде направлений до мережі блокчейн, де інші вузли повинні підтвердити, що пристрій та користувач, що створив запит є саме тим, кого за себе видає, все це проходить в автоматизованому режимі, підтвердження проходить за рахунок пристроїв, які мають запущеними додаток (навіть як сплячий процес). Після успішного підтвердження користувача надається доступ до можливості генерування мітки доступу для автентифікації. Якщо ви використовуєте Apple Watch, ви знаєте, що він пов’язаний з вашим iPhone (принаймні більшу частину часу). Він має доступ до більшості даних, які є на вашому iPhone – до ваших контактів, календарів, електронних листів, повідомлень тощо. Хоча Apple Watch підключається до iPhone з використанням систем автентифікації, все ж є ймовірність, що якщо ваш годинник загублений або вкрадений, хтось може отримати доступ до деяких ваших особистих даних. Додаток Watch

на iPhone дозволяє налаштувати багато налаштувань пристрою, і ви можете отримати доступ до деяких із них через додаток «Налаштування» самого годинника, де ви можете налаштувати параметри розблокування Apple Watch за допомогою iPhone, що робить Apple Watch доступним до використання, поки годинник знаходиться на зап'ясті. Ви можете налаштувати це налаштування в налаштуваннях пароля програми Watch. Якщо вимкнути це налаштування, то вам доведеться вводити пароль кожного разу, коли ви кладете годинник. За замовчуванням Apple Watch просить встановити чотиризначний пароль. Це й є основою автентифікації користувача. Як і в iPhone, існує налаштування самоочищення даних, яке видаляє всі користувацькі дані на Apple Watch при спробах брутфорсу пін-коду годинника. Зловмисник, що заволодіє годинником, але не вгадає пароль після десяти спроб, ніколи не отримає ваші дані.

6. Загрози iOs. Джейлбрейк. Програмні атаки на NFC

Деякі загрози безпеки можуть йти від самого користувача. Наприклад, не кожного власника брендових гаджетів задовольняє обмежена можливість оновлення програмного забезпечення і встановлення лише схвалених і перевірених розробником додатків. Такі користувачі роблять джелбрейк (jailbreak) – процедуру отримання повного доступу до файлової системи iOS, яка можлива завдяки наявності вразливостей в системі безпеки операційної системи. Після проведених маніпуляцій разом з можливістю встановлення сторонніх додатків зростає ймовірність проникнення шкідливих програм.

Джейлбрейк (від англ. Jailbreak – «Втеча з в'язниці») – це організація несанкціонованого розробником доступу до файлової системи в iOS з метою відкрити перед користувачем можливість установки додатків з неофіційних репозиторіїв і дослідження внутрішнього середовища ОС. Як правило, для цього використовуються виявлені в iOS вразливості. Саме тому можливість джейлбрейку з'являється зазвичай дещо пізніше виходу чергової версії iOS. Apple згодом закриває виявлені вразливості, але дослідники відшукують все нові і нові лазівки. На даний момент методи встановлення джейлбрейку прийнято ділити на дві умовні категорії.

Відв'язаний (неприв'язаний) джейлбрейк (untethered jailbreak) робиться один раз і назавжди, такий пристрій можна перезавантажувати без втрати доступу до файлової системи. Злітає він тільки після перепрошивки пристрою. Очевидно, що подібний джейлбрейк можливий далеко не на всіх версіях iOS.

Полувідв’язаний джейлбрейк (semi-untethered jail-break) працює лише до першого перезавантаження або відключення живлення пристрою. Після включення айфона потрібно заново запустити утиліту джейлбрейка, яка повторно заллє на телефон всі необхідні компоненти і змусить його завантажитися в робочому режимі.

Після виконання операції джейлбрейку на пристрій буде встановлений спеціальний магазин додатків “Cydia”. З цього магазину додатків можна встановити додаткове програмне забезпечення для модифікації системи, також інші магазини з програмним забезпеченням, за допомогою яких, використовуючи сертифікати корпоративних розробників, вони встановлюють на пристрій будь-якого користувача свій контент. Додатки підписуються як «корпоративні розробники», причому на одному такому акаунті можуть перебувати відразу декілька «магазинів». Корпоративний профіль купується в мережі і сфабрикувати необхідний не так вже й складно.

При завантаженні будь-якої програми з App Store на iPhone або iPad з'являється .ipa файл, який підписується вашим обліковим записом, щоб його не можна було запустити на іншому пристрої (наприклад, щоб ви після покупки гри не могли «передати» її одному безкоштовно). Сторонні «магазини» роблять те саме, підписуючи файли під своїм обліковим записом. Але щоб ці програми можна було встановити, на iPhone або iPad необхідно встановити спеціальний профіль, який підтвердить, що на вашому пристрої можна використовувати дані .ipa файли. Власне, користувачі роблять це самі. Після цього вони, задоволені, біжать

завантажувати безкоштовні програми на свої iPhone і iPad (або додаток зі зламаними вбудованими покупками). І дуже сильно ризикують.

Але деякі додатки можуть містити в собі зловмисний код, оскільки додатки в таких магазинах не перевіряють, як це робиться в офіційному магазині «App Store» від Apple.

Власники подібних «магазинів» можуть виявитися шахраями (в більшості випадків так воно і є), які залучають користувачів безкоштовними додатками. Самі вони поширюють програми, що містять шкідливий код, або, що ще гірше, інструменти для отримання доступу до даних на пристрої. Оскільки вони працюють безпосередньо з файлами додатків, звичайна гра може виявитися, наприклад, прихованою програмою.

При запуску додатків, створених за допомогою модифікованої версії Xcode, пристрій відправляв зловмисникам пакет даних про користувача. У нього входили назва програми, час, тип і унікальний ідентифікатор пристрою, країна місця знаходження та мова інтерфейсу, а також тип підключення до інтернету.

Крім цього, XcodeGhost відображав підроблені повідомлення від додатків (наприклад, щоб через фішингові схеми змусити користувача ввести свої дані), перехоплював процес відкриття сторонніх посилань, а також міг читати вміст буфера обміну системи. Останнє дозволяло зловмисникам красти паролі користувачів, скопійовані з сторонніх менеджерів кодів доступу на зразок 1Password. Хоча додатки в App Store проходять процедуру верифікації, в даному випадку модератори Apple не помітили попадання шкідливого коду в їх систему. На думку дослідників в Palo Alto Networks, в порівнянні з іншими вірусами, створеними для iOS, поведінка XcodeGhost було не таким вже й підозрілим. Метою впровадження вірусних програм до файлової системи iOS є отримання доступу до особистої інформації, паролів доступу до банківських сервісів і платіжних систем, стеження за користувачем, розсилка спаму і реклами тощо. Вберегтися від втручання зловмисників у роботу мобільних пристроїв Apple можна, ретельно дотримуючись правил безпеки:

- не використовувати модифіковані версії iOS;
- своєчасно оновлювати операційну систему після появи офіційних версій;
- для встановлення нових додатків користуватися лише AppStore, звертати увагу на відгуки інших користувачів.

7. Використання пристрою з модулем NFC як засіб автентифікації

Основною метою цього дослідження є проектування можливості використання телефону або іншого пристрою з NFC як засобу надійної автентифікації і розробка програмного забезпечення для безпечної автентифікації користувача за допомогою NFC. Для поліпшення безпеки автомобільних систем безпеки були введені безліч варіантів використання багатофакторної автентифікації для віддалених сервісів: SMS, TOTP цифрові ключі, спеціальні маркери доступу, але як показано з досліджень вище навіть стійка на перший погляд клієнт-серверна архітектура керування системою безпеки не надає необхідного ступеня безпеки, може мати в собі скриті загрози, бекдори та баги розробників. Такі системи можуть стати складні або незручні в застосуванні, наприклад при верифікації доступу до автомобілю за допомогою SMS, що буде ускладнювати життя господаря автомобіля. Тому пропонується розглянути систему автентифікації за допомогою NFC з можливістю виконувати автентифікацію в один дотик до зчитувача. За основу пропонується взяти пристрої на платформі iOS від компанії Apple, розробки якої описувалися вище, нас цікавлять смартфони, шо підтримують технологію NFC та «розумні» годинники Apple Watch, в яких присутній NFC-модуль, що дозволяє працювати в трьох режимах: зчитування і запису міток, режим p2p та режимі емуляції безконтактної банківської карти. Ці пристрої можуть працювати в режимі емуляції карти, який надає можливість обмінюватися APDU повідомленнями з іншими учасниками. Пристрої також підтримують інші стандарти, що необхідні для створення системи автентифікації: U2F – стандарт для швидкої, зручної та безпечної двофакторної автентифікації за допомогою окремого пристрою. Даний вид автентифікації передбачає наявність у користувача окремого фактора воло-

діння криптоключа. Протокол U2F використовує принцип посилки сервісом унікального challenge і відповіді клієнта з підписом, що використовують алгоритм ECDSA з еліптичної кривої secp256r1. Для роботи програмного модулю системи автентифікації розглянемо систему з використанням NFC в якості додаткової системи до вже встановленої системи сигналізації. Під час реєстрації пов'язаний пристрій власника транспортного засобу посилає іншим учасникам мережі повідомлення про наміри проведення автентифікації до транспортного засобу. Пристрої усіх учасників мережі отримують повідомлення про наміри іншого користувача автентифікуватися. Отримавши повідомлення, користувачі порівнюють передані дані з своїми блоками та визначають, чи валідний запит чи ні, після чого підтверджують транзакцію або ні, як і у випадку з іншою системою, що побудована на основі мережі блокчейн – біткоін. У випадку, коли транзакція буде підтверджена більшістю (більше за 51 % проголосувавших за визнання транзакції валідною). Результат операції повертається тому, хто запитував право на доступ до автомобіля. В якості ініціалізуючої системи виступає смартфон на базі iOs чи годинник Apple watch, що підтримують можливість використовувати технологію NFC для створення каналу зв'язку для проведення автентифікації користувача автомобіля і системи безпеки; у випадку співпадіння даних мітки користувачу буде дозволено поступ. Для користувача така система ще простіша – можна не мати при собі ключа від машини, а смартфон чи годинник багато користувачів мають з собою завжди. Таким чином, за допомогою описаних вище процедур цей додаток можна використовувати для безпечної автентифікації користувача з системами, що будуть підтримувати програмно-апаратну реалізацію системи з наявністю NFC передавача та мобільних операційних систем.

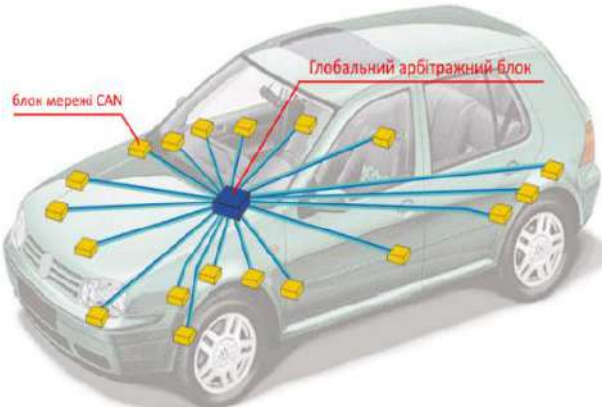


Рис. 2. Централізована схема архітектури попередження вторгнення

Архітектура являє собою мережу, що об'єднує всі блоки між собою, використовуючи спеціальний блок арбітражу, або, як можна його назвати, «глобальний арбітражний блок». Схематично архітектура являє собою систему, що зображена на рис. 2. Основу мережі складає арбітражний блок, який приймає пакети від інших складових блоків мережі CAN, що передають дані один одному. Цей блок визначається найголовнішим блоком в цій системі, якому надані повноваження щодо визначення, чи являються передані дані такими, що саме ці дані були передані від визначеного блоку. Іншими словами, гарантує цілісність даних, що були отримані від блоку, гарантує правильну доставку повідомлення до отримувача та загальну автентифікацію даних, що передаються блоками. Для цього необхідна реалізація системи автентифікації між компонентами системи, яка би являла собою криптографічний протокол встановлення достовірності твердження, що об'єкт у вигляді повідомлення від блоку має очікувані властивості, надавала б гарантії справжності ідентифікаційних даних від блоку, що ініціює передачу. Система повинна виключати можливість реалізації загроз типу «маскарад», «повтор», «підміна» та компрометацію заявленої інформації автентифікації. Розглянемо детальніше захищеність архітектури з глобальним арбітражним блоком від визначених загроз.

Загроза типу «маскарад» полягає в обмані одного об'єкта іншим об'єктом, коли нав'язаний об'єкт видається в якості достовірного, що, наприклад, можливо при перепрограмуванні блоку на необхідні дії, при цьому залишаються параметри, що належать достовірному блоку, тим самим видаючи себе в мережі за достовірний блок. Для захисту від загроз, що належать до такого типу, в системі планується використовувати спеціальні дані у вигляді шифрованого коду автентифікації алгоритмом A5/1.

Загроза типу «повтор» полягає у повторі інформації, що була передана раніше під виглядом нової. Використовувати механізми автентифікації на основі ЕЦП, що було б найкращим рішенням з огляду безпеки, бо ЕЦП забезпечує послугу неспростовності пред'явника найкращим чином, але використання такого виду криптоперетворення не підходить для такого виду системи через його розрахункову складність, бо система має бути побудована на не потужних компонентах. Для захисту від атак типу «повтор» необхідно ввести в систему мітку часу генерації пакету, що дозволяла б ідентифікувати невалідні пакети, якщо ті передаються пізніше ніж закінчився час життя пакета. Додатковою мірою захисту планується введення випадкового значення

Загроза типу «підміна» можлива за умови наявності заздалегідь перехоплених повідомлень від блоку, що необхідно скомпрометувати, або даних арбітражного блоку. Вона зводиться до модифікації істинної обмінної інформації на хибну. Для захисту проти загроз типу «підміна» краще використовувати послугу цілісності, наприклад з використанням для обміну при автентифікації ЕЦП чи коду автентифікації, а також шифрування. В даній архітектурі цю функцію буде використовувати алгоритм шифрування A5/1. Цілісність забезпечується за рахунок використання контрольних сум CRC або функції гешування SHA-1, що дозволяє ефективно захистити цілісність даних та захиститися від атак типу «підміна». Основною перевагою даної архітектури є можливість реалізації системи, що не потребувала б компонентів великої потужності, що робить систему більш економічно та технологічно обгрунтованою для масового використання у виробництві. Оскільки для роботи системи необхідний лише один арбітражний блок високої потужності, що може обробляти усі запити та відповіді від блоків, які передаються від одного до іншого, та виконує роботу з визначення параметрів безпеки передачі повідомлень лише відповідно до даних, що передаються, це дозволяє зменшити навантаження на інші блоки (складові) і дозволяє не робити різні рівні абстракції для мережі CAN, як це реалізовано зараз, але надавати рівень безпеки вищий ніж з використанням рівнів абстракції.

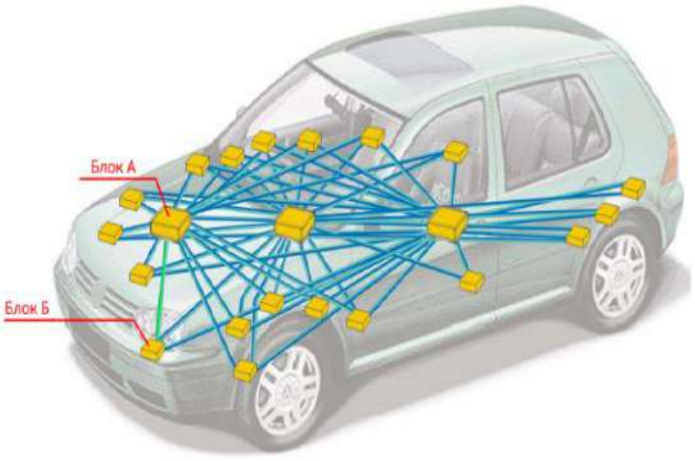


Рис. 3. Централізована схема архітектури попередження вторгнення

У іншому варіанті система представляє собою схожу архітектуру до першої, але її відмінність в тому, що вона побудована на принципах децентралізації та не має будь-яких арбітражних блоків чи рівнів абстракції за будь-якими параметрами зовсім. Схема архітектури зображена на рис. 3. Кожен із блоків являє собою частину децентралізованої мережі, кожен із яких сам відповідає за оброблення параметрів безпеки та визначення захисту від атак. На

рис. 3 показано як блоки А та Б з'єднуються між собою напряму, без будь-яких засобів арбітражу. Кожен з блоків підтримує систему взаємної автентифікації з двома проходами та використовує ідентичні системи гарантування безпеки, використовує базу використаних випадкових чисел, що зберігається на кожному з блоків та гарантує ефективний захист від атаки типу «повтор».

Таким чином, при використанні будь-якої архітектури з описаних можна ефективно забезпечити безпечну та цілісну передачу пакетів у мережі CAN між блоками з можливістю забезпечити ефективну роботу автомобільних систем.

Висновки

Використання технології блокчейн в системі автентифікації автомобіля дозволить розширити можливості безпеки автентифікації для доступу до автомобіля, роблячи цей процес простішим для користувача, бо всі дії можна виконувати за допомогою смартфону, що працює на широко відомій платформі, але ж і підвищується рівень безпеки та довіри, що не вимагає додаткових грошових вкладень, легкий до налаштування та використання та добре захищений від постквантових атак і від інших видів атак, що зараз є дуже загрозливими для безпеки сучасної автоіндустрії. Великим плюсом є, що Apple буде співпрацювати з виробниками автомобілів для CarKey, та є вірогідність виконання версії заводського варіанту, що зробить цю технологію ще більш доступною, простою для потенційних користувачів. Системи безпеки автомобіля будуть мати високий рівень безпеки автентифікації, для реалізації якої використовується децентралізована мережі блокчейн з вузлами для кожного автомобіля, що автентифікують користувача групово та 51 % інших вузлів має підтвердити запит на автентифікацію. В іншому випадку автентифікація буде неможливою і доступу до транспортного засобу надано не буде. Таким чином, вирішуються проблеми автентифікації та безпечності передачі даних між блоками між собою, що перетворює розроблену систему в покращений та надійний захід автентифікації на основі децентралізованої мережі блокчейн та двох комплексних оновлених схем системи передачі критичних даних всередині автомобіля.

Список літератури:

1 NISTIR 8202. Blockchain Technology Overview / NIST // NISTIR. Gaithersburg : US Department of Commerce, 2017. P.1-26.

2. Brown. Vehicle Security Systems // Build Your Own Alarm and Protection Systems. Newnes, 1601996. P. 7 – 155.

3. Knight A., Hacking Connected Cars: Tactics, Techniques, and Procedures. K. : Information Systems, 2019. P. 5-250

4. Car Security 101 [Електронний ресурс]. Режим доступу: www/ URL: https://www.lifewire.com/car-security-101-534872 – 01.05.2020 р.

Надійшла до редколегії 03.10.2020

Відомості про авторів:

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

Фесенко Дмитро Олександрович – магістрант, кафедра безпеки інформаційних технологій, факультет комп'ютерної інженерії та управління, Харківський національний університет радіоелектроніки, Україна; e-mail: ddfff21@gmail.com

УДК 004.056.5 **DOI:10.30837/rt.2020.4.203.10**

К.Ю. ШЕХАНІН, Ю.І. ГОРБЕНКО, канд. техн. наук,
Л.О. ГОРБАЧОВА, О.О. КУЗНЕЦОВ, д-р техн. наук

ДОСЛІДЖЕННЯ ВЛАСТИВОСТЕЙ НОСІЇВ ІНФОРМАЦІЇ ДЛЯ СТЕГАНОГРАФІЧНОГО ПРИХОВУВАННЯ ДАНИХ В КЛАСТЕРНИХ ФАЙЛОВИХ СИСТЕМАХ

Вступ

Із розвитком інформаційних технологій важливим стало питання як зберігати, передавати та оброблювати інформацію таким чином, щоб оптимізувати цей процес, тобто зменшивши витрати та підвищивши швидкодію та якість відповідних сервісів. Інколи інформація повинна бути захищена – цим займається галузь науки криптографія, яка гарантує доступ до інформації лише авторизованим користувачам. Але у разі використання криптографічних методів для неавторизованих користувачів (потенційних зловмисників) відомо про сам факт збереження або передачі інформації [1 – 3]. Це у подальшому може призвести до розкриття змісту інформації шляхом використання методів криптоаналізу. Щоб уберегти інформацію від розкриття використовують стеганографічні методи [4 – 6].

Стеганографія – це наука, яка забезпечує приховання самого факту обробки, зберігання чи передачі інформації, на відмінну від криптографії яка забезпечує лише захищеність змісту інформації [5]. Використання стеганографії доповнює криптографічні методи, тож ці методи є компліментарними один до одного з точки зору захищеності інформації. Як приклад можна згадати використання шифру Цезаря – це буде криптографічний метод, та використання «невидимих» чорнил – це буде стеганографічний метод [4, 5, 7]. А якщо сумісно використати ці два методи, то зловмиснику необхідно спочатку буде знайти текст, написаний невидимими чорнилами, а лише потім розшифрувати шифр Цезаря. Звісно, у сучасності данні методи не є ефективними. Наразі більшої популярності набувають методи комп'ютерної, або цифрової стеганографії [4, 5, 7 – 10]. Інформаційні повідомлення подаються у вигляді цифрових даних, які приховуються в інших цифрових даних (т.з. cover data). Cover files передаються та зберігаються у відкритому вигляді, це можуть бути, наприклад, цифрові зображення, які у великій кількості передаються сучасними каналами електронної пошти. Але вповноважений отримувач, який має секретний ключ, приймає cover file та може відновити таємне повідомлення. Звісно, що при цьому приховується сам факт існування таємного повідомлення, відслідкувати та дослідити всі cover files в інтернеті фізично неможливо [9 – 11].

Стеганографічні методи постійно вдосконалюються та розвиваються. Основна вимога до cover files є їхня надмірність (збитковість). Наприклад, надмірність цифрових зображень дозволяє приховати досить великі за обсягом інформаційні повідомлення.

Останніми роками набули розвитку методи технічної стеганографії. В таких системах приховування інформації досягається шляхом використання властивостей, які штучно зроблено людиною при побудові різних технічних засобів. Як приклад, можна навести мережеву стеганографію [12 – 16], в якій застосовуються різні особливості побудови сучасних телекомунікаційних систем та мереж, в тому числі штучна надмірність при визначенні форматів пакетів даних та способів їхньої передачі [17 – 19]. В 3D стеганографії використовуються надмірності цифрових 3D моделей та створених за їх допомогою фізичних об'єктів [20 – 24]. Наприклад, у роботах [25, 26] запропоновано приховувати інформацію шляхом створення фізичних об'єктів всередині інших (cover) об'єктів.

Ще одним прикладом технічної стеганографії є застосування особливостей побудови кластерних файлових систем. Зокрема, у роботах [27 – 29] запропоновано методи, які дозволяють ефективно приховувати інформацію шляхом зміни чергування (рос. – чередование) окремих кластерів т.з. покрівельних файлів. Імена (назви) таких файлів є ключовою інформацією і відновити приховане повідомлення без посилань (тобто без назв) покрівельних фай-

лів вкрай важко. Подальші дослідження кластерних файлових систем [30 – 36] дозволяють стверджувати, що застосування особливостей організації зберігання інформації дає змогу отримати надійний та безпечний механізм стеганографічного приховування інформаційних повідомлень. Звісно, що стійкість та швидкодія кластерних стеганосистем безпосередньо спирається на конкретні властивості файлової системи. Зокрема, безпека спирається на фрагментарність та переплетеність (в термінах робіт [27, 27, 30, 33]) покрівельних файлів, а швидкодія залежить від фрагментарності файлової системи та характеристик конкретного носія інформації. Отже, актуальним є питання аналізу різних носіїв інформації та відповідних файлових систем для можливого застосування в стеганографічних методах приховування, дослідження впливу окремих показників на ефективність кластерних стеганосистем.

Мета роботи – аналіз відомих технологій зберігання інформації, дослідження властивостей фрагментарності файлової системи та переплетеності окремих файлів на швидкість запису/зчитуванні інформації. Практичне значення отриманих результатів полягає у їх безпосередньому застосуванні до обґрунтування рекомендацій з побудови кластерних стеганосистем.

1. Методи приховування інформації у кластерні файлові системи

Файлова система встановлює порядок, спосіб організації, зберігання та іменування даних на носіях інформації в інформаційних системах, а також в іншому електронному обладнанні: цифрових фотоапаратах, мобільних телефонах і т.п. [37 – 39]. Файлова система визначає формат вмісту і спосіб фізичного зберігання інформації, яка групується у файли. Конкретна файлова система визначає розмір імен файлів і (каталогів), максимальний можливий розмір файлу і розділу, набір атрибутів файлу, тобто визначає метадані файлів. Деякі файлові системи надають сервісні можливості, наприклад, розмежування доступу або шифрування файлів.

Найпростіші методи приховування інформації у структурі файлових систем розглянуто в [32, 34 – 36]. Дані методи застосовують вільні кластери (або службові поля даних) для запису прихованої інформації, але такий спосіб, з точки зору конфіденційності інформації, є ненадійним [27, 29]. Інші методи, наприклад [27 – 31], ґрунтуються на використанні покриваючих файлів (cover file) і приховуванні інформаційних даних за допомогою взаємного перемішування файлів, тобто зміни відносних позицій кластерів декількох покриваючих файлів один щодо одного.

1.1. Приховування інформації через перемішування кластерів

Приховування інформації через перемішування кластерів різних cover files досліджено у роботах [27, 29]. Прихована інформація представляється у вигляді бітового масиву: $M = \{b_0, b_1, ..., b_{n-1}\}$, $b_i \in \{0,1\}$. На інформаційному носії обирають $p = 2^m$, $m \in N$ покриваючих файлів (cover files): $F_0, F_1, ..., F_{p-1}$. Порядок кластерів покриваючих файлів приховує інформаційне повідомлення, тобто після вбудовування покриваючи файли не можна модифікувати, видаляти та переміщувати. Натуральне число m та імена покриваючих файлів є секретним ключем. Важливий також порядок упорядкування cover files [29].

Формується масив номерів кластерів покриваючих файлів:

$$C = \begin{pmatrix} c_{0,0} & c_{0,1} & \dots & c_{0,L_0-1} & & & \\ c_{1,0} & c_{1,1} & \dots & \dots & \dots & \dots & c_{1,L_1-1} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ c_{p-1,0} & c_{p-1,1} & \dots & \dots & c_{p-1,L_{p-1}-1} & & \end{pmatrix},$$

де кожен рядок масиву містить номера кластерів відповідного файлу. Наприклад, файлу F_i відповідає i-й рядок масиву C, тобто номера кластерів i-го покриваючого файлу можуть бути подані у вигляді масиву $C_{F_i} = \{c_{i,0}, c_{i,1}, ..., c_{i,L_i-1}\}$, де L_i _ число кластерів в i-у покриваю-

чому файлі. Якщо при приховуванні інформації необхідно зберегти без зміни вміст покриваючих файлів, тоді потрібно, щоб виконувалися умови: $\forall i: L_i \geq k$, $k = n/m$.

Формується масив D номерів вільних кластерів файлової системи: $D = \{c_1, c_2, ..., c_{L_D}\}$, так щоб виконувалася умова $c_1 < c_2 < ... < c_{L_D}$. Число L_D дорівнює кількості вільних кластерів файлової системи, причому потрібно, щоб виконувалася умова: $L_D \geq \sum_{i=0}^{p-1} L_i$.

Інформаційне повідомлення M розбивається на блоки по m бітів: $M = \{B_1, B_2, ..., B_k\}$, де $k = \lceil n/m \rceil$ та якщо $k = n/m$, то $B_1 = \{b_0, b_1, ..., b_{m-1}\}$, $B_2 = \{b_m, b_{m+1}, ..., b_{2m-1}\}$, …, $B_k = \{b_{(k-1)m}, b_{(k-1)(m+1)}, ..., b_{km-1}\}$. Якщо $k < n/m$, то останній блок необхідно дописати неінформаційними значеннями, наприклад нулями, $B_1 = \{b_0, b_1, ..., b_{m-1}\}$, $B_2 = \{b_m, b_{m+1}, ..., b_{2m-1}\}$, …, $B_k = \{b_{(k-1)m}, b_{(k-1)(m+1)}, ..., b_{n-1}, \underbrace{0, 0, ..., 0}_{km-n}\}$. Кожен блок B_i, $i = 1, 2, ..., k$ подається як натуральне число, тобто $\forall i: 0 \leq B_i \leq p-1$. Кожне натуральне число B_i, $i = 1, 2, ..., k$ подається як номер покриваючого файлу з множини файлів $F_0, F_1, ..., F_{p-1}$.

Всі кластери покриваючих файлів перезаписуються у вільні кластери файлової системи, тобто масив D заповнюється номерами кластерів із масиву C. Порядок перезапису кластерів покриваючих файлів відповідає послідовності натуральних чисел $\{B_1, B_2, ..., B_k\}$, що задаються приховуваним повідомленням. Для прикладу, у перший вільний кластер записуємо перший кластер покриваючого файлу із номером B_1, у другий вільний кластер – наступний кластер покриваючого файлу із номером B_2 і так далі. Натуральні числа B_i можуть співпадати і в цьому разі записуємо наступний кластер того ж самого покриваючого файлу із номером B_i. Для посилення захисту від детектування та декодування стеганосистеми додатково можуть застосовуватися певні механізми, наприклад [29], обирається ключ ініціалізації B_0, а порядок перезапису кластерів покриваючих файлів задається послідовністю натуральних чисел $\{N_1, N_2, ..., N_k\}$, $N_i = B_{i-1} + B_i \bmod p$, $0 \leq N_i \leq p-1$. Тоді, у перший вільний кластер перезаписуються перший кластер покриваючого файлу із номером N_1, у другий вільним кластер – черговий кластер покриваючого файлу із номером N_2 і так далі.

В результаті виконання алгоритму перші k вільних кластерів файлової системи будуть записані кластерами покриваючих файлів. Отже, повинна виконуватися умова $k \leq L_D$.

Для вилучення прихованого повідомлення M формується масив D номерів кластерів покриваючих файлів: $D = \{c_1, c_2, ..., c_{L_D}\}$, причому необхідно, щоб виконувалась умова $c_1 < c_2 < ... < c_{L_D}$. Кожен номер кластеру з цього масиву співвідноситься тільки з одним кластером одного покриваючого файлу. Саме така відповідність пов’язана із логікою вбудовування інформації і використовується для вилучення прихованої інформації. Формується послідовність натуральних чисел $\{B_1, B_2, ..., B_k\}$, які відповідають блокам прихованого повідомлення: $B_1 = \{b_0, b_1, ..., b_{m-1}\}$, $B_2 = \{b_m, b_{m+1}, ..., b_{2m-1}\}$, …, $B_k = \{b_{(k-1)m}, b_{(k-1)(m+1)}, ..., b_{km-1}\}$. З цих бітових блоків формується інформаційне повідомлення $M = \{b_0, b_1, ..., b_{n-1}\}$, $b_i \in \{0,1\}$. Якщо $k < n/m$, тоді останній блок «обрізається» – його останні $km - n$ біт не несуть інформаційного значення.

Недоліком даного методу є незначний обсяг розміру прихованої інформації, який залежить від кількості покриваючих файлів та розміру покриваючих файлів у кластерах. У кожному кластері покриваючих файлів може бути приховано $\log_2 p = m$ інформаційних бітів.

1.2.Приховування інформації через додаткове перемішування кластерів кожного покрівельного файлу

Подальший розвиток розглянутого методу наведено у роботах [30, 31]. Для збільшення обсягу прихованого повідомлення в модифікованому методі запропоновано додаткове перемішування кластерів кожного cover files.

.

Модифікований метод приховування інформації в кластерних файлових системах ґрунтується на використанні одного або декількох покриваючих файлів (cover files) та приховуванні інформаційного повідомлення за шляхом зміни порядку позицій кластерів різних покриваючих файлів та зміні чергування кластерів у межах одного покриваючого файлу. На відміну від описаного методу, даний дозволяє досягти збільшення прихованої інформації на один біт за кожен кластер, при одних і тих значеннях ключових параметрів.

Приховувана інформація подається у вигляді бітового масиву: $M=\{b_0^*,b_1^*,...,b_{L_1+L_2+...+L_{p-1}-1}^*,b_0,b_1,...,b_{n-1}\}$, $b_i^*,b_i\in\{0,1\}$. На інформаційному носії обирають $p=2^m$, $m\in N$ покриваючих файлів (cover files): $F_0,F_1,...,F_{p-1}$. Формується масив номерів кластерів покриваючих файлів як в описаному вище методі. Для кожного покриваючого файлу змінюється порядок чергування кластерів у кожному покриваючому файлі. Порядок чергування задається інформаційною послідовністю M. Для цього, формується p бітових масивів інформаційних бітів:

$$M_1=\{b_0^*,b_1^*,...,b_{L_1-1}^*\},$$
$$M_2=\{b_{L_1}^*,b_{L_1+1}^*,...,b_{L_1+L_2-1}^*\},$$
$$\dots,$$
$$M_{L_p}=\{b_{L_1+L_2+...+L_{p-1}}^*,b_{L_1+L_2+...+L_{p-1}+1}^*,...,b_{L_1+L_2+...+L_{p-1}-1}^*\},$$

кожен з яких зіставляється із масивом номерів кластерів покриваючих файлів

$$C_{F_1}=\{c_{1,0},c_{1,1},...,c_{1,L_1-1}\},$$
$$C_{F_2}=\{c_{2,0},c_{2,1},...,c_{2,L_2-1}\},$$
$$\dots,$$
$$C_{F_p}=\{c_{p,0},c_{p,1},...,c_{p,L_p-1}\}.$$

Позиції кластерів кожного покриваючого файлу перезаписуються, тобто номери кластерів у кожному з масивів C_{F_1}, C_{F_2}, … , C_{F_p} змінюють своє чергування відповідно до значень бітових масивів M_1, M_2, … , M_{L_p}.

У результаті отримують нові масиви номерів кластерів $C_{F_1}^*$, $C_{F_2}^*$, … , $C_{F_p}^*$.

Перезапис позицій кластерів у кожному покриваючому файлі може здійснюватися різними способами. Наприклад, шляхом розбиття всіх номерів позицій кластерів $\{c_{i,0},c_{i,1},...,c_{i,L_i-1}\}$ на дві половини і співставлення кожної половини із значенням інформаційного біту. Тоді, наприклад, якщо $b_j^*=1$, $L_1+L_2+...+L_{i-1}-1<j\le L_1+L_2+...+L_i-1$, на j-у позицію в масиві $C_{F_i}^*$ розміщують кластер з першої половини впорядкованих номерів, якщо $b_0^*=0$ – з другої половини.

Сформовані таким чином масиви $C_{F_i}^*=\{c_{i,0}^*,c_{i,1}^*,...,c_{i,L_i-1}^*\}$ перезаписаних позицій номерів покриваючих файлів утворюють масив

$$C^*=\begin{pmatrix} c_{0,0}^* & c_{0,1}^* & ... & c_{0,L_0-1}^* & & & \\ c_{1,0}^* & c_{1,1}^* & ... & ... & ... & ... & c_{1,L_1-1}^* \\ ... & ... & ... & ... & ... & ... & ... \\ c_{p-1,0}^* & c_{p-1,1}^* & ... & ... & c_{p-1,L_{p-1}-1}^* & & \end{pmatrix}.$$

Зміна порядку чергування кластерів в кожному покриваючому файлі дозволяє приховати перші $L_1+L_2+...+L_{p-1}$ інформаційних бітів з масиву M, тобто інформаційну послідовність $\{b_0^*,b_1^*,...,b_{L_1+L_2+...+L_{p-1}-1}^*\}$. Решту n інформаційних бітів необхідно приховати так само, як і у розглянутому методі [29].

Формується масив D номерів вільних кластерів файлової системи: $D=\{c_1,c_2,...,c_{L_D}\}$, $c_1<c_2<...<c_{L_D}$. Послідовність із інформаційних бітів $\{b_0,b_1,...,b_{n-1}\}$ розбивається на блоки по m бітів кожен: $\{B_1,B_2,...,B_k\}$, кожен блок B_i, $i=1,2,...,k$ подається як натуральне число, тобто $\forall i: 0\le B_i\le p-1$. Кожне натуральне число B_i, $i=1,2,...,k$ подається як номер покриваючого файлу з множини файлів $F_0,F_1,...,F_{p-1}$.

Номери позицій кластерів покриваючих файлів перезаписуються у вільні кластери, тобто масив D заповнюється номерами кластерів з масиву $C*$ (перезаписаними кластерами, тобто із зміненим чергуванням кластерів у кожному покриваючому файлі). Порядок перезапису кластерів покриваючих файлів відповідає послідовності натуральних чисел $\{B_1,B_2,...,B_k\}$, які задаються приховуваним повідомленням. Наприклад, у перший порожній кластер перезаписуються перший кластер покриваючого файлу із номером B_1, у другий порожній кластер – черговий кластер покриваючого файлу із номером B_2 і т.д. Натуральні числа B_i можуть співпадати і в цьому разі записуються чергові кластери того ж самого покриваючого файлу із номером B_i. В результаті перші k вільних кластерів файлової системи будуть записані кластерами покриваючих файлів.

Для вилучення прихованого повідомлення M формується масив D номерів позицій кластерів покриваючих файлів: $D=\{c_1,c_2,...,c_{L_D}\}$. Кожен номер кластеру з цього масиву співвідноситися тільки з одним кластером одного покриваючого файлу. При цьому формується послідовність натуральних чисел $\{B_1,B_2,...,B_k\}$, які відповідають блокам прихованого повідомлення, тобто формується інформаційна послідовність $\{b_0,b_1,...,b_{n-1}\}$, $b_i\in\{0,1\}$.

Далі вилучається інформаційна послідовність $\{b_0^*,b_1^*,...,b^*_{L_1+L_2+...+L_{p-1}-1}\}$, $b_i^*\in\{0,1\}$.

Для цього аналізуємо масиви $C^*_{F_i}=\{c^*_{i,0},c^*_{i,1},...,c^*_{i,L_i-1}\}$ номерів кластерів кожного покриваючого файлу. Правило вилучення інформації відповідає логіці приховування. Наприклад, може застосовуватися розбиття всіх впорядкованих позицій номерів $\{c_{i,0},c_{i,1},...,c_{i,L_i-1}\}$ на дві половини і співставлення кожної половини із значенням інформаційного біту. Тоді, наприклад, якщо на j-й позиції в масиві $C^*_{F_i}$ розміщено кластер з першої половини масиву впорядкованих номерів $\{c_{i,0},c_{i,1},...,c_{i,L_i-1}\}$, приймають бітове значення $b^*_j=1$. Якщо з другої половини – приймають бітове значення $b^*_0=0$.

Таким чином, за рахунок додаткової зміни порядку чергування номерів кластерів у кожному із покриваючих файлів вдається підвищити обсяг прихованої інформації. Зокрема, в порівнянні із способом-прототипом, додатково вдається приховати по одному інформаційному біту на кожен кластер покриваючого файлу.

2. Аналіз відомих технологій зберігання інформації

У даній роботі проаналізовано носії інформації які використовують сучасні технології способу збереження інформації, а саме:

1. SSD (*Solid-State Drive*) – це енергонезалежний немеханічний запам'ятовуючий пристрій на основі мікросхем пам'яті та керуючому контролері;

2. HDD (*Hard (magnetic) Disk Drive*) – це енергонезалежний запам'ятовуючий пристрій оснований на принципі магнітного запису на диск;

3. Flash-USB (*Universal Serial Bus*) – це енергонезалежний запам'ятовуючий пристрій на основі мікросхем, має подібну структуру до SSD накопичувачів, але має менші показники вмістимості та швидкодії, тому здебільшого використовуються для перенесення інформації з пристрою на пристрій, та відокремленого збереження незначної кількості важливої інформації (паролі, ключи доступу, документи).

Так як Flash-USB є технологією подібною до SSD, то переваги й недоліки у даних технології будуть схожі. Але, Flash-USB обмежені максимальним об'ємом зберігаємої інформації, а також інтерфейсом USB (1.5 Мбіт/с – 5 Гбіт/с), що є значно повільнішим за SATA (1.5-6 Гбіт/с) чи M.2 PCIe (8-32 Гбіт/с), через які зазвичай підключають SSD накопичувачі до комп'ютерів. (https://3dnews.ru/623760).

Порівнюючи переваги та недоліки SSD та HDD накопичувачів, можна стверджувати, що SSD мають більше переваг ніж недоліків, зведена інформація наведена у табл. 1. Дані таблиці мають неточний характер через те, що кожен виробник має свої характеристики стосовно пристроїв SSD та HDD. Та одна й та ж технологія навіть у одного виробника може мати різні показники у залежності від цінової категорії пристрою. Головною метою було показати загальну тенденцію та різницю між SSD та HDD накопичувачами.

Таблиця 1

Порівняння основних характеристик SSD та HDD пристроїв

Архітектура накопичувача	SSD	HDD
Рівень шуму	майже відсутній	Значний, так як є рухомі частини
Механічна стійкість	висока	низька, при падінні рухомі частини можуть бути пошкодженні
Енергоспоживання	2-3 Ватт/годину	5-6 Ватт/годину
Магнітна чутливість	майже відсутня	Значна, так як електромагнітне поле безпосередньо впливає на магнітний диск
Розміри	менші розміри та вага	більші розміри через присутність рухомих частин
Паралельні операції	присутні, що значно пришвидшує запис/зчитування декількох файлів	відсутні
Швидкість запису/зчитування (Мб/с)	1000-3200/2000-4000	100-320/200-400
Ціна ($/Гб)	0.5	0.1
Циклів перезапису (разів)	10000	>100000
Вплив фрагментації на роботу	Майже відсутній, швидкість зчитування/запису не залежить від фрагментованості файлу	Значний, так як зчитування виконується однією оптичною головкою

Але з розвитком технологій можна зазначити, що SSD накопичувачі у порівнянні з аналогами п'ятирічної давнини мають значний приріст у показниках, у той час як показники HDD пристроїв майже не змінились.

Якщо ще у 2015 р. кількість HDD пристроїв значно переважала на ринку накопичувачів, то вже у 2020 р. кількість пристроїв HDD та SSD порівнялась. Зведена гістограма наведена на рис. 1.

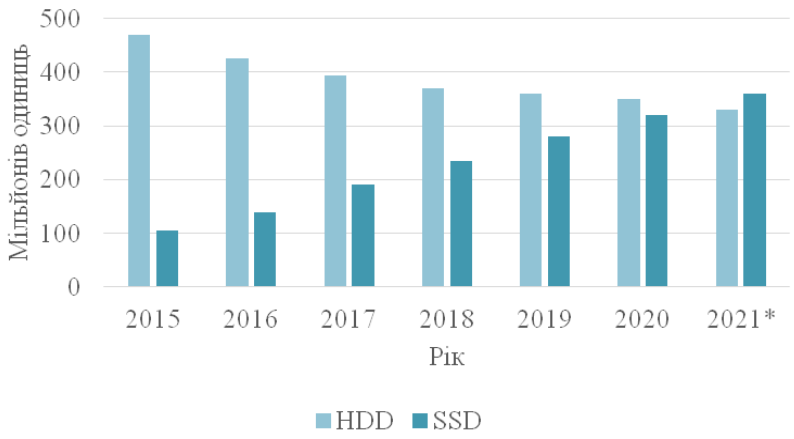


Рис. 1: Реалізація випущеної продукції накопичувачів інформації по всьому світі (у мільйонах одиниць)

Таким чином, можна стверджувати, що з кожним роком кількість SSD накопичувачів росте, забираючи долю ринка у HDD накопичувачів. Динаміка кількості HHD та SSD накопичувачів зазначена на рис. 2.

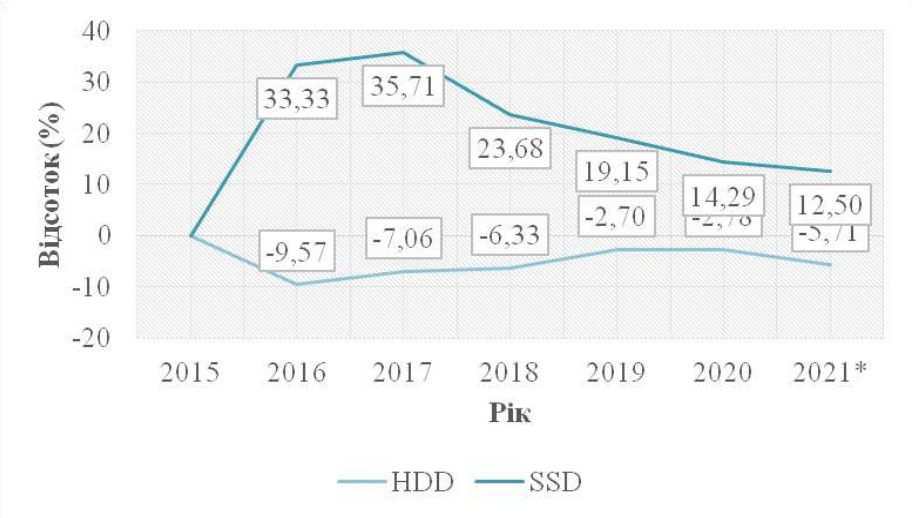


Рис. 2: Динаміка кількості HDD та SDD пристроїв

Для впливу технології накопичувача на можливості методу приховування інформації у структуру файлових систем [31, 33] більш детально оцінимо швидкодію кожної технології. Так як єдиної специфікації по SSD, HDD технологіям не існує, а швидкодія кожного пристрою залежить від виробника та цінової категорії, тож порівняльна оцінка зроблена по результатах електронного ресурсу UserBenchmark (https://www.userbenchmark.com). Даний ресурс збирає дані по компонентах комп'ютера (CPU, GPU, SSD, HDD, RAM, USB), проводячи тестування «opensource» програмним забезпеченням. Дані з UserBenchmark є об'єктивними, так як на ресурсі вказані результати більш ніж 160 мільйонів користувачів.

3. Методика дослідження та результати експериментів

У даній роботі нас цікавлять лише SSD та HDD накопичувачі. Так як для методу приховування інформації [31] важливим є параметр швидкості запису/зчитування з носія інформації, для цього виберемо найкращі пристрої за цими показниками. Для SSD накопичувачів це – Gigabyte GP-ASM2NE6100TTTD Aorus NVMe PCIe M.2 1TB (190$). Для HDD накопичувачів це – WD WD6001FZWX Black 6TB (225$).

Тестування даних пристрої проводилось методами:

1. Послідовного запису (*Sequential*) – це модель доступу до диску, при якій великі блоки даних записуються у сусідні блоки на поверхні пристрою з глибиною черги, що дорівнює одиниці. Даний термін використовується здебільшого у контексті порівняльного аналізу, швидкість вимірюють у МБ/с. Даний тип доступу часто використовують при зчитуванні/записі великих за розміром файлів, таких як відео, музика та зображення. Як демонструє практика, близько 50 % звичайного доступу користувача до диску на ПК буде складатись з послідовних операцій зчитування/запису. Накопичувачі, що в цілому використовуються для великих мультимедійних файлів та/або резервних копій, повинні мати відносно велику швидкість послідовного доступу до файлів;

2. Випадковий запис 4K (*Random 4k*) – це шаблон доступу до диску, при якому невеликі (4k) блоки даних записуються у випадкові місця на поверхні тестованого пристрою з глибиною черги, що дорівнює одиниці. Даний термін використовується здебільшого у контексті порівняльного аналізу, швидкість вимірюють у МБ/с. Даний метод оцінки швидкодії можна використовувати з урахування того, наскільки ефективно пристрій зчитує/записує невеликі фрагменти даних із випадкових місць. Даний шаблон значно розповсюджений під час запуску операційної системи, коли з накопичувача необхідно зчитати велику кількість файлів

конфігурації та драйверів. Як демонструє практика, близько 20 % звичайного доступу користувача до диску на ПК буде складатись з запису/зчитування з випадкових блоків накопичувача.

Результат тестування *Random 4k* є більш важливим для методу приховування інформації шляхом перемішування кластерів у структурі файлової системи, так як при приховуванні даних запис виконується у «випадкові» блоки накопичувача у залежності від приховуваної інформації, що відповідає швидкості доступу до файлу із значним рівнем фрагментації.

Також необхідно зазначити, що модифікований метод приховування даних у структуру файлової системи FAT (який запропоновано у [31]]) дозволяє використовувати 1 покриваючий файл з неперервним ланцюгом кластерів але з певним рівнем переплетеності.

Переплетеність – це властивість файлу, при якій кластери файлу розміщуються неперервно без проміжків між кластерами, але можливий зворотній напрямок у індексації кластерів. Як приклад, переплетений файл – це файл, кластери якого розміщені з 1 по 10 кластери, але ланцюг кластерів може мати вигляд як $Chain_F = [1,9,2,3,10,4,8,7,5,6]$. У загальному вигляді формула рівня переплетеності файлу:

$$Ent_F = \sum_{i=1}^{F_{len}} \left| Chain_F[i] - Chain_F[i+1] \right| - 1, \quad (1)$$

де Ent_F (*entanglement*) – рівень переплетеності файлу F; F_{len} – довжина файлу F у кластерах; $Chain_F[i]$ – i елемент ланцюгу кластерів файлу F.

Таким чином, рівень переплетеності файлу у попередньому прикладі

$$Ent_F = (|1-9|-1) + (|9-2|-1) + \ldots + (|5-6|-1) = 28.$$

Оскільки у даній роботі проаналізовано фізичні властивості носіїв інформації, то можна прирівняти вплив фрагментованості файлу до впливу переплетеності файлу на швидкість запису/зчитування. Адже що фрагментованість, що переплетеність так само змушує далі зміщувати головку зчитуючого пристрою (для HDD технології) для доступу до наступного кластеру.

Зведені результати тестувань пристроїв наведені у табл. 2 та 3.

Таблиця 2

Зведені результати швидкодії SSD та HDD пристроїв
за результатами UserBenchmark методом Sequential

Т	SSD (МБ/с)			HDD (МБ/с)		
Мт	Sequential			Sequential		
	Min.	Avg.	Max.	Min.	Avg.	Max.
R	809	1950	2318	102	167	215
W	1705	3115	3783	138	202	246
M	704	1998	2315	67.5	102	215

Таблиця 3

Зведені результати швидкодії SSD та HDD пристроїв
за результатами UserBenchmark методом Random 4k

Т	SSD (МБ/с)			HDD (МБ/с)		
Мт	Random 4k			Random 4k		
	Min.	Avg.		Min.	Avg.	
R	33	49.5	R	33	49.5	R
W	103	176	W	103	176	W
M	50.7	78.2	M	50.7	78.2	M

Примітка: Т – технологія пристрою; Мт – метод оцінювання; R (read) – швидкість зчитування даних; W (write) – швидкість запису даних; M (mixed) – швидкість почергового зчитування/запису даних.

Таким чином, якщо порівнювати швидкості накопичувачів, то безпосередньо SSD є більш швидким, у абсолютних значеннях. Якщо порівнювати спад швидкості Random 4k та Sequential, то SSD при фрагментованому записі має швидкість у 5 – 10 % у той час як HDD втрачають свою швидкість до 1,5 – 3 %. Звісно 5 – 10 % це мало, але значно краще ніж у HDD. Наведемо вплив фрагментованості носія на швидкість доступу до файлу. Для цього проаналізуємо середній час запису та читання даних з диску з фрагментацією та без.

Середній час читання з диска це час у секундах, який у середньому необхідний на одну операцію читання даних з носія інформації, результати вказані на рис. 3 (https://club.directum.ru/post/140).

Рис. 3: Середній час зчитування даних з диску при фрагментації та без фрагментації

Результати наведені у табл. 4.

Таблиця 4

Оцінка затраченого часу при читанні даних з диску

Операція	Мінімальне значення (с)	Середнє значення (с)	Максимальне значення (с)
З фрагментацією	0	0.23	0.5
Без фрагментації	0	0.08	0.26

Також проаналізуємо середній час запису на диск. Так само, оцінюючи час при фрагментованості та без фрагментованості. Результати показані на рис. 4 та в табл. 5. (https://club.directum.ru/post/140).

Порівнюючи результати обробки даних з фрагментацією та без фрагментації можна стверджувати, що обробка даних без фрагментації ефективніша на 40 – 60 %, ніж обробка фрагментованих даних. Але використання SSD здатне зменшити негативний вплив фрагментованості даних на швидкість обробки цих даних (https://club.directum.ru/post/140).

Виходячи з результатів методів *Random 4k* та *Sequential*, можна стверджувати, що чим більший рівень фрагментації, тим менша швидкість доступу до файлу. Особливо це впливає на швидкодію HDD накопичувачів, у той час як SSD накопичувачі дозволяють проводити запис/зчитування файлиа майже без втрати швидкості, навіть при значному рівні фрагментованості.

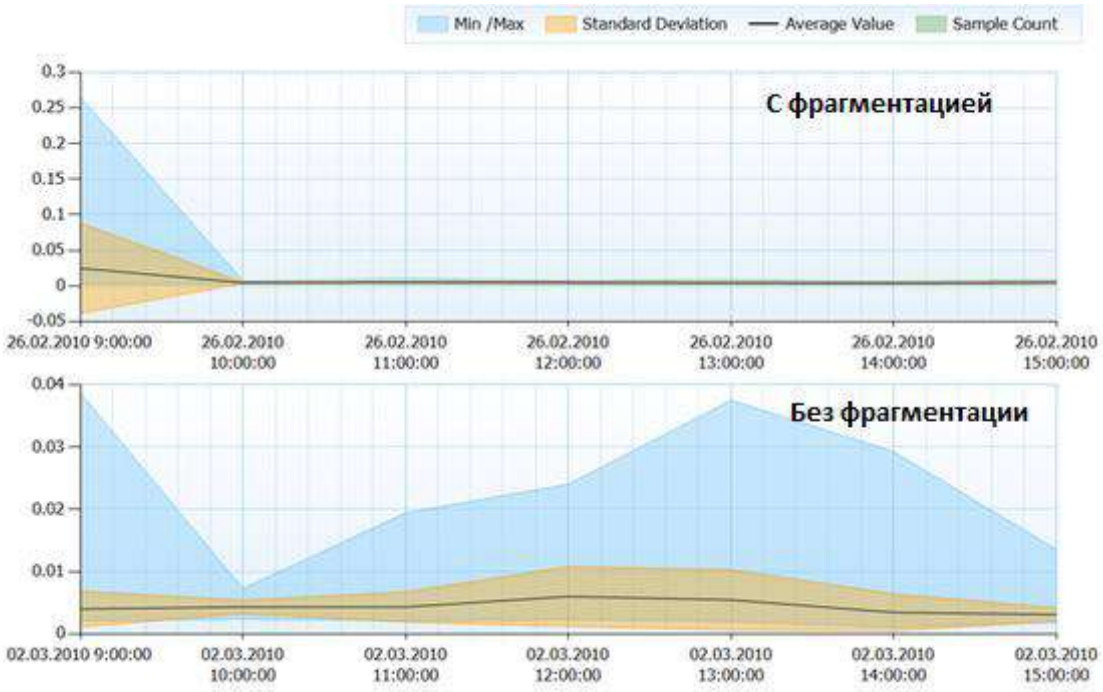


Рис. 4. Середній час запису даних на диску при фрагментації на без фрагментації

Таблиця 5

Оцінка затраченого часу при запису даних на диск

Операція	Мінімальне значення (с)	Середнє значення (с)
З фрагментацією	0,001787	0,007211
Без фрагментації	0,001044	0,004368

Висновки та рекомендації

Отже, можна стверджувати, що технологія SSD має значні переваги, завдяки чому накопичувачі з даною технологією стають більш розповсюдженими. SSD має у рази більшу швидкість доступу до файлів/секторів, навіть при значному показнику фрагментованості – це сприятливий показник для використання стеганографічних методів приховування даних. Також SSD має обмежену кількість циклів перезапису, і хоча це й недолік, але для методу приховування даних цей показник сприятливий, адже виконання дефрагментації є небажаною операцією для SSD.

Отже як висновок можна рекомендувати використання SSD носіїв інформації для приховування повідомлення у структуру файлової системи:

– через те що швидкість доступу до кластеру значно вища, що забезпечить більше швидке виконання стеганографічного методу;

– при збільшенні рівня фрагментованості (переплетеності) швидкість доступу до файлу втрачає не так багато, як у порівнянні з HDD технологією, що є значно важливішим показником при використанні методу приховування даних у структурі файлової системі;

– виконання дефрагментації SSD накопичувачів э небажаною процедурою, що призводить до збільшення загального рівня фрагментованості на носії інформації, що у свою чергу дозволяє приховати більше інформації без ризику розкриття (чим більший рівень фрагментованості на носії, тим більше інформації можна приховати [33]).

Таким чином, завдяки розповсюдженню SSD метод приховування інформації у структуру файлових систем шляхом перемішування кластерів покриваючих файлів є актуальним.

Список літератури:

1. Klima R.E., Klima R., Sigmon N.P., Sigmon N., Klima R., Sigmon N.P., Sigmon N. Cryptology: Classical and Modern. Chapman and Hall/CRC (2018). https://doi.org/10.1201/9781315170664.
2. Delfs H., Knebl H. Introduction to Cryptography. Springer Berlin Heidelberg. Berlin, Heidelberg (2015). https://doi.org/10.1007/978-3-662-47974-2.
3. Childs L.N. Cryptology and Error Correction: An Algebraic Introduction and Real-World Applications. Springer International Publishing, Cham (2019). https://doi.org/10.1007/978-3-030-15453-0.
4. Manoj I.V.S. Cryptography and Steganography // IJCA. 1, 63–68 (2010). https://doi.org/10.5120/257-414.
5. Yahya A. Introduction to Steganography // Yahya A. (ed.) Steganography Techniques for Digital Images. pp. 1–7. Springer International Publishing, Cham (2019). https://doi.org/10.1007/978-3-319-78597-4_1.
6. Qin J., Luo Y., Xiang X., Tan Y., Huang H.: Coverless Image Steganography: A Survey // IEEE Access. 7, 171372–171394 (2019). https://doi.org/10.1109/ACCESS.2019.2955452.
7. Schöttle P., Böhme R. Game Theory and Adaptive Steganography. IEEE Transactions on Information Forensics and Security. 11, 760–773 (2016). https://doi.org/10.1109/TIFS.2015.2509941.
8. Yahya A. Steganography Techniques // Yahya, A. (ed.) Steganography Techniques for Digital Images. pp. 9–42. Springer International Publishing, Cham (2019). https://doi.org/10.1007/978-3-319-78597-4_2.
9. Fridrich J. Steganography in Digital Media: Principles, Algorithms, and Applications. Cambridge University Press, Cambridge; New York (2009).
10. Cox I., Miller M., Bloom J., Fridrich J., Kalker T. Digital Watermarking and Steganography. 2nd Ed. Morgan Kaufmann, Amsterdam, Boston (2007).
11. Kim C.R., Lee S.H., Lee J.H., Park J.-I. Blind decoding of image steganography using entropy model // Electronics Letters. 54, 626–628 (2018). https://doi.org/10.1049/el.2017.4276.
12. Rowland C.H. Covert channels in the TCP/IP protocol suite, https://firstmonday.org/ojs/index.php/fm/article/download/528/449?inline=1, last accessed 2020/11/08.
13. Mazurczyk W., Lubacz J. LACK – a VoIP steganographic method // Telecommun Syst. 45, 153–163 (2010). https://doi.org/10.1007/s11235-009-9245-y.
14. Lubacz J., Mazurczyk W., Szczypiorski K. Principles and Overview of Network Steganography // IEEE Communications Magazine. 52, (2012). https://doi.org/10.1109/MCOM.2014.6815916.
15. Mazurczyk W., Smolarczyk M., Szczypiorski K. On information hiding in retransmissions // Telecommun Syst. 52, 1113–1121 (2013). https://doi.org/10.1007/s11235-011-9617-y.
16. Cauich E., Gómez Cárdenas R., Watanabe R. Data Hiding in Identification and Offset IP Fields // Ramos, F.F., Larios Rosillo, V., and Unger, H. (eds.) Advanced Distributed Systems. pp. 118–125. Springer, Berlin, Heidelberg (2005). https://doi.org/10.1007/11533962_11.
17. Wang M., Gu W., Ma C. A Multimode Network Steganography for Covert Wireless Communication Based on BitTorrent, https://www.hindawi.com/journals/scn/2020/8848315/, last accessed 2020/11/08. https://doi.org/10.1155/2020/8848315.
18. Seo J.O., Manoharan S., Mahanti A. Network steganography and steganalysis – a concise review // 2016 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT). pp. 368–371 (2016). https://doi.org/10.1109/ICATCCT.2016.7912025.
19. Noskov A. Analysis of Network Protocols: The Ability of Concealing the Information // Computer and Network Security. (2020). https://doi.org/10.5772/intechopen.88098.
20. A High Capacity 3D Steganography Algorithm, https://www.computer.org/csdl/journal/tg/2009/02/ttg2009020274/13rRUwdIOUD, last accessed 2020/11/08. https://doi.org/10.1109/TVCG.2008.94.
21. Paramasivan T., Natarajan V., Gnanasekaran A., Venkatesan V., Anitha R. Pattern based 3D image Steganography. 3D Research. 4, (2014). https://doi.org/10.1007/3DRes.01(2013)1.
22. Chao M.-W., Lin C., Yu C.-W., Lee T.-Y. A high capacity 3D steganography algorithm // IEEE Trans Vis Comput Graph. 15, 274–284 (2009). https://doi.org/10.1109/TVCG.2008.94.
23. Li N., Hu J., Sun R., Wang S., Luo Z. A High-Capacity 3D Steganography Algorithm With Adjustable Distortion // IEEE Access. 5, 24457–24466 (2017). https://doi.org/10.1109/ACCESS.2017.2767072.
24. Thiyagarajan P., Natarajan V., Aghila G., Prasanna Venkatesan V., Anitha R. Pattern based 3D image Steganography. 3D Res. 4, 1 (2014). https://doi.org/10.1007/3DRes.01(2013)1.
25. Kuznetsov A., Stefanovych O., Gorbenko Y., Smirnov O., Krasnobaev V., Kuznetsova K. Information Hiding Using 3D-Printing Technology // 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS). pp. 701–706 (2019). https://doi.org/10.1109/IDAACS.2019.8924352.
26. Kuznetsov A.A., Stefanovych O.O., Prokopovych-Tkachenko D.I., Kuznetsova K.O. 3D STEGANOGRAPHY INFORMATION HIDING. TRE. 78, (2019). https://doi.org/10.1615/TelecomRadEng.v78.i12.30.
27. Khan H., Javed M., Mirza F., Khayam S. Evading Disk Investigation and Forensics using a Cluster-Based Covert Channel. (2012).

28. Khan H., Javed M., Khayam S.A., Mirza F. Designing a cluster-based covert channel to evade disk investigation and forensics. Computers & Security. 30, 35–49 (2011). https://doi.org/10.1016/j.cose.2010.10.005.
29. Venčkauskas A., Morkevicius N., Petraitis G., Ceponis J. Covert Channel for Cluster-based File Systems Using Multiple Cover Files // Information technology and control. 42, (2013). https://doi.org/10.5755/j01.itc.42.3.3328.
30. Kuznetsov A., Shekhanin K., Kolhatin A., Mikheev I., Belozertsev I. Hiding data in the structure of the FAT family file system // 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT). pp. 337–342 (2018). https://doi.org/10.1109/DESSERT.2018.8409155.
31. Shekhanin K.Y., Kolhatin A.O., Demenko E.E., Kuznetsov A.A.: ON HIDING DATA INTO THE STRUCTURE OF THE FAT FAMILY FILE SYSTEM. TRE. 78, (2019). https://doi.org/10.1615/TelecomRadEng.v78.i11.50.
32. Vokorokos L., Madoš B., Ádám N., Baláž A., Porubän J., Chovancová E. Multi-Carrier Steganographic Algorithm Using File Fragmentation of FAT FS. COMPUTING AND INFORMATICS. 38, 343-366–366 (2019).
33. Shekhanin K., Kuznetsov A., Krasnobayev V., Smirnov O. Detecting Hidden Information // FAT. IJCNIS. 12, 33–43 (2020). https://doi.org/10.5815/ijcnis.2020.03.04.
34. Aycock J., de Castro D.M.N. Permutation Steganography in FAT Filesystems // Shi, Y.Q. (ed.) Transactions on Data Hiding and Multimedia Security X. pp. 92–105. Springer, Berlin, Heidelberg (2015). https://doi.org/10.1007/978-3-662-46739-8_6.
35. Davis J., MacLean J., Dampier D. Methods of Information Hiding and Detection in File Systems. (2010). https://doi.org/10.1109/SADFE.2010.17.
36. Neuner S., Voyiatzis A.G., Schmiedecker M., Brunthaler S., Katzenbeisser S., Weippl E.R. Time is on my side: Steganography in filesystem metadata // Digital Investigation. 18, S76–S86 (2016). https://doi.org/10.1016/j.diin.2016.04.010.
37. FAT File System, https://www.keil.com/pack/doc/mw/FileSystem/html/fat_fs.html, last accessed 2020/11/08.
38. FAT File Systems. FAT32, FAT16, FAT12 – NTFS.com, https://www.ntfs.com/fat_systems.htm, last accessed 2020/11/08.
39. Overview of FAT, HPFS, and NTFS File Systems, https://support.microsoft.com/en-us/help/100108/overview-of-fat-hpfs-and-ntfs-file-systems, last accessed 2020/11/08.

Надійшла до редколегії 05.11.2020

Відомості про авторів:

Шеханін Кирил Юрійович – аспірант кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук, Харківський національний університет імені В.Н. Каразіна, Україна; e-mail: kyryl.shekhanin@nure.ua, ORCID: https://orcid.org/0000-0002-1441-7814

Горбенко Юрій Іванович – канд. техн. наук, перший заступник головного конструктора, АТ «Інститут інформаційних технологій», Україна; e-mail: gorbenkou@iit.kharkov.ua, ORCID: https://orcid.org/0000-0003-0073-9107

Горбачева Людмила Олегівна – студентка кафедри моделювання систем і технологій, факультет комп'ютерних наук, Харківський національний університет імені В.Н. Каразіна, Україна; e-mail: lusyag23@gmail.com, ORCID: https://orcid.org/0000-0002-6053-7235

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

УДК 004.056.52 **DOI:10.30837/rt.2020.4.203.11**

В.О. ПОДДУБНИЙ, О.В. СЄВЄРІНОВ, канд. техн. наук

МЕНЕДЖМЕНТ ВРАЗЛИВОСТЕЙ З ВИКОРИСТАННЯМ ФОРМАЛІЗОВАНОГО ОПИСУ

Вступ

Захист інформації в інформаційно-телекомунікаційних системах (далі – ІТС) під час її функціонування потребує не тільки дотримання політики безпеки, здійснення організаційних заходів чи технічного обслуговування засобів захисту, але й ефективного менеджменту, моніторингу, контролю та оцінки ризиків інформаційної безпеки (далі – ІБ). Однією із складових ефективного менеджменту ІБ в ІТС є правильне реагування на вразливості. Адже жодний розробник не може гарантувати, що в його продукті відсутні вразливості, які в свою чергу можуть призвести до негативних наслідків (від сповільнення роботи продукту до його ураження зловмисником та взяття під адміністративний контроль). Для покращення роботи ІТС необхідно відповідним чином здійснювати менеджмент вразливостей в системі, який включає систему оцінки ризиків та прийняття рішень. Тому проблема оцінки ризиків при виявленні вразливостей та правильного реагування є досить актуальною та потребує детального дослідження.

Проблеми, що виникають під час процесу керування вразливостями

Якщо розбирати основні етапи керування вразливостями в ІТС, то це будуть наступні дії [1]:

– підготовка;
– сканування на наявність вразливостей;
– визначення дій щодо виправлення;
– здійснення виправлення;
– повторне сканування.

Схематично ці етапи зображено на рис. 1.

Рис. 1. Схема менеджменту вразливостями

Якщо сканування можливо автоматизувати (за допомогою спеціального програмного забезпечення), то етап визначення та прийняття дій майже цілком залежить від адміністратора

безпеки та аудиту. Адміністратор повинен здійснити оцінку ризику та відреагувати відповідним чином (оновлення, відкат, мінімізація роботи процесу, здійснення налаштувань тощо). Незважаючи на наявність систем оцінки вразливостей (таких як CVSS), які надають якісну оцінку серйозності певної вразливості, вплив і поводження окремої вразливості різний для кожної інформаційної системи, так як такі системи оцінки не враховують безліч факторів (структуру і склад інформаційної системи, критичність ресурсів, взаємозв'язки процесів). Тобто вся система стає залежною виключно від досвіду та знань адміністратора. Ця проблема становиться більш гострою в складних системах, з великою кількістю компонентів, які взаємодіють між собою, адже в такій системі складно прослідкувати вплив вразливості. Під час зміни персоналу ІТС стає найбільш вразливою, оскільки новому адміністратору потрібний час для опанування принципів роботи ІТС.

В даний час існує низка міжнародних стандартів серії ISO/IEC 27035 [2] (який є гармонізованим стандартом в Україні [3]), які можуть допомогти в прийнятті рішень. Проте серія ISO/IEC 27035 є загальним зводом практик, а не конкретною інструкцією щодо визначень ризиків чи дій адміністратору. Міжнародний стандарт ISO/IEC 27005 [4] забезпечує рекомендації для управління ризиків ІБ в організації, особливо підтримуючи вимоги СУІБ (ISMS) згідно ISO/IEC 27001 [5]. Однак цей міжнародний стандарт не забезпечує певної методології для управління ризиків ІБ[6].

Тому на даний момент необхідна така система оцінювання ризиків, яка:

– відслідковуватиме вплив вразливості на компоненти системи;

– забезпечуватиме відтворюваність результатів;

– буде ефективною для складних систем;

– повинна бути зрозумілою та гнучкою у використанні.

Така система не виключить вплив адміністратора безпеки та аудиту, проте допоможе йому в прийнятті рішень, оцінці ризиків, зменшить вірогідність помилок, допоможе новому персоналу під час вибору рішень.

Неформалізований та формалізований опис ІТС

Під час опису інформаційної системи та системи захисту інформації зазвичай використовують неформалізований опис, тому, на перший погляд, створювана система оцінювання та прийняття рішень повинна також бути неформалізованою, але це не найкращий варіант, адже неформалізований опис створює безліч проблем, а саме: складність розуміння системи новим персоналом, громіздкість опису систем, відсутність єдиного структурованого опису, погіршення опису взаємозв’язків процесів, знецінення важливої інформації, погану гнучкість.

Відсутність структурованого опису походить від того, що при неформалізованому описі системи розробник не має чітких вимог до структури та форми опису системи, тому зазвичай розробники ІТС під час опису керуються власними нормами або узгоджують їх з клієнтом. Тому опис різних ІТС може відрізнятися якщо вони були створені різними розробниками, навіть якщо ці системи створені однією фірмою, то вони можуть відрізнятися в залежності від типу ІТС, замовника, працівників, що займалися розробкою.

Громіздкість опису системи походить від того, що вся інформація при неформалізованому описі зазвичай подається у вигляді тексту та відсутності структурованого опису. Чим більша система, чим більше процесів та об’єктів, тим більший опис з’являється на виході. Ситуація погіршується, якщо описувана система має обширні або специфічні зв’язки між об’єктами.

Гнучкість опису системи проявляється при її модернізації. Під час модернізації неформалізованого опису необхідне редагування безлічі частин опису, які можуть бути пов’язані або залежати одна від одної. Тому внесення навіть мінімальних правок в систему призводить до перегляду всього опису в цілому, не кажучи вже про додавання або виключення компонентів системи.

Під час такого опису погіршується відображення взаємозв'язків процесів, адже чим довше та складніше дерево об'єктів або процесів, тим складніше його описати та тим більше буде опис системи. Також під час такого опису неможливо чітко дати оцінку впливу вразливості в одному об'єкті ІТС на інший, оскільки не існує метрик, формул та правил взаємодії. Ці правила встановлюються емпіричним методом на базі знань адміністратора.

З цих проблем виникає складність розуміння новим персоналом специфіки роботи системи. Такому персоналу слід обробити безліч інформації в текстовому представленні, яка структурно може відрізнятися від тієї з якою персонал працював раніше.

Під час такої обробки складно виділяти та концентрувати увагу, відслідковувати взаємозв'язки процесів та об'єктів, структурно та логічно класифікувати її, тому можливе погіршення обробки інформації та її знецінення.

Ці проблеми переходять на створювану систему оцінки вразливостей та посилюються там. Така система буде нечіткою, вузькоспеціалізованою, не враховуватиме всіх взаємозв'язків процесів та матиме вигляд зводу практик (аналогічно ISO/IEC 27035). Такі практики не надають методів обчислення ризиків чи впливу вразливості на різні компоненти ІТС. Весь тягар оцінки впливу вразливостей, оцінки ризику, прийняття рішень, покладено на адміністратора безпеки. При різних адміністраторах одна і та ж ситуація може трактуватися порізному, відповідно і рішення будуть прийняті різні в залежності від досвіду, темпераменту адміністратора. В додаток до цих проблем неформалізований опис не може гарантувати рівень гарантій вище ніж Г-2 [7]. Для рівнів Г-3, Г-4, Г-5 стиль опису ІТС повинен бути частково-формалізований, для Г-6 та Г-3 – формалізований.

На відміну від неформалізованого опису системи формалізований має чітку структуру та форму опису, відображає взаємозв'язки процесів, є гнучким та універсальним. В такій системі вплив вразливості легко відслідкувати від точки контакту до всіх об'єктів інформаційної системи. Формалізація дає змогу виявити загальну структуру системи, сформулювати на цій основі загальні закони і правила, за якими відбувається визначення впливу вразливостей на ІТС. Така система зводить до мінімуму вплив адміністратора безпеки, покладаючи оцінку впливу та ризиків на чіткі та закріплені методики, забезпечуючи однозначність та відтворюваність результатів. Тому розроблена система оцінювання ризиків повинна бути формалізованою та побудованою над формалізованим описом ІТС.

Суміщення формалізованого опису та менеджменту вразливостями

Варіантом формалізованого опису ІТС може бути опис послуг безпеки в ІТС. Під час такого опису об'єкти та процеси інформаційної системи представляються в описі зі сторони послуг безпеки, які вони надають або обробляють. Ці послуги передаються від об'єкта до об'єкта, посилюються або взаємодіють з ними. Під час такої реалізації, вразливості будуть розцінюватися як небезпека для конкретної послуги безпеки.

Суміщення формалізованого опису та менеджменту вразливостей допоможе виявляти слабкі місця в ІТС, відслідковувати вплив окремої вразливості на компоненти, масштабувати вразливості, відслідковувати їх взаємозв'язок. При додаванні якісного оцінювання вразливостей можливе створення методик та інструкцій щодо оцінки ризиків. Такі методики можуть надати числову оцінку загрози як системи в цілому, її окремим компонентам, а оцінка ризиків допоможе адміністратору в виборі дій. Так як значення ризику мають числове представлення, то можливе створення чітких інструкцій щодо дій адміністратору. Також така система буде досить гнучкою і універсальною, адже будуватиметься над структурованим описом системи.

Якісне оцінювання вразливостей

Для якісного оцінювання впливу окремої вразливості на конкретний об'єкт доцільно використовувати системи оцінки вразливостей. Однією з таких систем є Common Vulnerability Scoring System (CVSS). CVSS фіксує основні технічні характеристики програмних, технічних та програмно-технічних вразливостей. Її результати включають числові показники, що вказують на серйозність вразливості відносно інших вразливостей.

CVSS складається з трьох основних метричних груп, це: базова (Base), часова (Temporal), та метрика середовища (Environmental)

Базовий показник відображає ступені якості вразливості відповідно до її внутрішніх характеристик, які є постійними в часі і передбачає найгірший вплив у різних розгорнутих середовищах (її вплив на конфіденційність, доступність та цілісність).

Часові метрики регулюють Базову групу вразливості на основі факторів, які змінюються з часом, наприклад наявності експлойтів, які використовують дану вразливість.

Показники середовища змінюють базові та часові метрики для конкретного обчислювального середовища. Вони розглядають такі фактори, як наявність пом'якшення наслідків у цьому середовищі.

Базові оцінки, зазвичай, виробляються організацією, що підтримує продукт з вразливістю, або третьою стороною від її імені. Базові метрики не змінюються з часом і є загальними для всіх середовищ

Споживачі CVSS повинні доповнити базовий показник, тимчасовими та показниками середовища, характерними для використання вразливого продукту, щоб створити точнішу оцінку для їх середовища.

Споживачі можуть використовувати інформацію CVSS як вклад у процес управління організаційною вразливістю, який також враховує фактори, які не є частиною CVSS, щоб класифікувати загрози для їх технологічної інфраструктури та приймати обґрунтовані рішення щодо виправлення.

Такими факторами можуть бути: кількість клієнтів на товарній лінійці, грошові втрати через порушення, загроза життю чи майну, або громадські настрої щодо вразливих місць. Вони виходять за рамки CVSS.

До переваг CVSS можна віднести стандартизовану методологію оцінювання вразливості для постачальників та платформ. Це відкрита структура, що забезпечує прозорість індивідуальних характеристик та методології, яка використовується для отримання оцінки [8].

CVSS є досить розповсюдженою системою, тому існує безліч баз даних, які надають доступ до оцінок вразливостей, які постійно оновлюються, таким чином, вона якнайкраще підходить для якісного оцінювання вразливостей. Однією із таких баз є National Vulnerability Database (NVD) інформаційна база даних національного органу стандартизації США, Національного інституту стандартів і технології [9]. Така база надає доступ до опису всіх виявлених вразливостей, включно з оцінкою CVSS (рис. 2).

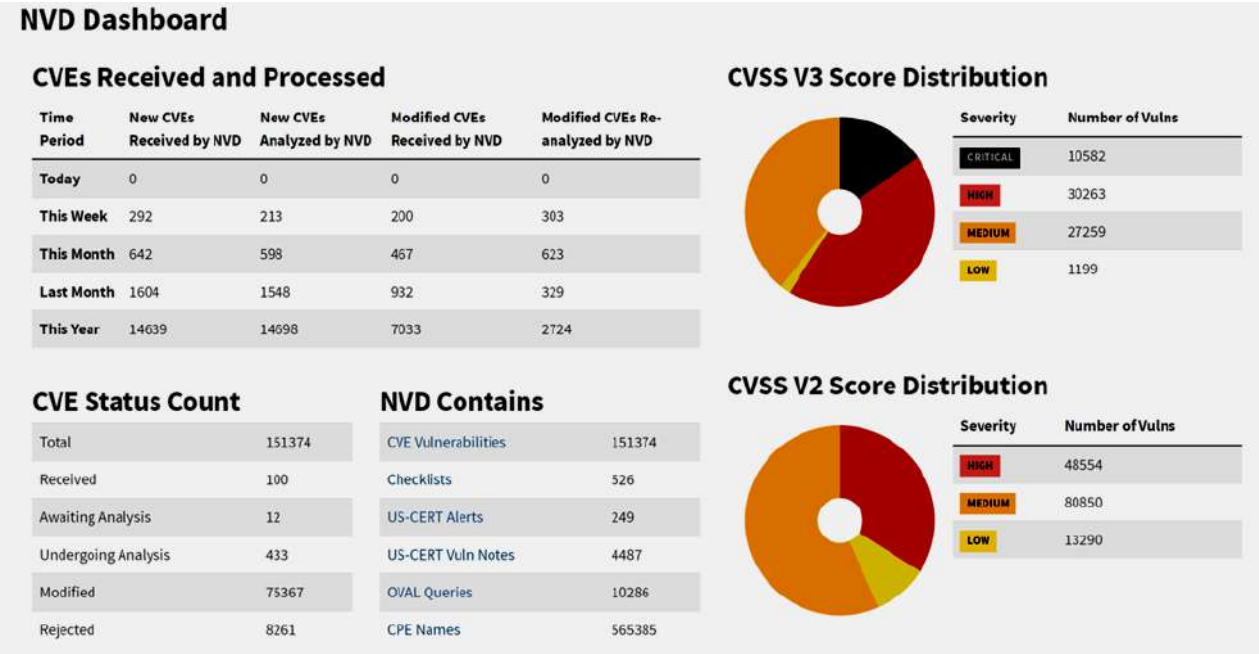


Рис. 2. Загальна інформація з бази даних NVD

Висновок

Отже, для розроблення ефективної системи керування вразливостей необхідно використовувати формалізований опис системи та систему оцінки вразливостей, на базі яких можливо формування методик, інструкцій та правил оцінки ризику. Ця система повинна бути побудована на базі формалізованого опису ІТС, так як такий опис має цілу низку переваг. Як варіантом це може бути опис послуг безпеки в ІТС. Така система буде відповідати всім сучасним вимогам, буде гнучкою, однозначною, простішою у використанні, дозволить відслідковувати вплив вразливості на всі компоненти ІТС. Також для неї легко створювати методики оцінювання ризиків для всієї системи в цілому, такі методики можуть бути модифіковані для більш точного налаштування та будуть являтися чіткими інструкціями щодо дій адміністратору. Додатковою перевагою такої системи є можливість автоматизації процесів оцінки та прийняття рішень (можливість створення ПЗ, яке на вході матиме опис системи та базу вразливостей, а на виході – оцінку ризику для кожного компоненту та процесу ІТС). Також така система може бути частиною "Матриці СУІБ" та допомогти при модернізації системи захисту інформації [10].

Список літератури:

1. Tom Palmaers, Dennis Distler, Implementing a Vulnerability Management Process // SANS Institute Information Security Reading Room, 2013. 24 с.
2. ISO/IEC 27035:2016. Information technology – Security techniques – Information security incident management, 2016. (Міжнародний стандарт)
3. Про прийняття національних стандартів, про прийняття поправок до національних стандартів: затв. Національним Органом Стандартизації від 10 грудня 2018 р. №470
4 ISO/IEC 27005 Information technology – Security techniques – Information security risk management, 2018. (Міжнародний стандарт)
5 ISO/IEC 27001 Information technology – Security techniques – Information security management systems – Requirements, 2013. (Міжнародний стандарт)
6. Сєвєрінов О. В., Черниш В. І., Молчанова М. Є. Управління інформаційною безпекою згідно міжнародних стандартів //Системи управління, навігації та зв'язку. Вип. 2011. Т. 4. С. 250-253.
7. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Київ : Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, 1999. 61с.
8. Common Vulnerability Scoring System version 3.1: Specification Document [Електронний ресурс] Режим доступу: https://www.first.org/cvss/specification-document
9. National Vulnerability Database [Електронний ресурс] Режим доступу: https://nvd.nist.gov
10. Замула А. А., Северинов А. В., Корниенко М. А. Анализ моделей оценки рисков информационной безопасности для построения системы защиты информации // Наука і техніка Повітряних Сил Збройних Сил України. 2014. №. 2. С. 133-138.

Надійшла до редколегії 03.11.2020

Відомості про авторів:

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

Поддубний Вадим Олександрович –магістрант, кафедра безпеки інформаційних технологій, факультет комп'ютерної інженерії та управління, Харківський національний університет радіоелектроніки, Україна; e-mail: vadym.poddubnyi@nure.ua

МЕТОДИ СИНТЕЗУ ТА АНАЛІЗУ СИГНАЛІВ

УДК 621.391 **DOI:10.30837/rt.2020.4.203.12**

І.Д. ГОРБЕНКО, д-р техн. наук, О.А. ЗАМУЛА, д-р техн. наук, ХО ЧІ ЛИК

МЕТОДИ СИНТЕЗУ І ФОРМУВАННЯ СИСТЕМ НЕЛІНІЙНИХ ДИСКРЕТНИХ СИГНАЛІВ ДЛЯ СУЧАСНИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ

Вступ

Один з основних напрямків розвитку сучасних інформаційно-комунікаційних систем (ІКС) базується на розробці і впровадженні методів багатостанційного доступу із застосуванням кодового розподілення шумоподібних складних сигналів (ШСС), які належать абонентам. Їх застосування дозволяє забезпечити високоефективне використання смуги частот, високу завадостійкість прийому сигналів, скритність, конфіденційність і імітозахищеність передавання даних при впливі сукупності різноманітних завад та наявності завмирань у радіоканалах, які обумовлені як умовами розповсюдження сигналів, так і багатопроміневістю каналів зв'язку. Основними задачами, які необхідно вирішувати при реалізації зазначеного напрямку, є синтез класів ШСС у залежності від умов функціонування і призначення ІКС, а також ефективних алгоритмів обробки ШСС на фоні сукупності структурних широкосмугових та вузькосмугових завад.

Процес вибору раціональних по тих чи інших критеріях структур складних сигналів тотожний синтезу відповідних маніпулюючих дискретних послідовностей (ДП). Як критерії вибору класу дискретних сигналів (ДС), як правило, орієнтуються на критерій мінімуму взаємних перешкод (мінімаксний критерій). Застосовувані в ІКС широкосмугові сигнали повинні володіти такими кореляційними властивостями, коли бічні піки кореляційних функцій (КФ) ШСС є якомога меншими, тобто в ідеальному випадку повинні прагнути до нуля [1 – 2]. Використовувані в ІКС методи інформаційного обміну, а також класи ШСС, що застосовуються в якості фізичного переносника даних (множини лінійних рекурентних послідовностей (М-послідовності), Касамі, Голда, Камалєтдінова і ін.), які мають порівняно невеликі значення бічних пелюсток авто- і взаємних КФ, не дозволяють забезпечити необхідні (для відповідних додатків ІКС) показники інформаційної безпеки і завадозахищеності [3].

До ІКС, що створені і функціонують на об'єктах критичної інфраструктури, пред'являються все більш жорсткі вимоги щодо забезпечення ефективності їх функціонування: достовірності і швидкості передачі інформації, живучості, завадозахищеності, інформаційної і кібербезпеки. У таких умовах особливого значення набуває наявність і застосування захищених ІКС. Під захищеністю систем необхідно розуміти, в широкому сенсі, їх здатність забезпечувати необхідні показники з завадозахищеності, імітостійкості, інформаційної, енергетичної і структурної скритності, швидкості передавання інформації, частотної і енергетичної ефективності.

Метод синтезу систем нелінійних дискретних сигналів із застосуванням випадкових (псевдовипадкових) процесів

Дослідження [4 – 5] показали, що дискретні послідовності (ДП) повинні бути засновані на нелінійних правилах побудови і мати покращені кореляційні, ансамблеві і структурні властивості.

Продуктивним кроком, з точки зору нового напряму використання систем складних сигналів у захищених ІКС, є синтез систем нелінійних дискретних сигналів (КС). Такі дискретні сигнали володіють необхідними, але обмеженими (значеннями «щільної упаковки»), кореляційними і ансамблевих властивостями.

Авторами сформульована у загальному вигляді і вирішена задача синтезу нового класу сигналів-фізичних переносників даних для застосування у сучасних ІКС, – нелінійних складних дискретних криптографічних сигналів (КС) [6 – 7]. Крім того, теоретично обґрунтовано [6] комплексне вирішення проблеми забезпечення завадозахищеності та інформаційної безпеки функціонування ІКС на основі реалізації динамічного режиму передачі інформації, при якому відповідність: біт повідомлення – складний сигнал змінюється з плином часу за законом, визначення якого можливо з імовірністю, що не перевищує допустимого в системі значення, і застосування (в якості фізичних переносників даних) сигналів з необхідними кореляційними, ансамблевими, структурними властивостями. При цьому системи сигналів повинні ґрунтуватися на нелінійних правилах побудови. Під криптографічними дискретними сигналами (КС) пропонується розуміти сукупність послідовностей (векторів) символів певного алфавіту, які мають необхідні (задані) структурні, ансамблеві і кореляційні властивості, часову і просторову складності, і існує можливість їх формування на основі криптографічних ключів. Необхідно відзначити особливі властивості систем КС: синтез таких сигналів засновано на використанні випадкових або псевдовипадкові процесів, у тому числі алгоритмів криптографічного перетворення інформації; можливість їх відновлення в просторі і в часі із застосуванням параметрів, які обумовлені принципами їх синтезу, у тому числі ключів, причому довжина ключа може бути істотно менше за період (тривалість) самого сигналу. Подальші дослідження [8] показали, що саме такий спосіб інформаційного обміну і застосування саме КС як фізичних переносників даних забезпечують можливість побудови захищених каналів ІКС, у яких можуть бути реалізовані необхідні значення показників інформаційної безпеки та завадозахищеності в умовах впливу структурних, загороджувальних, ретрансльованих та інших видів перешкод. При такому підході структурна скритність і інформаційна безпека ІКС забезпечуються шляхом застосування (як основи синтезу) випадкових або псевдовипадкових процесів (з використанням криптографічних ключів), і формування, таким чином, ДП, властивості яких близькі до властивостей випадкових послідовностей. Завадостійкість прийому забезпечується необхідними кореляційними властивостями системи сигналів, що синтезується. При використанні таких сигналів, як фізичного переносника інформації або сигналів синхронізації, часові витрати на розкриття структури використовуваних сигналів зростають і постановка «оптимальних», з точки зору станції протидії, перешкод стає проблематичною.

Постановка задачі синтезу нелінійних дискретних криптографічних сигналів (КС)

Під задачею побудування (синтезу) КС будемо розуміти [9] задачу побудови підмножин дискретних послідовностей (W_l^q), $q=\overline{1,N}$, $l=\overline{1,L}$, сукупність яких утворює систему дискретних сигналів заданого алфавіту розмірності $M_k = N \times L$, таких, що в кожній із підмножин (словнику) виконуються умови, що висуваються до підмножини КС в частині структурних, ансамблевих, кореляційних властивостей, просторової та часової складності їх генерування. Правила синтезу КС ґрунтуються на основі використання та аналізу періодичних та аперіодичних функцій кореляції та зводиться до наступних етапів.

1. Побудова КС W^q, періодична функція автокореляції (ПФАК) кожного з яких, задовольняє системі нелінійних параметричних нерівностей (НПН):

$$R_{a_1}^q(l) \le \sum_{i=1}^{L} W_i^q (W_{i+l}^q)^* \le R_{a_2}^q(l),\ l=\overline{1,L-1},\ q=\overline{1,N}, \qquad (1)$$

де $R_{a_1}^q(l)$ і $R_{a_2}^q(l)$ – задані значення реалізації ПФАК, а індекси обчислюються по модулю $(i+1) \bmod L$.

При $1=L$ для усіх $q=\overline{1,N}$ (1) дає згортку зі значенням L:

$$\sum_{i=0}^{L} W_i^q W_i^q = L,\ q=\overline{1,N}. \qquad (2)$$

3. Побудова пар КС W^q та W^p, функції взаємної кореляції (ФВК) яких задовольняють вимогам, що визначаються сукупністю систем НПН (3-7), а також задовольняють вимогам до стикових функцій взаємної кореляції (СФВК) пар КС W^q та W^p зі стиковими дискретними словами W^{qp} і W^{pq}:

$$R_{b_{1,1}}^{qp}(l) \le \sum_{i=0}^{L-K} W_i^q \times (W_{i+l}^p)^* + \sum_{i=L-K+1}^{L-1} W_i^q \times (W_{i-l+K}^p)^* \le R_{b_{2,1}}^{qp}(l); \quad (3)$$

$$R_{b_{1,2}}^{qp}(l) \le \sum_{i=0}^{L-K} W_i^q \times (W_{i+l}^q)^* + \sum_{i=L-K+1}^{L-1} W_i^q \times (W_{i-l+K}^p)^* \le R_{b_{2,2}}^{qp}(l); \quad (4)$$

$$R_{b_{1,3}}^{qp}(l) \le \sum_{i=0}^{L-K} W_i^q \times (W_{i+l}^p)^* + \sum_{i=L-K+1}^{L-1} W_i^q \times (W_{i-l+K}^q)^* \le R_{b_{2,3}}^{qp}(l); \quad (5)$$

$$R_{b_{1,4}}^{qp}(l) \le \sum_{i=0}^{L-K} W_i^p \times (W_{i+l}^p)^* + \sum_{i=L-K+1}^{L-1} W_i^p \times (W_{i-l+K}^q)^* \le R_{b_{2,4}}^{qp}(l); \quad (6)$$

$$R_{b_{1,5}}^{qp}(l) \le \sum_{i=0}^{L-K} W_i^p \times (W_{i+l}^q)^* + \sum_{i=L-K+1}^{L-1} W_i^p \times (W_{i-l+K}^p)^* \le R_{b_{2,5}}^{qp}(l); \quad (7)$$

причому $l=\overline{1,L-1}$ для всіляких поєднань q і p, $q=\overline{1,N}$, $p=\overline{1,N}$, $q \ne p$, де $R_{b_{1,j}}^{qp}(l)$ і $R_{b_{2,j}}^{qp}(l)$, задані (необхідні) реалізації ПФВК і СФВК відповідно, $j=\overline{1,5}$.

Дослідження показали [10], що вказаний клас задач може розв'язуватись при застосуванні методу, який включає такі етапи:

1. Формування дискретних послідовностей з використанням випадкових (псевдовипадкових процесів, у тому числі із використанням алгоритмів криптографічного перетворення інформації).

2. Побудова необхідного числа потенційних КС W^q згідно системи (1).

4. Знаходження пар чи підмножин КС W^q та W^p, які задовольняють вимогам (3) – (7).

5. Побудова матриці станів взаємно-кореляційних функцій всіх можливих пар потенційних КС, які пройшли відбір за результатами попереднього кроку та мають необхідні ансамблеві, кореляційні властивості.

6. Аналіз матриці станів та формування необхідного числа підмножин чи пар КС згідно з (1) – (2) та (3) – (7) та відбір в підмножину лише тих, що задовольняють встановленим вимогам, у тому числі граничним значенням бічних пелюсток функцій кореляції для відповідних значень періоду послідовностей.

Аналіз зазначених кроків показує, що продуктивність синтезу системи КС у ряді випадків не може задовільнити вимоги власників (користувачів) ІКС. Дійсно, загальний час синтезу одного з безлічі КС може бути обчислено за виразом

$$T_{CS} = h \cdot (T_{GEN} + T_{PFAC} + T_{R_{\max}} + T_{IF} + (R_{\max} \le R_{\max}^*) \cdot T_{write}) \ , \quad (8)$$

де: h – кількість спроб вибору КС W^q, який задовольняє умові (1) (етапи 1 - 2 методу);

T_{GEN} – час, необхідний для генерації КС (етап 1 методу);

T_{PFAC} – час, необхідний для обчислення значень ПФАК;

$T_{R_{\max}}$ – час, необхідний для пошуку максимальних значень бокових пелюсток $R_{\max}$ ПФАК;

T_{IF} – час, необхідний для порівняння $R_{\max}$ з встановленим граничним значенням $R_{\max}$ (перевірка вимог (3) – (7) (етап 4 методу));

T_{write} – час, необхідний для запису обраного КС у структуру даних (список, файл та інше).

Останній доданок $R_{\max} \le R^*_{\max}$ приймає значення: якщо цей вислів істинно, то буде 1 помножене на T_{write} (тобто сформований сигнал записується в ту чи іншу структуру даних) і 0 помножене на T_{write} - в іншому випадку (тобто сигнал відкидається і час T_{write} не буде враховано).

Наведемо приклад синтезу множини сигналів з застосуванням наведеного методу.

Приклад: Припустимо для формування одного сигналу нам треба застосувати три спроби, другого сигналу – десять спроб. Тоді, загальний час формування множини сигналів:

$$T_{CS} = \begin{array}{l} 3\cdot(T_{GEN} + T_{PFAC} + T_{R_{\max}} + T_{IF} + (R_{\max} \le R^*_{\max})\cdot T_{write}) + \\ +10\cdot(T_{GEN} + T_{PFAC} + T_{R_{\max}} + T_{IF} + (R_{\max} \le R^*_{\max})\cdot T_{write})\cdot \end{array} \quad (9)$$

Узагальнюючи наведені міркування, можна отримати вираз для розрахунку часу, який є необхідний для синтезу всієї системи КС для визначеного періоду N.

Тобто, вираз для часу формування ансамблю КС із заданими властивостями буде мати наступний вигляд:

$$T_{total} = \sum_{i=1}^{M} T_{CS\,i} \ , \quad (10)$$

де M – об'єм системи сигналів для числа елементів послідовності N.

Метод синтезу систем нелінійних дискретних сигналів із застосуванням операції децимації

Пропонується новий метод синтезу системи КС для визначеного періоду ДП N.

Твердження. Якщо криптографічну послідовність W_i періоду N піддати операції децимації з індексом децимації k, причому k є взаємно простим з N, то результуюча послідовність V_{ik} буде такою ж криптографічною послідовністю, такого ж періоду з властивостями, що є ідентичними властивостям вихідної послідовності W_i.

Операція децимації зводиться до вибору кожного k-го символу послідовності W_i і запису отриманих таким чином елементів послідовності один за одним, так що $W_i = V_{ik}$.

У табл. 1 наведено приклад вихідної послідовності W_i з числом елементів $N = 256$.

Таблиця 1

Signal: [-1, 1, -1, 1, -1, -1, -1, 1, 1, 1, -1, 1, -1, -1, 1, 1, 1, 1, -1, 1, -1, -1, 1, -1, 1, -1, 1, 1, -1, 1, -1, 1, 1, 1, -1, -1, -1, 1, -1, 1, 1, 1, -1, 1, -1, 1, 1, 1, -1, 1, 1, -1, -1, -1, 1, -1, -1, 1, -1, 1, -1, -1, -1, -1, -1, 1, -1, -1, -1, -1, -1, -1, 1, 1, 1, 1, 1, -1, 1, 1, 1, -1, 1, -1, -1, -1, 1, 1, -1, 1, -1, 1, -1, 1, 1, 1, -1, -1, -1, 1, 1, -1, 1, 1, -1, 1, 1, -1, 1, 1, -1, 1, -1, -1, 1, 1, 1, -1, -1, -1, 1, -1, 1, -1, 1, -1, -1, 1, 1, -1, 1, 1, 1, -1, -1, -1, -1, -1, 1, 1, -1, -1, 1, -1, 1, -1, -1, -1, -1, -1, 1, 1, -1, -1, -1, -1, -1, -1, 1, 1, -1, 1, 1, 1, -1, 1, 1, 1, -1, -1, -1, 1, 1, -1, -1, 1, -1, 1, 1, 1, 1, 1, -1, 1, 1, -1, 1, -1, 1, 1, 1, -1, -1, -1, 1, 1, -1, 1, -1, 1, 1, 1, 1, 1, 1, -1, 1, 1, 1, 1, 1, 1, -1, -1, -1, -1, 1, 1, 1, -1, 1, 1, 1, 1, 1, -1, -1, 1, -1, 1, 1, 1, -1, 1, -1, 1, 1, 1, -1, 1, -1, 1]

У табл. 2 – 3 наведено приклади реалізації процедури децимації послідовності G_i з числом елементів $N = 256$ за індексами децимації $k = 3$ і $k = 5$ відповідно.

Таблиця 2

0) [1, -1, 1, -1, 1, -1, -1, -1, -1, 1, 1, 1, -1, -1, 1, -1, -1, 1, 1, 1, -1, -1, 1, 1, 1, -1, -1, -1, -1, 1, 1, -1, 1, 1, 1, -1, 1, -1, 1, -1, 1, 1, 1, -1, 1, 1, 1, 1, 1, -1, -1, 1, -1, -1, -1, 1, -1, -1, 1, -1, -1, 1, 1, -1, 1, 1, -1, 1, -1, 1, -1, -1, -1, 1, 1, -1, -1, 1, 1, 1, 1, 1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, 1, -1, 1, -1, -1, -1, 1, -1, 1, -1, 1, -1, 1, -1, 1, 1, -1, 1, -1, 1, 1, -1, -1, -1, -1, -1, 1, -1, 1, -1, 1, -1, 1, -1, 1, 1, -1, -1, 1, -1, -1, -1, 1, -1, 1, 1, 1, 1, 1, 1, 1, -1, -1, -1, 1, -1, 1, -1, 1, -1, -1, -1, -1, 1, -1, 1, 1, 1, -1, 1, 1, 1, 1, -1, 1, 1, -1, -1, -1, 1, 1, 1, 1, 1, 1, 1, -1, -1, 1, -1, 1, 1, 1, 1, 1, -1, -1, -1, 1, -1, -1, -1, -1, 1, -1, 1, 1, 1, 1, 1, 1, 1, -1, -1, -1, 1, 1, 1, -1, 1, 1, 1, 1, -1, -1, -1, 1, -1, 1, 1, 1, -1, -1, 1, 1, -1, -1, 1, 1, 1, 1, 1, 1, -1, -1, 1, -1, 1, -1, 1, -1, 1, -1, 1, 1, 1, 1, -1, 1, -1, -1, -1, -1, -1, 1, 1, 1, -1, 1, 1, 1, -1, -1, 1]

Таблиця 3

1) [-1, 1, 1, -1, -1, 1, -1, 1, 1, 1, -1, 1, -1, 1, 1, -1, 1, -1, 1, -1, 1, -1, 1, 1, -1, 1, -1, -1, -1, 1, -1, 1, -1, 1, 1, -1, -1, -1, 1, 1, 1, 1, 1, -1, 1, 1, -1, 1, 1, -1, -1, -1, 1, 1, -1, -1, -1, -1, 1, -1, -1, 1, 1, -1, -1, 1, 1, 1, -1, -1, 1, -1, -1, 1, -1, 1, 1, 1, -1, 1, 1, 1, 1, -1, 1, -1, 1, 1, 1, -1, -1, -1, -1, -1, 1, -1, -1, -1, -1, -1, -1, -1, 1, 1, 1, 1, 1, -1, 1, -1, -1, 1, 1, 1, 1, -1, -1, -1, -1, 1, -1, -1, 1, 1, 1, -1, 1, 1, 1, -1, -1, -1, 1, 1, 1, 1, 1, -1, 1, -1, -1, -1, 1, 1, -1, -1, -1, -1, -1, -1, 1, 1, -1, 1, 1, -1, -1, -1, -1, -1, -1, -1, 1, 1, 1, 1, 1, 1, 1, 1, 1, -1, -1, -1, 1, 1, -1, -1, 1, -1, 1, 1, -1, 1, 1, -1, -1, 1, -1, -1, 1, -1, 1, -1, 1, -1, -1, 1, 1, -1, -1, 1, 1, 1, -1, -1, 1, -1, 1, -1, -1, 1, -1, -1, 1, 1, -1, 1, -1, 1, 1, -1, -1, -1, -1, 1, 1, 1, 1, -1, -1, -1, -1, 1, -1, -1, 1, 1, 1, -1, -1, 1, -1, 1, -1, -1, 1, 1, 1, -1, -1, 1, -1, -1, -1, 1, -1, 1, -1, 1]

Оцінимо час, необхідний для реалізації синтезу системи КС із застосуванням запропонованого методу.

Аналіз операцій, які визначені вищенаведеним твердженням, показує, що час, який необхідно для синтезу одного з множини КС із застосуванням операції децимації, може бути визначено, як

$$T_D = T_{read} + T_{pos} + T_{perm} + T_{write}, \tag{11}$$

де: T_{read} – час, необхідний для зчитування вихідних даних (вихідна послідовність (W_i), індекс децимації);

T_{pos} – час, необхідний для розрахунку позиції за індексом децимації, що використовується;

T_{perm} – час, необхідний для запису елементів вихідної послідовності (W_i) за новими позиціями, які визначені відповідним індексом децимації (k);

T_{write} – час, необхідний для запису сформованої шляхом децимації послідовності (V_{ik}) у структуру даних.

Час, необхідний для формування всієї системи (ансамблю) КС, для числа елементів N, може бути визначено (за умови, що вихідний сигнал (W_i) попереднє сформовано), як

$$T_{total} = T_{coprimes} + \varphi(N) \cdot T_D, \tag{12}$$

де: $\varphi(N)$ – функція Ейлера;

$T_{coprimes}$ – час, необхідний для розрахунку множини чисел, які є взаємно простими з N;

T_D – час, необхідний для реалізації процедури децимації для формування однієї з послідовностей (V_{ik}) за методом децимації.

Якщо попередньо вихідний сигнал (W_i) не сформовано, вираз (12) буде мати вигляд

$$T_{total} = T_{CS} + T_{coprimes} + \varphi(N) \cdot T_D. \tag{13}$$

Програмне моделювання процесу синтезу КС із застосуванням методу, що використовує випадкові (псевдовипадкові) процеси (вирази (1) – (7)) показує, що середній час на синтез ансамблю КС (128 послідовностей) з числом елементів $N = 256$, у середньому складає 60.821875 секунд. Середній час на синтез ансамблю КС (128 послідовностей) з числом елементів $N = 256$, із застосуванням запропонованого методу децимації у середньому складає 0.009375 секунди (за умови, що попередньо вихідний сигнал W_i сформовано). Таким чином, виграш у часі формування системи сигналів із застосуванням методу децимації для наведеного прикладу складає приблизно $6{,}5 \cdot 10^3$. Якщо вихідний сигнал W_i попереднє не сформовано (вираз (13)) виграш у часі формування системи сигналів із застосуванням методу децимації складає більш ніж 10^2.

У табл. 4 наведено розраховані нормовані статистичні характеристики ($\frac{R_{б\max}}{\sqrt{N}}$ – максимальне значення бокових піків кореляційних функцій (КФ); $\frac{m_{|R|}}{\sqrt{N}}$ – математичне очікування модуля бокових піків КФ; $\frac{D_{|R|}}{\sqrt{N}}$ – дисперсія модуля бокових піків КФ; $\frac{D_{|R|}^{1/2}}{\sqrt{N}}$ – середнєквадратичне відхилення модуля бокових піків КФ; $\frac{D_R^{1/2}}{\sqrt{N}}$ – середнєквадратичне відхилення бокових піків КФ; $\frac{\gamma}{\sqrt{N}}$ - коефіцієнт ексцесу) різних КФ для КС (ПФАК, АФАК – періодична і аперіодична функції автокореляції, відповідно; ПФВК, АФВК – періодична і аперіодична функції взаємної кореляції, відповідно).

Таблиця 4

Тип функції кореляції (КФ)	Сигнал	N	$\frac{R_{б\max}}{\sqrt{N}}$	$\frac{m_{\|R\|}}{\sqrt{N}}$	$\frac{D_{\|R\|}}{\sqrt{N}}$	$\frac{D^{1/2}_{\|R\|}}{\sqrt{N}}$	$\frac{D^{1/2}_{R}}{\sqrt{N}}$	$\frac{\gamma}{\sqrt{N}}$
ПФАК	Вихідний сигнал	256	1.996105	0.764257	4.051119	0.502695	0.914000	5.882533
	Сигнали, що отримані методом децимації	256	1.996105	0.762401	4.058512	0.503153	0.914000	5.882533
АФАК	Вихідний сигнал	256	1.996105	0.507131	2.954548	0.429301	0.664171	10.894494
	Сигнали, що отримані методом децимації	256	1.954520	0.505330	2.675348	0.407925	0.649360	11.255518
ПФВК	Вихідний сигнал з іншими ізоморфізмами	256	2.966434	0.807777	6.096691	0.616376	1.015907	0.047603
	Сигнали, що отримані методом децимації	256	2.876332	0.807561	6.147075	0.618564	1.017259	0.049834
АФВК	Вихідний сигнал з іншими ізоморфізмами	256	2.273342	0.535305	3.353158	0.456910	0.703664	0.132458
	Сигнали, що отримані методом децимації	256	2.380771	0.543414	3.555152	0.470007	0.718335	0.126386

Аналіз даних табл. 4 показує, що значення максимальних бокових піків (пелюсток), а також статистичних характеристик різних КФ для КС, що отримані із використанням методу, заснованому на застосуванні випадкових (псевдовипадкових) процесів і методу децимації практично ідентичні.

Висновки

Запропоновано методи синтезу і формування системи сигналів одного класу нелінійних дискретних складних сигналів, а саме, так званих, криптографічних сигналів. Наведено математичну модель синтезу зазначених систем сигналів. Перший метод, що представлено, використовує випадкові (псевдовипадкові) процеси, у тому числі, алгоритми криптографічного

перетворення інформації із застосуванням секретних ключів, і заснований на використанні та проведенні аналізу періодичних та аперіодичних функцій кореляції. Інший метод засновано на реалізації операції децимації вихідної дискретної послідовності символів, яка отримана за результатами реалізації першого методу і забезпечує синтез системи сигналів для визначеної тривалості сигналу. Отримано аналітичні вирази для визначення часу синтезу системи сигналів із застосуванням запропонованих методів. На основі реалізованої програмної моделі показано, що швидкодія методу формування сигналів на основі операції децимації, для визначеної тривалості сигналу, більш ніж на три порядки перевищує швидкодію методу, що засновано на використанні випадкових (псевдовипадкових) процесів. При цьому, на основі проведеного комп'ютерного моделювання показано, що сигнали, які отримані із застосуванням запропонованих методів, володіють ідентичними властивостями (кореляційними, ансамблевими, структурними).

Отримані результати можуть знайти застосування при побудові захищених сучасних інформаційно-комунікаційних систем, до яких висуваються підвищені вимоги до завадостійкості прийому сигналів при впливі різноманітних завад, скритності, конфіденційності, імітозахищеності і швидкості передачі інформації.

Список літератури:

1. Sarvate, D.V. Crosleration Properties of Pseudorandom and Related Sequences / D.V. Sarvate, M.V. Parsley // IEEE Trans. Commun. 1980. Vol. Com 68. P. 59–90.
2. Варакин Л. Е. Системы связи с шумоподобными сигналами. 1985. 384 с.
3. Gorbenko I. D., Zamula A. A., Morozov V. L. Information security and noise immunity of telecommunication systems under conditions of various internal and external impacts // Telecommunications and Radio Engineering Volume 76, 2017 Issue 19, pages 1705-1717 DOI: 10.1615/TelecomRadEng.v76.i19.30.
4. Methods for implementing communications in info-communication systems based on signal structures with specified properties / I. D. Gorbenko, A. A. Zamula, V. L. Morozov // 2017 4th International Scientific-Practical Conference Problems of Info communications Science and Technology, PIC S and T 2017. Proceedings. DOI: 10.1109/INFOCOMMST.2017.8246359.
5. Gorbenko I. D., Zamula A. A., Ho Tri Luk Synthesis of derivatives of complex signals based on nonlinear discrete sequences with improved correlation properties // Радіотехніка. 2019. Вип. 199. С. 110 -120.
6. Gorbenko I. D., Zamula A. A. Cryptographic signals: requirements, methods of synthesis, properties, application in telecommunication systems // Telecommunications and Radio Engineering Volume 76, 2017. Issue 12, pages 1079-1100. DOI: 10.1615/TelecomRadEng.v76.i12.50.
7. Gorbenko I.D., Zamula A.A., Semenko Ye.A. Ensemble and correlation properties of cryptographic sig-nals for telecommunication system and network applications // Telecommunications and Radio Engineering. Vol. 75, 2016 Issue 2. Pages 169-178. DOI: 10.1615/TelecomRadEng.v75.i2.60.
8. Gorbenko I. D., Zamula A. A., Morozov V. L. Information and communication systems based on signal systems with improved properties building concept. Workshop Proceedings 2019 CEUR.
9. Горбенко І.Д., Замула О.А. Моделі та методи синтезу криптографічних сигналів та їх оптимізація за критерієм часової складності // Математичне та комп'ютерне моделювання. Серія: Фіз.-мат. науки : зб. наук. праць / Інститут кібернетики імені В.М. Глушкова Національної академії наук України, 2017. Вип. 15. 272 с.
10. Горбенко І.Д., Замула О.А., Хо Чі Лик Оптимізація пошуку дискретних складних сигналів з необхідними властивостями для застосування у сучасних інформаційно-комунікаційних системах // Математичне та комп'ютерне моделювання. Серія: Техн. науки : зб. наук. праць / Інститут кібернетики імені В.М. Глушкова Національної академії наук України, 2019. Вип. 19. 160 с.

Надійшла до редколегії 17.09.2020

Відомості про авторів:

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

Замула Олександр Андрійович – д-р техн. наук, професор, професор кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук, Харківський національний університет імені В.Н. Каразіна, Україна; email: zamylaaa@gmail.com, ORCID: http://orcid.org/0000-0002-8973-6190

Хо Чі Лик – магістрант кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук, Харківський національний університет імені В.Н. Каразіна,Україна.

УДК 621.391 **DOI:10.30837/rt.2020.4.203.13**

С.Г. РАССОМАХІН, д-р техн. наук, О.А. ЗАМУЛА, д-р техн. наук,
І.Д. ГОРБЕНКО, д-р техн. наук, ХО ЧІ ЛИК

ПОРІВНЯЛЬНИЙ АНАЛІЗ ЗАВАДОСТІЙКОСТІ ПРИЙОМУ НЕЛІНІЙНИХ СКЛАДНИХ ДИСКРЕТНИХ СИГНАЛІВ ЗІ СТАНДАРТНИМИ СИГНАЛАМИ АФМ-16 BPSK

Вступ

Підвищені вимоги до ефективності функціонування інформаційно-комунікаційних систем (ІКС) в умовах внутрішніх і зовнішніх впливів в значній мірі не враховуються існуючими інформаційними технологіями. Має місце суперечність між жорсткими вимогами щодо забезпечення достовірності, скритності, конфіденційності, цілісності даних, що передаються по лініях зв'язку ІКС [1], з одного боку, і існуючими моделями, методами і технологіями управління ІКС, інформаційною безпекою (ІБ), послугами і якістю обслуговування – з іншого боку.

Проектування ІКС багато в чому ґрунтується на знаходженні дискретно-кодованих сигналів (ДКС) з відповідними ансамблевими, кореляційними, структурними, технологічними та іншими властивостями. В якості маніпулюючих (які розширюють спектр) в широкосмугових системах використовуються сигнали з лінійним законом формування. Такі сигнали володіють досить обмеженими ансамблевими характеристиками і мають низьку кодову стійкість проти розкриття законів їх формування (низьку структурну скритність) [2]. Підвищення показників ефективності функціонування ІКС, а саме: завадостійкість прийому сигналів, інформаційна скритність і імітостійкість системи може бути досягнуто за рахунок використання ДКС, які існують для широкого спектру значень періоду сигналу, мають покращені ансамблеві, кореляційні, структурні властивості. Однак лінійні класи сигналів, що застосовуються у сучасних ІКС, мають незадовільні (особливо для систем критичного призначення) кореляційні, спектральні, ансамблеві та структурні властивості, що, в свою чергу, призводить до погіршення зазначених вище показників функціонування ІКС. Основними шляхами вирішення зазначеного протиріччя є підвищення завадозахищеності (зокрема, енергетичної і структурної скритності, завадостійкості прийому сигналів) і ІБ (зокрема, іміто -і криптостійкості) ІКС на основі удосконалення методологічних основ побудови ІКС шляхом створення нових моделей, методів і технологій управління телекомунікаційними мережами, інформаційною безпекою, послугами і якістю обслуговування, розробки методів інформаційного обміну, методів синтезу нових класів складних дискретних сигналів – переносників даних з необхідними ансамблевими, кореляційними і структурними властивостями.

У роботі наведена статистична імітаційна модель для дослідження завадостійкості різних класів сигналів в гауссовому каналі. Для порівняльного аналізу в якості нелінійних дискретних складних сигналів застосовуються характеристичні дискретні сигнали та криптографічні сигнали.

Характеристичні дискретні сигнали: основні властивості, метод синтезу (ХДС)

ХДС – це нелінійні складні дискретні сигнали, синтез яких базується на використанні характеру ψ мультиплікативної групи поля *GF (P)* [3-4]. ХДС існують для числа позицій (період послідовності): $L = 4x+2$ та $L = 4x$. Відомо, що для $L = 4x+2$ ХДС мають дворівневу періодичну функцію автокореляції $R_{\mu} = \{-2, 2\}$; Для $L = 4x$ – $R_{\mu} = \{-4, 0\}$ і $R_{\mu} = \{0, 4\}$ відповідно. Щодо ансамблевих властивостей, ХДС існують для усіх $N = P^n - 1$ (P – просте, а n – ціле число), кількість ізоморфізмів (об'єм системи сигналів): $\varphi(N)$ – функція Ейлера.

Синтез ХДС базується на використанні найменшого за значенням первісного елемента Θ_j поля $GF(P)$ і задається твердженням 1.

Твердження 1 [4]. Нехай характер мультиплікативної групи поля фіксується функцією

$$\psi(a_i) = e^{j\pi U_i}, \tag{1}$$

тоді алгоритм побудови характеристичного сигналу описується наступними кроками:

1) Формується масив елементів-чисел A_i, $i = \overline{0, P-2}$ поля $GF(P)$:

$$A(i) = \Theta_j^i (\mathrm{mod}\, P). \tag{2}$$

2) Формується група чисел поля $GF(P)$, зрушена за значеннями на одиницю, відповідно до правила:

$$\begin{aligned} &H(i) = A(i)+1, \text{ якщо } \Theta_j^i + 1 \neq 0(\mathrm{mod}\, P); \\ &H(i) = 1, \text{ якщо } \Theta_j^i + 1 \equiv 0(\mathrm{mod}\, P). \end{aligned} \tag{3}$$

3) Формується масив індексів $X(i)$, $i = \overline{0, P-2}$, значеннями якого є відповідні елементу поля індекси $i+1$, впорядковані за вмістом за адресом

$$A(i) : X(i) = X[A(i)]. \tag{4}$$

4) Будується масив індексів $J(i)$, значеннями якого є індекси масиву $X(i)$, які вибрані за адресом $H(i) : J(i) = X[H(i)]$, $i = \overline{0, P-2}$.

5) Обчислюється характер поля за правилом [1, 3]:

$$\psi(a_i) = \psi[J(i)] = \begin{cases} 1, \text{ якщо } J(i) \neq 0(\mathrm{mod}\, 2); \\ -1, \text{ якщо } J(i) \equiv 0(\mathrm{mod}\, 2). \end{cases} \tag{5}$$

Для розкриття закону формування ХДС необхідно знати $\frac{P^n - 1}{2}$ символів послідовності, у той час, як для m-послідовностей та послідовностей Голда необхідно знати сегменти з лише $2 \cdot m$ і $4 \cdot m$ (m – ступінь поліному, у відповідності до якої формується m – послідовність) символів. У зв'язку з тим, що ХДС володіють високою структурною скритністю і відносяться до оптимальних (з точки зору періодичної функції автокореляції (ПФАК)) сигналів, володіють покращеними у порівнянні з взаємно-кореляційними властивостями m-послідовностей, викликає інтерес провести оцінку завадостійкості прийому таких сигналів при застосуванні їх у сучасних ІКС.

Криптографічні сигнали (КС): основні властивості, метод синтезу

КС – нелінійний клас дискретних послідовностей, які мають покращені, у порівнянні з більшістю лінійних класів сигналів, ансамблеві, структурні, кореляційні, а також – криптографічні властивості. Для синтезу складних нелінійних дискретних криптографічних сигналів використовуються випадкові або псевдовипадкові процеси і, на відміну від ХДС, ці сигнали можуть бути побудовані для будь-яких значень періоду. Розмір ансамблю таких сигналів залежить від вимог до кореляційних властивостей, що визначаються границями «щільної упаковки» [2].

Метод синтезу КС з заданими властивостями включає такі етапи [5 – 6]:

1. Генерація масиву псевдовипадкових послідовностей символів заданого періоду з використанням криптографічного алгоритму (джерел випадкових або псевдовипадкових послідовностей символів).

2. Тестування отриманих послідовностей із застосуванням критеріїв та показників якості генераторів, визначених міжнародними та відомчими стандартами [7 – 9].

3. Формування дискретних послідовностей (ДП) символів визначено періоду.

4. Відбір ДП, значення бічних пелюсток періодичної функції автокореляції (ПФАК) яких близькі до границі «щільної упаковки»:

5. Отримання матриці станів взаємно-кореляційних функцій всіх можливих пар послідовностей, які пройшли відбір за результатами попереднього кроку.

6. Обробка матриці, яка полягає в тому, що здійснюється відбір послідовностей, що задовольняють межам «щільної упаковки» для відповідних кореляційних функцій.

Використання наведеного методу дозволяє формувати великі ансамблі дискретних послідовностей практично будь-якого періоду з заданими, але фізично реалізованими, значеннями бічних пелюсток функцій автовзаємної і стикової функції кореляції в періодичному і аперіодичному режимах роботи, а також статистичними характеристиками кореляційних функцій, які не поступаються аналогічним характеристикам кращих класів лінійних сигналів. Що стосується структурної скритності цих сигналів, то вони володіють абсолютною скритністю, тобто володіють властивостями, які притаманні випадковим процесам. Тому оцінки завадостійкості прийому таких сигналів у порівнянні із завадостійкістю для існуючих сигналів також, з точки зору побудови сучасних ІКС, представляє інтерес.

Основні результати дослідження

Найбільш поширеною моделлю безперервних каналів з завадами є гауссов канал. Пов’язано це з тим, що: багато реальних каналів добре описуються даною моделлю; завада в такому каналі має максимальну приведену диференціальну ентропію у порівнянні з будь-якими іншими моделями завад; Гауссов канал відноситься до числа небагатьох каналів, для яких в явному вигляді розраховано величину пропускної здатності. З точки зору умов передачі інформації, гауссов канал є найбільш несприятливим випадком. Результати дослідження завадостійкості, які отримані для гауссового каналу, можуть бути тільки покращені для будь-яких інших моделей каналів та завад [10]. Завада в гауссовому каналі являє собою стаціонарний випадковий процес, в якому два будь-яких вимірювання некорельовані та незалежні. Такий процес володіє рівномірним, нескінченим, за смугою частот, спектром, а отже має нескінчену потужність. Через наявність нескінченого спектру такий процес називають «білим» і, оскільки він взаємодіє з сигналами простим підсумуванням, то – «адитивним» [10]. На рис. 1 представлена загальна структурна схема каналу зв’язку з адитивним білим гауссовим шумом (АБГШ). При моделюванні гауссового шуму обмежуються деякою фіксованою смугою частот, в якій формуються гармонічні коливання з випадковими амплітудами та фазами. Амплітуда гармоніки шуму розподілена за нормальним законом розподілу з нульовим математичним сподіванням та дисперсією N_0, яку називають спектральною щільністю потужності шуму, оскільки вона характеризує середню потужність, яка приходить на 1 Гц смуги частот [10]. При побудові імітаційних моделей каналів з АБГШ формування випадкового шуму здійснюється таким чином, щоб ширина його ефективного спектру та тривалість реалізації були не менше аналогічних сигналів, які випробовуються в моделі.

Була створена модель для випробування сигналів в умовах адитивного білого гауссового шуму.

У створеній моделі реалізовано наступні функції:

– визначення відношення сигнал/шум в діапазоні від 1 до N;

– виконання M обчислювальних експериментів імітації передачі та демодуляції сигналу при різних випадкових реалізаціях завади з підрахунком кількості біт, прийнятих з помилкою із повідомлення довжиною k;

– обчислення ймовірності помилки «на біт» при кожному значенні сигнал/шум;

– повернення вектору, який містить N знайдених значень ймовірностей;

– побудова графіків залежності ймовірності помилки від відношення сигнал/шум.

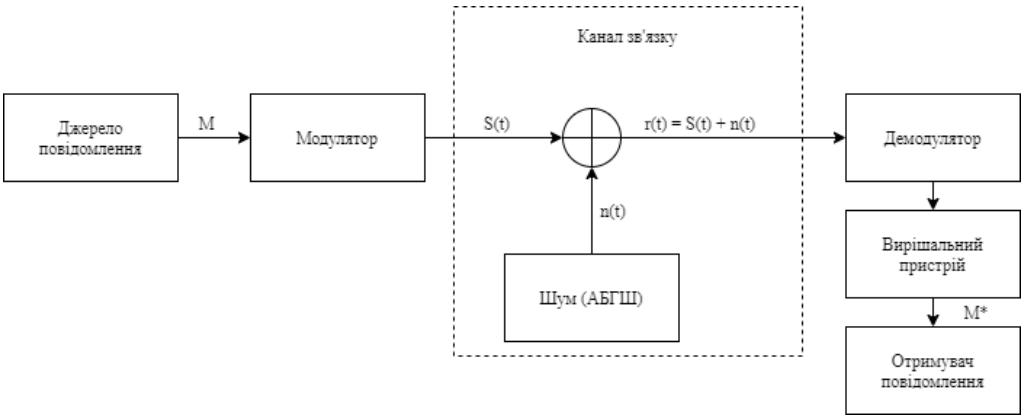


Рис. 1. Структурна схема каналу зв’язку з АБГШ

Реалізація моделі здійснюється у відповідності з блок-схемою (рис. 2).

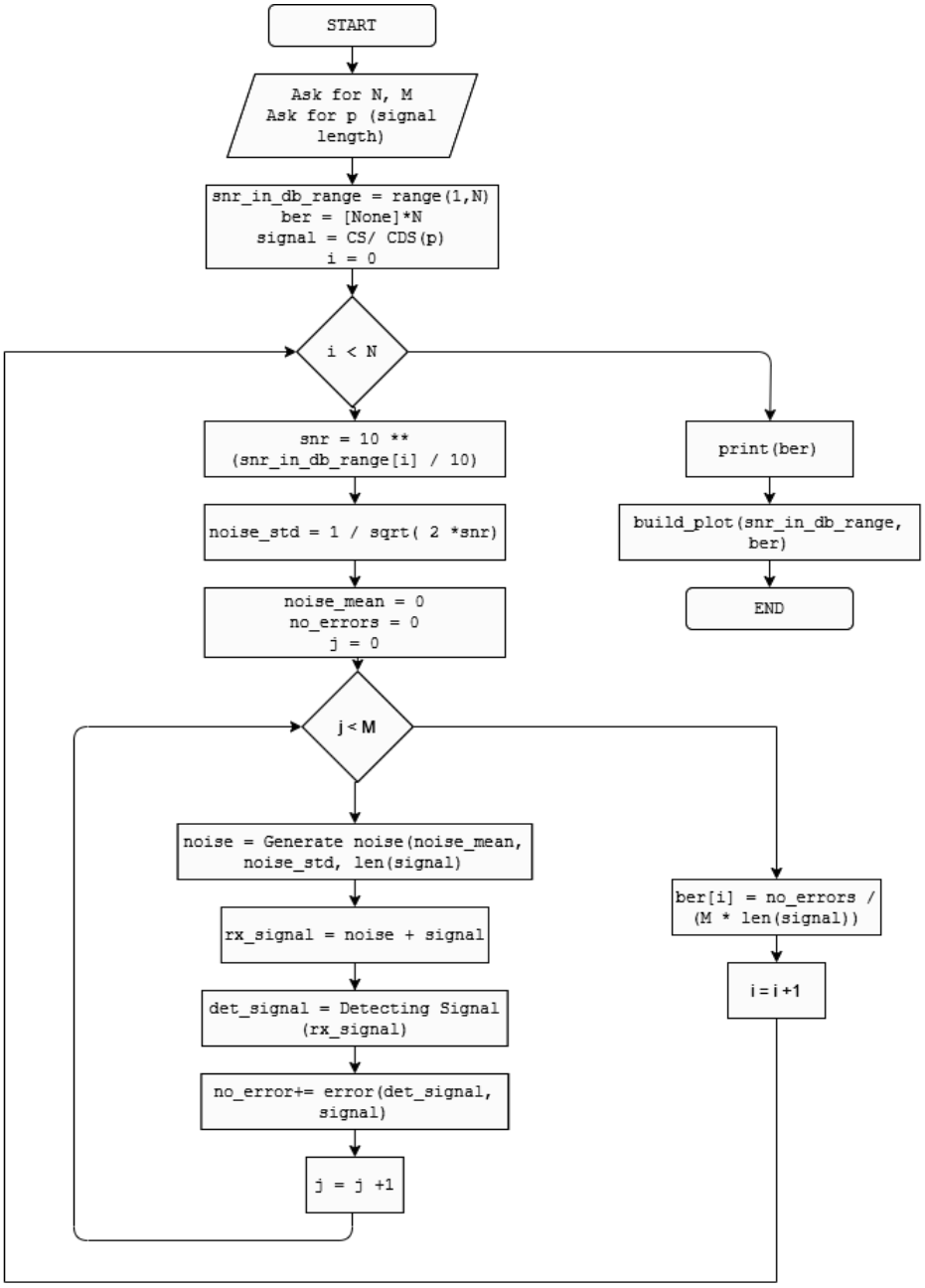


Рис. 2. Блок – схема імітаційної моделі для дослідження завадостійкості прийому сигналів в каналі з АБГШ

На рис. 2 наведено такі операції:

snr_in_db_range – діапазон відношень сигнал/шум (приймає значення від 1 до N);

snr – значення відношення сигнал/шум;

ber – структура даних, в яку буде записано отримані значення ймовірності помилки на біт при заданому SNR;

signal – початковий сигнал, що досліджується (це може бути CS (КС) або CDS (ХДС));

noise_std – середньо-квадратичне відхилення (СКВ), за яким формуються випадкові (гауссові) коефіцієнти амплітуд;

noise_mean – математичне сподівання, за яким сформовано шум;

no_errors – кількість знайдених помилок;

noise – шум, який сформовано за параметрами: noise_mean і noise_std;

rx_signal – сигнал, який передається по каналу з АБГШ (початковий сигнал + шум);

det_signal – сигнал, який виявлено вирішальним пристроєм;

Detecting Signal – процедура виявлення сигналу. Параметри, які приймає ця процедура: rx_signal;

error – процедура, яка підраховує кількість біт, які не збіглися, між signal і det_signal. Параметри, які приймає ця процедура: det_signal, signal;

build_plot – процедура, яка виконує функції побудування графіків для оцінки BER (ймовірність помилки на біт). Параметри, які приймає ця процедура: snr_in_db_range, ber;

Логіка, за якою працює вирішальний пристрій зображена на рис. 3: якщо отримане значення більше 0, то отримали «1», в противному випадку – «-1». Підрахунок кількості біт, які не збіглися, між отриманим сигналом та сигналом, який було відправлено, виконується за алгоритмом, блок-схема якого зображена на рис. 4.

На рис. 3 наведено такі операції:

Reading received signal (rx_signal) – зчитування по каналу з АБГШ сигналу, що передається;

det_sig –сигнал, що виявлено;

len(rx_signal) – тривалість сигналу rx_signal.

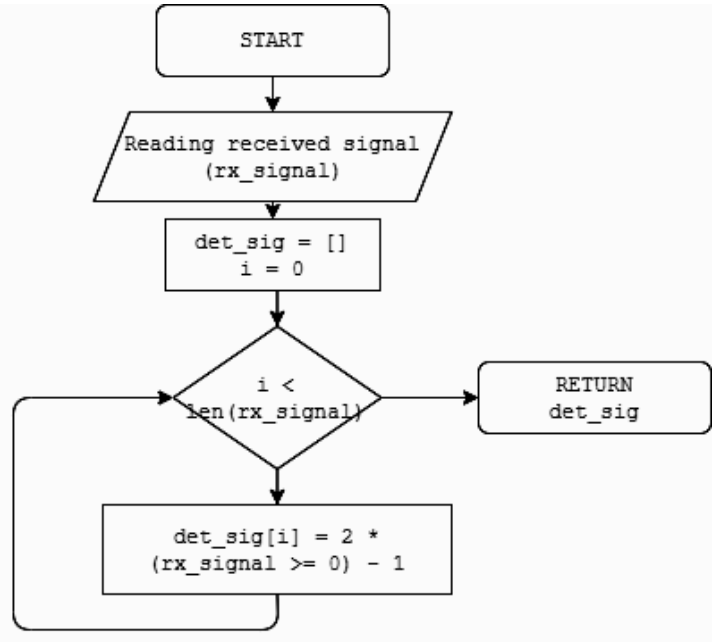


Рис. 3. Вирішальний пристрій

На рис. 4 наведено такі операції:

Reading received signal (det_signal, tx_signal) – зчитування виявленого сигналу та початкового сигналу (того, що було сформовано джерелом повідомлення);

cnt – змінна, яка зберігає кількість біт, що не збіглися;

len(det_signal) – тривалість сигналу det_signal

Програмна реалізація моделі виконувалася на комп'ютері з наступними системними характеристиками:

– Intel Core i7-4500U 1.80 – 2.40 GHz;
– 8 ГБ оперативної пам'яті;
– Windows 10 x64;

Відеокарта Nvidia 740m 2GB.

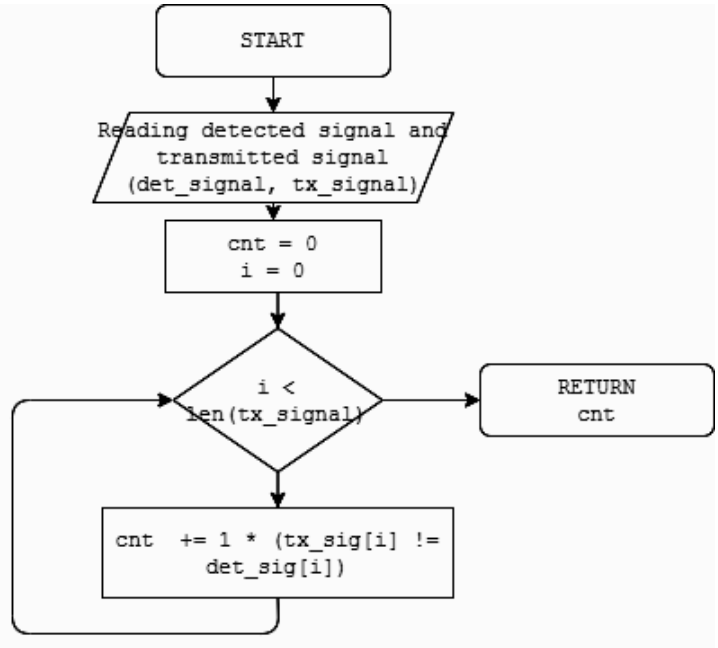


Рис. 4. Підрахунок кількості біт, які не збіглися

Тестування моделі здійснювалося за таких параметрів: відношення сигнал/шум в діапазоні від $N=1$ до $N=10$. Виконання $M=10000$ обчислювальних експериментів імітації передачі та демодуляції сигналу при різних випадкових реалізаціях завади з підрахунком кількості біт, прийнятих з помилкою із повідомлення довжиною $k=256$. Результатами, які отримані на виході моделі, є кількість знайдених помилок та ймовірність помилки на біт при заданому відношенні сигнал/шум (табл. 1).

З використанням отриманих результатів були побудовані графіки залежності ймовірності помилки на біт від значення відношення сигнал/шум (рис.).

Таблиця 1

SNR	Кількість помилок		Ймовірність помилки	
	ХДС	КС	ХДС	КС
1	144237	143922	0.056342578125	0.05621953125
2	96032	96267	0.0375125	0.037604296875
3	58362	58563	0.02279765625	0.022876171875
4	31976	31919	0.012490625	0.012468359375
5	15304	15180	0.005978125	0.0059296875
6	6136	6193	0.002396875	0.002419140625
7	1978	2055	0.00077265625	0.000802734375
8	481	525	0.000187890625	0.000205078125
9	90	78	3.515625e-05	3.046875e-05
10	12	9	4.6875e-06	3.515625e-06

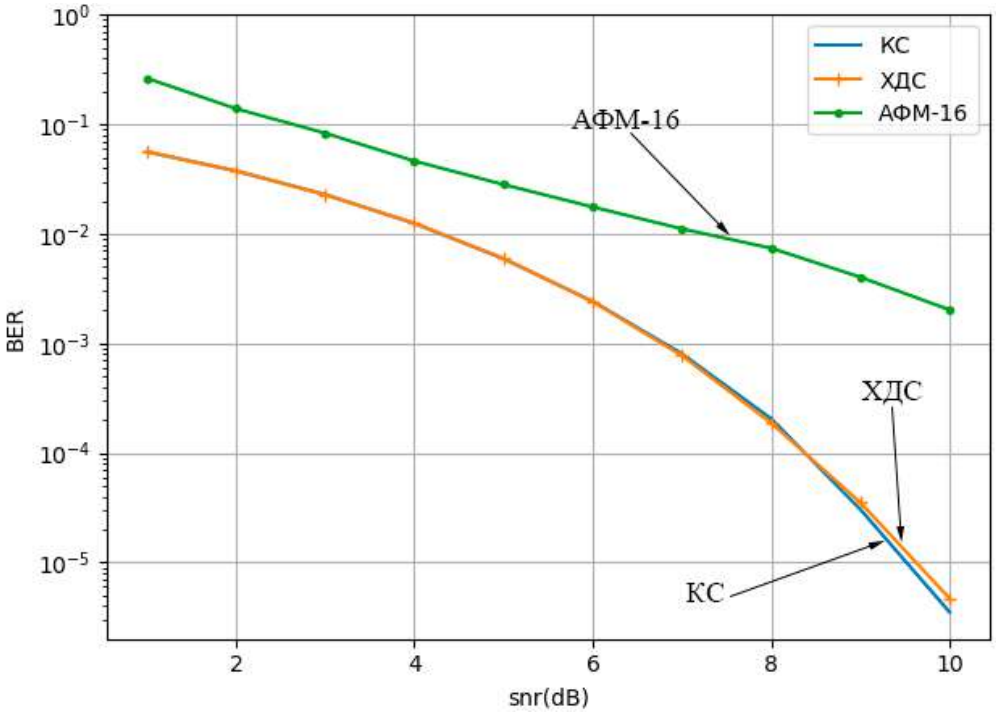


Рис. 5. Графік залежності ймовірність помилки на біт (BER) від відношення сигнал/шум

Для АФМ-16 отриманий вектор BER виглядає наступним чином [0.264275, 0.1391, 0.0832, 0.04625, 0.028225, 0.0176, 0.011125, 0.0074, 0.004025, 0.002025, 0.001375, 0.00085, 0.0008, 0.0003, 0.000125, 0.000125, 7.5e-05, 5e-05, 2.5e-05]. Аналіз отриманих результатів, які наведено у табл. 1, та порівняння їх з результатами для АФМ-16, показують, що сигнали ХДС та КС володіють достатньо низькою ймовірністю помилки, нижчою за АФМ-16.

Висновки

Результати дослідження завадостійкості, які були отримані при використанні розробленої моделі, можуть бути тільки покращені для будь-яких інших моделей каналів та завад. Тому порівняльні дослідження будь-яких ІКС проводять саме в умовах моделі каналу з АБГШ. Для низьких відношень сигнал/шум, ХДС та КС забезпечують низьку ймовірність помилки (0.056 для $SNR = 1$), тому використання саме таких сигналів в «поганих» каналах є ефективним. Порівняння застосування ХДС та КС з АФМ-16 показує, що саме сигнали, що досліджувалися, мають нижчу ймовірність помилки. Так, для відношення сигнал/шум – 10 ймовірність помилки для ХДС складає 4.6875e-06, для КС – 3.515625e-06, а для – АФМ-16 – 0.002025. Таким чином, використання нелінійних складних дискретних сигналів, зокрема ХДС та КС, дозволяє суттєво підвищити завадостійкість прийому сигналів у сучасних ІКС. При цьому, зважаючи на покращені ансамблеві і структурні властивості зазначених нелінійних сигналів, є можливість значно поліпшити показники крипто- і імітозахищеності функціонування систем.

Список літератури:

1. Горбенко, І.Д. Прикладна криптологія / І.Д. Горбенко, Ю.І. Горбенко. Харків : ХНУРЕ, 2012. 868 с.
2. Варакин Л. Е. Системы связи с шумоподобными сигналами. 1985. 384 с. 1
3. Свердлик М. Б. Оптимальные дискретные сигналы. Москва : Радио и связь, 1975. 200 с.
4. Горбенко И.Д., Замула А.А., Морозов В.Л. Информационная безопасность и помехозащищенность в телекоммуникационных системах условиях различных внутренних и внешних воздействий // Радиотехника. 2017. Вып. 189. С. 107 – 116.
5. Gorbenko I. D., Zamula A. A. Cryptographic signals: requirements, methods of synthesis, properties, application in telecommunication systems // Telecommunications and Radio Engineering Volume 76, 2017. Issue 12, p.p. 1079-1100. DOI: 10.1615/TelecomRadEng.v76.i12.50.

6. Горбенко І.Д., Замула О.А. Моделі та методи синтезу криптографічних сигналів та їх оптимізація за критерієм часової складності // Математичне та комп'ютерне моделювання. Серія: Фіз.-мат. науки : зб. наук. праць / Інститут кібернетики імені В.М. Глушкова Національної академії наук України, 2017. Вип. 15. 272 с.
7. Application Notes and Interpretation of the Scheme (AIS) 20. Functionality classes and evaluation methodology for physical random number generators. Certification body of the BSI in context of certification scheme. BSI, 1999.
8. Application Notes and Interpretation of the Scheme (AIS) 31. Functionality classes and evaluation methodology for physical random number generators. Certification body of the BSI in context of certification scheme. BSI, 2001.
9. NIST 800-90 b Recommendation for the Entropy Sources Used for Random Bit Generation, 2012.
10. Rassomakhin, S.G. Mathematical and physical nature of the channel capacity // Telecommunications and Radio Engineering. 2017. 76(16). P. 1423-1451.

Надійшла до редколегії 05.11.2020

Відомості про авторів:

Рассомахін Сергій Геннадійович – д-р техн. наук, професор, завідувач кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук, Харківський національний університет імені В.Н. Каразіна, Україна.

Замула Олександр Андрійович – д-р техн. наук, професор, професор кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук, Україна, Харківський національний університет імені В.Н. Каразіна; email: zamylaaa@gmail.com, ORCID: http://orcid.org/0000-0002-8973-6190

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

Хо Чі Лик – магістрант кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук, Харківський національний університет імені В.Н. Каразіна,Україна.

УДК 621.391 **DOI:10.30837/rt.2020.4.203.14**

О.А. ЗАМУЛА, д-р техн. наук, І.Д. ГОРБЕНКО, д-р техн. наук, ХО ЧІ ЛИК

СТАТИСТИЧНІ ВЛАСТИВОСТІ ПОХІДНИХ СИСТЕМ СИГНАЛІВ

Вступ

Завадозахищеність інформаційно-комунікаційних систем (ІКС), і одна з її складових, – структурна скритність системи, у значній мірі визначаються структурними або статистичними властивостями сигналів-переносників даних користувачів системи. Досягнення необхідних значень завадозахищеності, скритності, криптографічної стійкості може бути реалізовано на основі використання в радіоканалах динамічного режиму передачі даних в поєднанні із застосуванням дискретних складних сигналів, що володіють заданою структурною скритністю, необхідними кореляційними і ансамблевими властивостями. У свою чергу відомо [1], що для технології розширеного спектру зазначені властивості сигналів тотожні властивостям дискретних послідовностей (ДП), згідно із законом яких маніпулюють параметрами високочастотної несучої. Динамічний режим передбачає такий спосіб передачі інформації по радіоканалу, при якому здійснюється динамічна зміна за певним (випадковим) законом відповідності: «інформаційний біт – складний сигнал». Момент зміни відповідності повинен визначатися керуючої послідовністю (УП) або гамою.

Проведений аналіз [1 – 3] показав, що у даний час відсутні регулярні методи синтезу ДП оптимальних за мінімаксним критерієм. Завдання синтезу ДП виявляється ще складнішим, якщо висуваються вимоги до розмірності (об'єму) системи сигналів, структурним властивостям і числу елементів ДП. Таким чином, досить актуальною проблемою залишається пошук ефективних методів синтезу дискретних сигналів (послідовностей), що відповідають потенційно можливим граничним характеристикам кореляційних функцій (мінімаксним властивостям або границі «щільної упаковки») і володіють необхідними кореляційними, структурними, статистичними, ансамблевими властивостями.

У [4] авторами запропоновано метод синтезу похідних систем сигналів, для яких у якості вихідних застосовуються ортогональні сигнали, а у якості таких, що продукують, – нелінійні дискретні складні криптографічні сигнали (КС). Синтез останніх засновано на використанні випадкових (псевдовипадкових) процесів, у тому числі алгоритмів криптографічного перетворення інформації. Показано [5], що синтезовані таким чином похідні сигнали володіють покращеними (у порівнянні з лінійними класами сигналів) ансамблевими і кореляційними властивостями, тоді як статистичні властивості таких систем сигналів є не вивченими.

Вимоги до статистичних властивостей сигналів – переносників даних

Очевидно, що вимоги до статистичних властивостей сигналів відповідають вимогам, що пред'являються до генераторів, які формують випадкові (псевдовипадкові) послідовності. Крім того, повинна існувати можливість виконати оцінку відповідності властивостей синтезованих сигналів певним вимогам.

Методи формування послідовностей символів для додатків керуючих сигналів і сигналів-переносників інформації можна розділити на два великі класи – випадкові (фізичні) і псевдовипадкові [6 – 7]. Засоби, що забезпечують генерацію випадкових послідовностей чисел або бітів, будемо називати генераторами випадкових послідовностей (ГВП), а генератори, що забезпечують генерацію псевдовипадкових послідовностей (ПВП), – детермінованими генераторами випадкових послідовностей (ДГВП). ДГВП є одним з базових примітивів для більшості криптографічних додатків. Одним з основних властивостей і переваг ДГВП є забезпечення відновленності послідовності в просторі і часі. У той же час ПВП повинні мати гарантовані властивості щодо періоду повторення, відновлення відрізків ПВП в просторі і часі, можливість проведення попереднього дослідження їх властивостей і інше [6]. При цьому необхідно враховувати, що ніякий детермінований алгоритм не може генерувати повністю випадкові послідовності, він може тільки апроксимувати деякі властивості випад-

кових послідовностей. Більшість ДГВП мають ряд серйозних недоліків, а послідовності, які генеруються такими генераторами, не відповідають вимогам, що пред'являються криптографічними додатками і додатками, пов'язаними з реалізацією динамічного режиму функціонування систем зв'язку зі складними сигналами.

Основними недоліками ДГВП є:

– неприпустимо короткий або недоведений період повторення послідовності;

– недостатня нерозрізненість гами, що також робить її певним чином передбачуваною «вперед і назад»;

– властивості випадковості, рівноймовірності, незалежності та однорідності не відповідають вимогам і інші.

Існує кілька підходів до визначення вимог до рівнів гарантій ДГВП. Перший підхід пов'язаний з тестуванням ПВП на нерозрізненість, для чого, наприклад, застосовуються федеральні стандарти FIPS 140-1, FIPS 140-2, FIPS 140-3. Більш детальні вимоги і механізми реалізації визначені в AIS 20, що дозволяє реалізувати різні рівні гарантій: К1, К2, К3, К4 [8].

Основними загальними вимогами до ДГВП є [6]:

- вимога нерозрізненості вихідних послідовностей ДГВП від істинно випадкових послідовностей;

- вимога непередбачуваності вихідних бітів для порушника з обмеженими обчислювальними ресурсами;

- вимога незворотності генератора в сенсі попередньо заданої малої ймовірності компрометації ключа самого ДГВП.

Таким чином, ПВП повинна мати деякі статистичні властивості [9], які притаманні істинно випадковим послідовностям.

Найбільш прийнятними (з точки зору практичного використання) методиками тестування є: FIPS PUB 140-1, AIS 20 і AIS 31, NIST 800-90b, NIST 800-22. До складу NIST 800-22 [10] входять 16 статистичних тестів, при цьому обчислюються 188 значень ймовірностей. Всі тести спрямовані на виявлення різних дефектів випадковості (невідповідність вимогам випадковості).

Порядок тестування.

1. Висувається нульова гіпотеза H_0 – припущення про те, що двійкова послідовність, яка підлягає тестуванню, є випадковою.

2. Для послідовності, що формується генератором, розраховується статистика тесту.

3. З використанням спеціальної функції і статистики тесту розраховується значення ймовірностей $P \in [0,1]$.

4. Значення ймовірності P порівнюється з рівнем значущості α, $\alpha \in [0,001; 0,01]$. Якщо $P \geq \alpha$, то гіпотеза H_0 приймається. В іншому випадку приймається альтернативна гіпотеза.

В результаті тестування ПВП символів формується вектор значень ймовірності $\mathrm{P} = \{\mathrm{P}_1, \mathrm{P}_2, ..., \mathrm{P}_{188}\}$. У NIST використовуються два пороги для прийняття рішення про результати тестування – це 0.96 і 0.99, тобто для різних рівнів значимості встановлюється, що з 100 блоків може не пройти чотири і один тест відповідно.

Основні результати досліджень

З використанням NIST SP 800-22 було виконано тестування реалізацій похідних криптографічних послідовностей символів (ПКПС). Для тестування із залученням NIST SP 800-22 для точності розрахунків необхідно мати послідовність символів довжиною не менше 100. Для тестування було синтезовано 20 похідних сигналів на основі криптографічних послідовностей з періодом $N = 1024$. Для тестування ПКПС були застосовані наступні тести NIST SP 800-22: частотний побітовий тест (monobit test), частотний блоковий тест (frequency within block test), тест на послідовність однакових біт (runs test), тест на найдовшу послідовність

з одиниць в блоці (the longest run test), спектральний тест (spectral test), тест на підпослідовності (serial test). Результати тестування за зазначеними тестами наведено у табл. 1 – 6.

Таблиця 1

Результати тестування похідних сигналів (ПКПС) з $N = 1024$ (монобітний тест)

Номер похідного сигналу	Кількість «1»	Кількість «0»	$P-value$	$P-value > 0.01$
1	515	509	0.8512686236882057	Так
2	515	509	0.8512686236882057	Так
3	497	527	0.34850142376108484	Так
4	503	521	0.5737754036327304	Так
5	492	532	0.21129954733371054	Так
6	478	546	0.033586612896897634	Так
7	522	502	0.5319710580974011	Так
8	518	506	0.7076604666545525	Так
9	522	502	0.5319710580974011	Так
10	530	494	0.26058903427361774	Так
11	538	486	0.10416255883043911	Так
12	518	506	0.7076604666545525	Так
13	516	508	0.8025873486341526	Так
14	526	498	0.38157390570502125	Так
15	538	486	0.10416255883043911	Так
16	512	512	1.0	Так
17	529	495	0.2880087580039419	Так
18	551	473	0.014789214221761392	Так
19	511	513	0.9501646619415056	Так
20	515	509	0.8512686236882057	Так

Таблиця 2

Результати тестування похідних сигналів (ПКПС) з $N = 1024$ (частотний блоковий тест)

Номер похідного сигналу	Кількість блоків	Довжина блоків	$P-value$	$P-value > 0.01$
1	51	20	0.33940489399393925	Так
2	51	20	0.5534531438608977	Так
3	51	20	0.8813982930103362	Так
4	51	20	0.6488836444446106	Так
5	51	20	0.40437005733917836	Так
6	51	20	0.3748688142935794	Так
7	51	20	0.5293703452563876	Так
8	51	20	0.7456190658758038	Так
9	51	20	0.5293703452563878	Так
10	51	20	0.6872742496942255	Так
11	51	20	0.2927697888058552	Так
12	51	20	0.2678516820668022	Так
13	51	20	0.9033253460171587	Так
14	51	20	0.9188302753065043	Так
15	51	20	0.1469610705317797	Так
16	51	20	0.7456190658758047	Так
17	51	20	0.4736606532819697	Так
18	51	20	0.35338907550154847	Так
19	51	20	0.9073701122564067	Так
20	51	20	0.2500343356092065	Так

Таблиця 3

Результати тестування похідних сигналів (ПКПС) з $N = 1024$ (тест на послідовність однакових біт)

Номер похідного сигналу	π	$2/\sqrt{n}$	$V(obs)$	$P-value$	$P-value > 0.01$
1	0.5029296875	0.0625	509	0.8521250020025395	Так
2	0.5029296875	0.0625	503	0.5745108154065952	Так
3	0.4853515625	0.0625	522	0.5137393123371727	Так
4	0.4912109375	0.0625	499	0.4220554377618176	Так
5	0.48046875	0.0625	507	0.7917222651893452	Так
6	0.466796875	0.0625	499	0.5000821445021373	Так
7	0.509765625	0.0625	526	0.3747852254608464	Так
8	0.505859375	0.0625	517	0.7512906048863373	Так
9	0.509765625	0.0625	529	0.2823222794660727	Так
10	0.517578125	0.0625	537	0.10870671148349663	Так
11	0.525390625	0.0625	488	0.15527454436985028	Так
12	0.505859375	0.0625	525	0.4139245820069865	Так
13	0.50390625	0.0625	513	0.9486062978096323	Так
14	0.513671875	0.0625	521	0.5572946676001701	Так
15	0.525390625	0.0625	504	0.6755378568281317	Так
16	0.5	0.0625	519	0.6617487760817584	Так
17	0.5166015625	0.0625	513	0.9220226305700431	Так
18	0.5380859375	0.0625	487	0.16609336473330275	Так
19	0.4990234375	0.0625	538	0.10413523041859732	Так
20	0.5029296875	0.0625	489	0.1508741397898685	Так

Таблиця 4

Результати тестування похідних сигналів (ПКПС) з $N = 1024$
(тест на найдовшу послідовність з одиниць в блоці)

Номер похідного сигналу	M	K	N	χ^2	$P-value$	$P-value > 0.01$
1	8	3	16	2.5848131767158087	0.4601582158650065	Так
2	8	3	16	4.910991740701903	0.17843200168629486	Так
3	8	3	16	2.840887683858429	0.4168132306658415	Так
4	8	3	16	2.299431426250259	0.5126298393652022	Так
5	8	3	16	1.4862582449817263	0.6854455326497724	Так
6	8	3	16	2.3224200745898065	0.508239427919698	Так
7	8	3	16	3.1691947567842096	0.3662670999085182	Так
8	8	3	16	10.258130285753692	0.01649468713031408	Так
9	8	3	16	0.2232915342847958	0.9736854118111586	Так
10	8	3	16	1.966671701487854	0.5793528537379324	Так
11	8	3	16	10.946509638593566	0.012018662584735648	Так
12	8	3	16	1.0802337929911223	0.7818477379705312	Так
13	8	3	16	4.754440741329501	0.19068693056675992	Так
14	8	3	16	0.519846469107887	0.9145094314246653	Так
15	8	3	16	3.0901474502960573	0.37793397002883145	Так
16	8	3	16	0.5456175029974611	0.9087605671831471	Так
17	8	3	16	0.5456175029974611	0.9087605671831471	Так
18	8	3	16	5.474477981185082	0.14017311067991284	Так
19	8	3	16	0.9697299296305197	0.8085758557302485	Так
20	8	3	16	0.3992037675828323	0.9404034454800299	Так

Таблиця 5

Результати тестування похідних сигналів (ПКПС) з $N = 1024$ (спектральний тест)

Номер похідного сигналу	H_0	N_1	$P-value$	$P-value > 0.01$
1	486.4	483	0.32955189239856303	Так
2	486.4	480	0.06645742001693215	Так
3	486.4	480	0.06645742001693215	Так
4	486.4	478	0.016002207003436186	Так
5	486.4	486	0.9086766781799538	Так
6	486.4	480	0.06645742001693215	Так
7	486.4	481	0.12148844104797517	Так
8	486.4	486	0.9086766781799538	Так
9	486.4	490	0.30189844442852465	Так
10	486.4	486	0.9086766781799538	Так
11	486.4	486	0.9086766781799538	Так
12	486.4	491	0.1871221556836583	Так
13	486.4	488	0.6463551955394854	Так
14	486.4	492	0.10829365589900763	Так
15	486.4	492	0.10829365589900763	Так
16	486.4	490	0.30189844442852465	Так
17	486.4	485	0.6880685751927309	Так
18	486.4	485	0.6880685751927309	Так
19	486.4	486	0.9086766781799538	Так
20	486.4	485	0.6880685751927309	Так

Крім того, було проведено тестування ПКПС з використанням стандарту FIPS-140. Для того щоб виконати тести FIPS-140, необхідно мати 20000 символів. В цьому випадку було вирішено «склеїти» 20 ПКПС з періодом $N = 1024$, які використовувались при тестуванні за тестами NIST SP 800-22 SP. Були використані наступні статистичні тести FIPS-140: частотний побітовий тест (monobit test), тест покеру (poker test), тест на послідовність однакових біт (runs test), тест на найдовшу послідовність з одиниць/нулів (the longest run test). Результати тестування ПКПС за зазначеними тестами наведено в табл. 7 – 8.

Таблиця 6

Результати тестування похідних сигналів (ПКПС) з $N = 1024$ (тест на підпослідовності)

Номер	ψ_m^2	ψ_{m-1}^2	ψ_{m-2}^2	$\nabla\psi_m^2$	$\nabla^2\psi_m^2$	$P-value1$	$P-value2$	$P > 0.01$
1	5.28125	2.015625	0.1328125	3.265625	1.3828125	0.91659944429465	0.847176717754098	Так
2	14.3125	3.015625	0.4609375	11.296875	8.7421875	0.18543852707816513	0.06787671836894967	Так
3	9.0	3.578125	2.1484375	5.421875	3.9921875	0.71167936424658895	0.40706418913507897	Так
4	9.125	4.28125	1.3984375	4.84375	1.9609375	0.77413839112877647	0.7429435663716482	Так
5	12.40625	6.625	3.265625	5.78125	2.421875	0.67171988224295573	0.6586777475527147	Так
6	31.65625	18.59375	9.796875	13.0625	4.265625	0.10971720056655933	0.37124935114918887	Так
7	11.90625	4.21875	1.546875	7.6875	5.015625	0.46457579096932533	0.28569802683920476	Так
8	5.40625	0.5625	0.34375	4.84375	4.625	0.77413839112877647	0.32798191520517467	Так
9	18.5	9.0625	1.78125	9.4375	2.15625	0.30674264714918487	0.7070464216929457	Так
10	22.625	12.6875	4.78125	9.9375	2.03125	0.26944004415793343	0.73001099814728893	Так

11	34.25	19.0625	7.53125	15.1875	3.65625	0.055600554198860314	0.4545210498689997	Так
12	9.8125	2.5	0.84375	7.3125	5.65625	0.5033219991047654	0.22633255639493863	Так
13	9.8125	4.8125	0.125	5.0	0.3125	0.7575761331330662	0.9889930346992064	Так
14	12.75	6.625	1.78125	6.125	1.28125	0.6332322827218166	0.8645486214149056	Так
15	50.1875	19.75	5.53125	30.4375	16.21875	0.00017685119110517008	0.0027392506072084983	Ні
16	4.03125	1.28125	0.140625	2.75	1.609375	0.9490538343829868	0.8071061737365048	Так
17	8.78125	3.875	2.2578125	4.90625	3.2890625	0.767547686281258	0.5106670730463856	Так
18	36.21875	23.4375	14.5234375	12.78125	3.8671875	0.11960103247709221	0.42427835448812967	Так
19	8.46875	5.3125	2.6484375	3.15625	0.4921875	0.9241725499586169	0.9742570565851398	Так
20	12.6875	6.828125	2.3203125	5.859375	1.3515625	0.662980451379133	0.852568453615844	Так

Таблиця 7

Результати тестування похідних сигналів (ПКПС) з $N = 1024$
(монобітний тест, тест покеру, тест на максимальну довжину серії FIPS-140)

Назва тесту	X	Умова успішного тесту	X задовольняє умові
Монобітний тест	10104	$9654 < X < 10346$	Так
Тест покеру	16.806400000000394	$1.03 < X < 57.4$	Так
Тест на максимальну довжину серії	12	$X < 34$	Так

Таблиця 8

Результати тестування похідних сигналів (ПКПС) з $N = 1024$ (тест серій FIPS-140)

Символ	Довжина серії						Тест пройдено
	1	2	3	4	5	6+	
«1»	2504	1245	605	298	159	187	Так
«0»	2540	1248	605	303	141	162	Так

Висновки

Численні дослідження статистичних властивостей похідних нелінійних криптографічних послідовностей символів із застосуванням NIST SP 800-22, FIPS-140 показали, що параметри, які оцінюються при реалізації відповідних тестів, знаходяться в межах допустимих значень. А це, в свою чергу, означає, що похідні системи сигналів, для яких у якості сигналів, що продукують, застосовуються нелінійні дискретні складні криптографічні сигнали, задовольняють вимогам, що пред'являються до псевдовипадкових послідовностей: непередбачуваність, незворотність, випадковість, незалежність символів і ін. По суті такі сигнали не відрізняються від випадкових послідовностей. Таким чином, використання саме таких похідних сигналів як фізичного переносника даних дозволить поліпшити показники завадозахищеності і інформаційної безпеки сучасних ІКС.

Список літератури:

1. Sarvate D.V. Crosleration Properties of Pseudorandom and Related Sequences / D.V. Sarvate, M.V. Parsley // IEEE Trans. Commun. 1980. Vol. Com 68. P. 59–90.

2. Варакин Л. Е. Системы связи с шумоподобными сигналами. Москва : Сов. радио. 1985. 384 с.

3. Ipatov Valery P. Spread Spectrum and CDMA. Principles and Applications / University of Turku, Finland and St. Petersburg Electrotechnical University ‘LETI’. Russia. John Wiley & Sons Ltd. The Atrium, Southern Gate, Chichester, West Sussex PO19 8SQ, England. 2005. 385 p.
4. Gorbenko I. D., Zamula A. A., Ho Tri Luk Synthesis of derivatives of complex signals based on nonlinear discrete sequences with improved correlation properties // Радіотехніка. 2019. Вип. 199. С. 110-120.
5. Gorbenko I. D., Zamula A. A., Tri Luc Ho Derived signals systems for information communication systems applications: synthesis, formation, processing and properties // International Conference problems of info communications science and technology PIC S&T′2020. 6-9. October 2020. Kharkov, Ukraine. P. 3-10.
6. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Теорія. Практика. Застосування. Харків : Форт, 2012. 880 с.
7. Горбенко Ю.І. Побудова, аналіз, стандартизація та застосування криптографічних систем ; за ред. І.Д. Горбенко. Харків : Форт, 2015. 959 с.
8. Application Notes and Interpretation of the Scheme (AIS) 20. Functionality classes and evaluation methodology for physical random number generators. Certification body of the BSI in context of certification scheme. BSI, 1999.
9. Andrea Rock. Pseudorandom Number Generators for Cryptographic Applications // Diplomarbeit zur Erlangung des Magistergrades an der Naturwissenschaftlichen Fakultat der Paris-London-Universitat Salzburg. Salzburg, 2005.
10. NIST 800-22 A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, 2000.

Надійшла до редколегії 17.10.2020

Відомості про авторів:

Замула Олександр Андрійович – д-р техн. наук, професор, професор кафедри безпеки інформаційних систем і технологій, факультет комп’ютерних наук, Харківський національний університет імені В.Н. Каразіна, Україна; email: zamylaaa@gmail.com, ORCID: http://orcid.org/0000-0002-8973-6190

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

Хо Чі Лик – магістрант кафедри безпеки інформаційних систем і технологій, факультет комп’ютерних наук, Харківський національний університет імені В.Н. Каразіна, Україна.

621.396.96, 621.397.48:004.932.2 DOI:10.30837/rt.2020.4.203.15

В.М. КАРТАШОВ, д-р техн. наук, В.Н. ОЛЕЙНИКОВ, канд. техн. наук,
В.И. ЛЕОНИДОВ, канд. техн. наук, В.В. ВОРОНИН, канд. техн. наук,
А.И. КАПУСТА, И.С. СЕЛЕЗНЕВ, Е.В. ПЕРШИН

КОМПЛЕКСНАЯ ОБРАБОТКА СИГНАЛОВ ИНТЕГРИРОВАННОЙ СИСТЕМЫ НАБЛЮДЕНИЯ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ С ИСПОЛЬЗОВАНИЕМ ЦЕЛЕУКАЗАНИЯ

Введение

Беспилотные летательные аппараты (БПЛА) способны выполнять широкий спектр полезных функций, но в то же время они представляют потенциальную угрозу для различных областей деятельности человека – хозяйственной, повседневной и военной [1]. Значительные технические возможности, широкая номенклатура и сравнительно невысокая стоимость БПЛА в сочетании с трудностями их наблюдения и контроля, приводящими к повышению безнаказанности и массовости противоправных действий с их использованием [2 – 5], – основные особенности данной проблемы.

При обнаружении и измерении координат беспилотных летательных аппаратов используют, радиолокационные, акустические, оптические и инфракрасные методы и средства [6 – 12], а также комплексные системы, в которых указанные средства интегрированы в единую структуру [13 – 23].

Первой информационной задачей локационных систем является задача обнаружения. Однако хорошо разработанные методы энергетического обнаружения сигналов по отношению к БПЛА не показывают достаточной эффективности [24, 25, 43, 44]. Вследствие этого на практике обнаружение БПЛА при наличии подобных ему объектов реализуют как задачу «обнаружения-распознавания», т.е. решение задачи обнаружения дрона сопровождается анализом наличия некоторых дополнительных признаков у принимаемого сигнала.

Известные системы комплексной обработки сигналов информационных каналов, используемые для обнаружения и наблюдения БПЛА, рассматриваются в ряде публикаций. В [26] рассмотрена система, включающая радиолокационный, оптический и радиочастотный информационные каналы. Исследуются особенности функционирования мультисенсорных систем обнаружения БПЛА, особенности измерения пространственных координат в комплексной системе, а также различные варианты объединения результатов и решений отдельных информационных каналов. Алгоритм обработки информации содержал сопоставление данных в различных каналах, обнаружение целей, определение местоположения. В условиях присутствия нескольких целей в зоне обзора предварительно осуществлялось обнаружение целей непосредственно в имеющихся информационных каналах, а далее происходило сопоставление и совмещение решений об обнаружении на предмет принадлежности их к определенному объекту. Результатом такой комплексной обработки являются решения о соответствии определенных отметок целям, либо о соответствии их ложной тревоге, вынесенной в канале. Анализировался также вклад каждого информационного канала в принятие решения об обнаружении. Далее осуществлялась комплексная обработка данных с целью измерения координат и определения пространственного местоположения объектов.

В работе [27] обсуждаются вопросы объединения информации в комплексной системе, включающей радиолокационный, акустический и оптические каналы – в видимом и коротковолновом инфракрасном (SWIR) диапазонах, при решении задач обнаружения, распознавания наблюдаемых БПЛА и определения их пространственных координат. Комплексная сис-

тема обеспечивает погрешности измерения пеленга по азимуту и углу места соответственно 1,5 и 2,5 град. Определение направления в акустическом канале реализовано с использованием сверхразрешающих методов пространственного спектрального анализа.

Отмечается, что комплексирование радиолокационного и акустического каналов обеспечило значительное сокращение количества наблюдаемых ложных тревог, а комплексирование изображений видимого и инфракрасного спектральных диапазонов обеспечивает более оперативное и достоверное обнаружение БПЛА при наличии различного рода помех, дыма и неблагоприятного фона на изображениях.

В [28] осуществлялось наблюдение БПЛА с использованием статических и мобильных пунктов, расположенных в городской черте. Комплексная система включала радиолокационные, акустические, оптические средства и лазерный локатор. В акустическом канале осуществлялась пеленгация и определение местоположения с использованием метода триангуляции, обеспечивающего определение местоположения с ошибкой в 6 м.

В ряде известных работ при объединении данных различных информационных каналов комплексных систем обнаружения БПЛА применялись методы и средства искусственного интеллекта.

В [29] для предварительного обнаружения БПЛА использовалась радиолокационная станция, а далее информация об обнаруженных объектах использовалась акустической системой. Выходная информация последней использовалась для выявления БПЛА с помощью предварительно обученного алгоритма глубокого обучения, состоящего из трех ветвей MLP. Комплексная система обеспечивала малую вероятность ложных тревог и успешное обнаружение БПЛА в полевых условиях на дальности порядка 50 м. Хотя дальность оказалась небольшой, но и стоимость такой комплексной системы также невелика.

Для объединения информации радиолокационного, акустического, видимого и инфракрасного каналов комплексной системы [30] использовался фильтр Калмана. Решение формировалось с использованием классификатора ближайшего соседа. Система обеспечивала наблюдение воздушных транспортных средств на удалении до 800 м.

Комплексная система [31] включала 30 видеокамер и 3 микрофона. Информация оптического и акустического каналов анализировалась с использованием классификаторов SVM, обученных предварительно с использованием изображений дронов и акустических сигналов, порождаемых БПЛА. Система успешно работала при полетах БПЛА на высотах до 100 м и на дальности до 200 м.

Количество работ, обнаружению и наблюдению БПЛА на фоне разнообразных помех, существующим методам и системам, предназначенным для решения этих задач, постоянно увеличивается. Внимание в литературе уделяется и мультисенсорным системам, построенным с использованием различных физических датчиков. Анализируются различные методы приема, обработки сигналов, их последующего интеллектуального анализа. Однако эффективность функционирования комплексных систем и соответствующих методов обработки сигналов на практике является недостаточной. В целом проблема наблюдения и противодействия БПЛА не получила удовлетворительного решения, она является сложной, многогранной, и требует комплексного, системного подхода при её решении.

Статья посвящена анализу возможностей систем с комплексной обработкой информации, получаемой по каждому из используемых каналов, синтезу и анализу эффективных методов комплексной обработки сигналов в интегрированной комплексной системе наблюдения беспилотных летательных аппаратов, построенных с учетом естественного пространственного эшелонирования различных информационных каналов и с использованием целеуказания.

Постановка задачи комплексной обработки

При наличии нескольких информационных каналов в комплексной системе обнаружения БПЛА вначале происходит канальная обработка сигналов, принимаются некоторые достаточно простые решения, не требующие длительной выборки, значительной информативности входных сигналов, длительного времени анализа и значительных вычислительных ресур-

сов. Например, вначале принимается решение об энергетическом обнаружении целей в канале. Далее полученные входные сигналы и извлеченная из них информация, а также вновь поступившая на вход сигналы используются при последующей обработке и принятии более сложных решений.

В то же время полученную предварительную информацию об обнаруженных по энергетическому критерию целях, среди которых будут присутствовать как БПЛА, так и птицы и иные объекты, целесообразно использовать далее для целеуказания иным информационным каналам интегрированной системы. Это позволит облегчить и ускорить процесс нахождения ими уже обнаруженных ранее другим каналом целей, а информацию и сигнал наиболее «дальнозоркого» канала следует использовать совместно с информацией сигналов других каналов при принятии более сложных и обоснованных решений (например, об обнаружении, распознавании, классификации целей и т.д.).

Под целеуказанием будем понимать информационное сообщение о пространственных координатах, векторе движения и иных характеристиках БПЛА, переданное от одного канала комплексной системы обнаружения БПЛА, другому информационному каналу с целью более быстрого обнаружения объекта последним. «Энергетическим» будем называть процесс обнаружения объектов, выполняемый без учета информационных свойств, отделяющих БПЛА от иных находящихся в зоне обзора объектов.

Заметим, что цифровые методы обработки сигналов позволяют сохранять входные выборки, которые использовались при принятии решений на ранней стадии обработки – при формировании предварительных решений. Также позволяют сохранять извлеченную ранее из сигналов информацию в виде некоторых решений (об обнаруженных целях, результатах измерения их координат) и использовать все это при принятии более сложных решений на последующих этапах обработки.

Рассмотрим информационные возможности каждого из методов и соответствующих средств, входящих в состав комплексной системы обнаружения, измерения координат и параметров движения БПЛА.

Радиолокационный метод имеет достаточно хорошие поисковые возможности, значительную дальность действия, обеспечивает измерение пространственных координат (дальности и угловых координат), траектории перемещения объекта и оценку микродоплеровской сигнатуры, в виде набора информационных параметров, характеризующих особенности конструкции планера, двигателя и т.д. [2, 12, 22, 24, 25, 43, 44].

Оптический и инфракрасный методы имеют неплохие, но более скромные, чем радиолокационный метод, поисковые возможности. Они обеспечивают измерение пеленга, дальности, траектории и вектора скорости движения (по совокупности отметок целей), позволяют формировать «портреты» объектов в оптическом и инфракрасном диапазонах, используемые при решении задачи обнаружения-распознавания [6, 7, 17, 19].

Акустический метод имеет сравнительно невысокую дальность действия, но достаточно хорошие поисковые возможности. Этот метод обеспечивает измерение пеленга в двух плоскостях, позволяет определять пространственное местоположение объекта триангуляционным методом (но реализация этих возможностей на практике представляется труднореализуемой), позволяет формировать частотный портрет объекта, используемый далее в процессе решения задачи обнаружения-распознавания [4, 5, 8 – 10, 13, 14].

При наличии совокупности взаимосвязанных методов и средств обработки сигналов БПЛА, в условиях дефицита времени и ресурсов, обработка должна строиться таким образом, что вначале используются методы, имеющие лучшие поисковые возможности, затем последовательно подключаются другие методы в соответствии с их поисковыми, энергетическими и информационными возможностями.

Часть целей может быть отбракована еще на этапе последовательного подключения возможностей комплексной системы. По мере приближения объекта включаются все большие информационные возможности и соответствующие алгоритмы, и более сложные ситуации (в частности по распознаванию и отделению БПЛА от птиц и иных объектов) обрабатывают-

ся и принимаются решения с заданными показателями качества тогда, когда интегральная информативность комплексного (векторного) сигнала обеспечивает такую возможность.

Таким образом, обеспечивается последовательное подключение имеющихся в комплексной системе информационных ресурсов с учетом наличия у соответствующих методов поисковых возможностей.

Следует отметить, что в каждом канале вначале происходит энергетическое обнаружение объекта (обнаружение объекта на фоне шумов и помех), а затем либо в одном канале, либо по информации, получаемой из нескольких каналов, происходит информационное обнаружение БПЛА (распознавание его на фоне сходных с ним по некоторым признакам объектов). Далее осуществляется разрешение, оценка параметров, формирование траекторий и т.д. На каждом из указанных этапов решение может приниматься по сигналам одного, либо нескольких каналов.

Комплексирование различных каналов, методов и средств, применяемых при обнаружении БПЛА в интегрированной системе происходит с целью последовательного накопления и повышения качества и объема получаемой от объекта (объектов) информации в силу естественного пространственного эшелонирования имеющихся средств обнаружения и наблюдения, а также с целью повышения качества имеющихся или формирующихся решений об обнаружении, распознавании, разрешении, оценки координат и параметров движения объекта.

Пространственное эшелонирование информационных каналов

Рассмотрим более детально энергетические и поисковые возможности методов и средств, входящих в состав комплексной системы обнаружения БПЛА, с целью организации целесообразной комплексной обработки сигналов с учетом естественного пространственного эшелонирования.

Возможности различных средств обнаружения, распознавания и сопровождения малых БПЛА приведены в таблице.

Радиолокационной энергетической характеристикой БПЛА является эффективная площадь рассеяния, которая имеет единицы измерения м^2 и зависит от размеров объекта, его формы, материала из которого он изготовлен, длины волны и поляризации падающего поля. При решении задач распознавания и классификации БПЛА пользуются сигнатурой (или микро-доплеровской сигнатурой), которая представляет собой, по сути, радиолокационный портрет объекта. Сигнатура определяется кинематическими свойствами цели, а также модуляцией зондирующего сигнала при рассеянии движущимися элементами объекта – винтов, лопаток турбореактивного двигателя и т.д., геометрическими и физическими и особенностями цели.

В [36] приведены результаты выполненных расчетов дальности обнаружения БПЛА, имеющих различные характеристики. Результаты получены для РЛС с длиной волны 3 см. В расчетах использовались следующие характеристики БПЛА: масса аппаратов m изменялась в диапазоне от 5 до 200 кг, а ЭПР σ в диапазоне 0,05 – 5 м^2.

Как видно из рис. 1, на высоте 3 км дальность обнаружения БПЛА с $m=200$ кг ($\sigma=5$ м^2) составляла 11,8 км, а для БПЛА с $m=5$ кг ($\sigma=0{,}05$ м^2) – 2,1 км. На высоте 2 км: при $m=200$ кг ($\sigma=5$ м^2) дальность составляла 10,6 км, при $m=5$ кг ($\sigma=0{,}05$ м^2) – 2 км. На высоте 0,5 км при $m=200$ кг ($\sigma=5$ м^2) дальность обнаружения – 6 км, при $m=5$ кг ($\sigma=0{,}05$ м^2) – 1,1 км.

Таким образом, уменьшение массогабаритных характеристик БПЛА сопровождается существенным уменьшением дальности их обнаружения. В случае использования радиопрозрачных (композиционных) материалов в конструкции летательных аппаратов процесс их обнаружения и наблюдения с использованием радиолокационных средств затрудняется еще более.

Возможности различных типов средств разведки при решении задач идентификации сопровождения малых БПЛА [35, 36]

Характеристика	Радио		Оптические			Акустические
	Средства РЛР (РЛС)	Средства РРТР	Средства ОЭР в видимом диапазоне	Средства ОЭР в ИК диапазоне	Лазерные средства	Средства АР
Обнаружение дневное время	+	+	+	–	+	+
Обнаружение в ночное время	+	+	–	+	+	+
Обнаружение в условиях естественных помех	+	+	+	+	+	+
Обнаружение БПЛА среди естественных объектов (прежде всего – птиц)	–	+	–	–	–	±
Обнаружение в сложных погодных условиях	±	+	–	–	–	–
Идентификация БПЛА	–	+	±	±	–	+
Селекция одиночных и групповых целей	+	+ (по различным каналам)	+	+	+	+ (для БПЛА различных типов)
Сопровождение и формирование траектории	+	+ (для многопоз. системы)	+	+	+	+ (для многопозиционной. системы)
Дальность действия	высокая	высокая	средняя	средняя	средняя	низкая

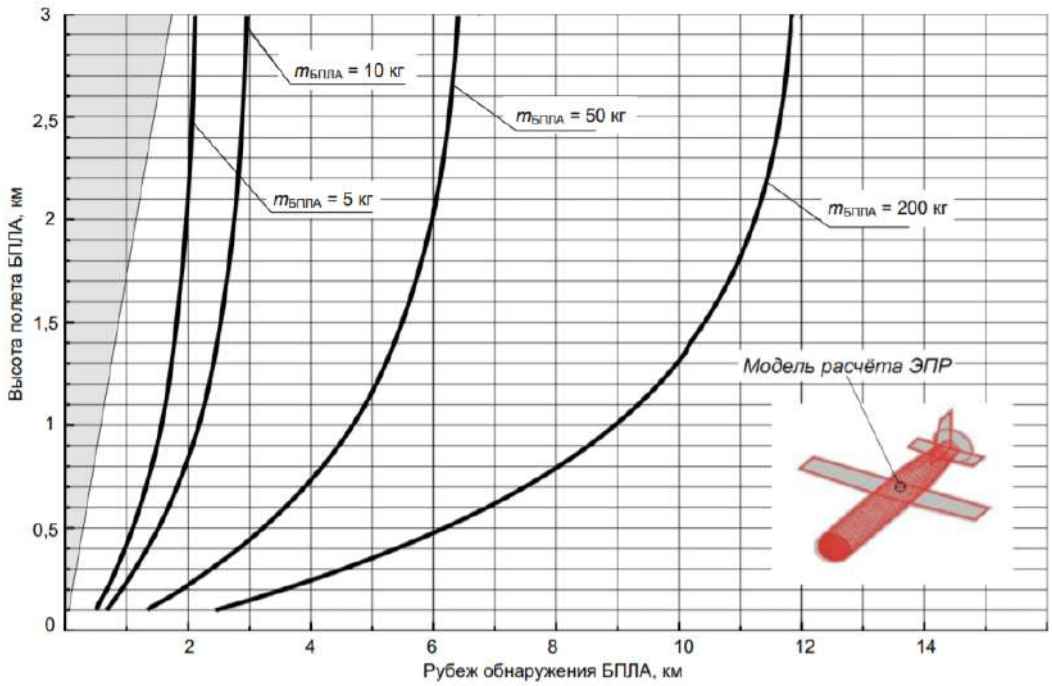


Рис. 1. Дальности обнаружения БПЛА, имеющих различные характеристики, РЛС с длиной волны λ=3 см [36]

Методы и технические средства оптического обнаружения и наблюдения БПЛА (методы и средства оптико-электронной разведки – ОЭР), работающие в видимом диапазоне волн, обеспечивают достаточно хорошие характеристики по обнаружению БПЛА, в том числе малоразмерных и малоскоростных. В то же время эффективность оптического наблюдения летательных аппаратов зависит в значительной степени от состояния атмосферы, имеющихся погодных условий и времени суток.

Наблюдение БПЛА средствами ОЭР становится возможным при обеспечении формирования проекции его визуального облика на плоскость приемной сигнальной матрицы. С этой целью используются различные способы повышения контрастности и восстановления пропущенных элементов визуального графического образа наблюдаемого объекта. Для этого может быть использовано комплексирование изображений, получаемых в различных диапазонах электромагнитного спектра [17].

Увеличение дальности наблюдения БПЛА средствами ОЭР обеспечивается путем уменьшения поля зрения, зоны обзора и увеличения времени поиска. В этом смысле средства ОЭР БПЛА в видимом диапазоне спектра не обладают значительными поисковыми возможностями и им требуются внешние целеуказания, чтобы реализовать их возможности по наблюдению и сопровождению БПЛА.

Особенности процесса наблюдения БПЛА в видимом диапазоне спектра по сравнению с пилотируемыми летательными аппаратами обусловлены незначительной контрастностью их относительно наблюдаемого фона, сравнительно небольшими габаритными размерами, отсутствием на БПЛА световых маяков, меньшей площадью отражения, отсутствием (или уменьшенным размером) факела двигателя [38]. Критерии обнаружения и распознавания БПЛА техническими средствами оптического наблюдения сформулированы в [40].

На рис. 2 представлены дальности обнаружения БПЛА средствами ОЭР, приведенные в [36]. Данные получены расчетным путем для БПЛА с различными массогабаритными характеристиками при использовании объектива, имеющего угол поля зрения 20^0 и фокусное расстояние f=230 мм. Расчет производился при коэффициенте рассеяния атмосферы в видимой области спектра $\gamma \leq 0{,}0392$, что соответствует метеорологической дальности видимости не менее 100 км.

С приведенными на рис. 2 результатами неплохо соотносится информация о дальности обнаружения БПЛА, полученная расчетным путем в [39]. Для нано-, микро- БПЛА дальность обнаружения оптическими средствами составляет 300 – 500 м; а для средних БПЛА (типа «Тахион», «Орлан») дальность находится в диапазоне 500 – 5000 м в зависимости от различных условий.

Результаты полигонных испытаний [37, 41] показывают, что средняя дальность оптического наблюдения БПЛА имеющимися средствами ОЭР при наблюдении полета БПЛА с боковых ракурсов составляет 150 – 700 м, а спереди – 100 – 400 м. Эксперименты полигонных испытаний показали, что при полете малых БПЛА на высотах 300 – 1000 м их оптическое (визуальное) обнаружение достаточно затруднительно [37, 41].

Использование средств оптического увеличения, используемых в качестве дублер-прицелов в российских зенитно-ракетных и зенитно-артиллерийских комплексах, обеспечивает увеличение дальности обнаружения БПЛА в 4,5-14 раз [37]: при использовании 4,5-кратного увеличения – до 2,2 км; при использовании 14-кратного – до 6,7 км.

Очевидно, что при использовании оптического увеличения ухудшаются поисковые возможности средств ОЭР вследствие уменьшения области обозреваемого пространства [37].

В реальных условиях прозрачность атмосферы будет меньшей, чем та, что заложена в расчетах, что, следовательно, приведет к уменьшению дальности наблюдения БПЛА, а при

наличии в атмосфере осадков, тумана, пыли оптический метод наблюдения становится практически неэффективным [36].

Дополнительным средством обнаружение БПЛА являются средства ОЭР, работающие в ИК-диапазоне, которые наиболее эффективны в ночное время.

В литературе отсутствуют данные о дальности обнаружения БПЛА с использованием тепловизионных камер в различных условиях, однако отмечается, что дальность такого метода в целом не превышает дальности наблюдения БПЛА в видимом диапазоне электромагнитных волн.

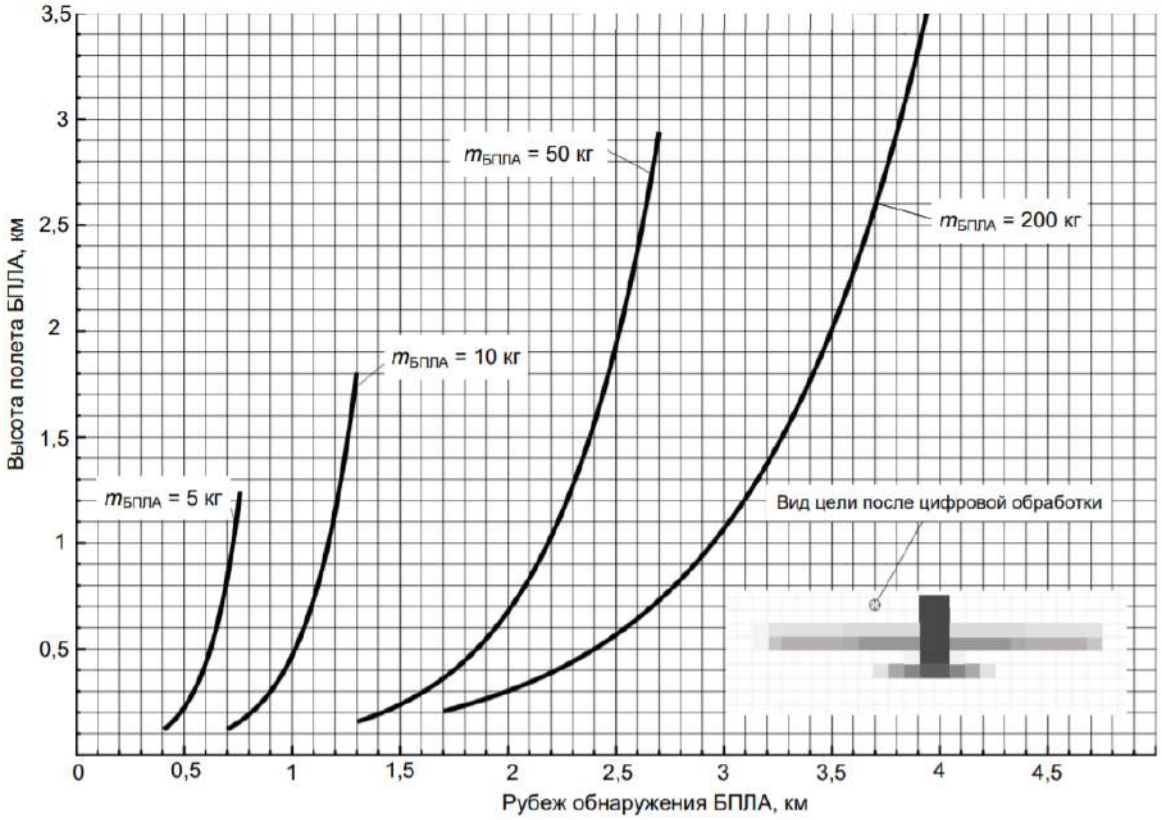


Рис. 2. Дальности обнаружения БПЛА оптическими средствами

Использование и прием акустических волн, излучаемых БПЛА в процессе полета, позволяет повысить достоверность обнаружения БПЛА в условиях, когда «традиционные» средства – оптические и радиолокационные, не могут обеспечить требуемых качественных показателей его обнаружения.

Применение средств акустической разведки (АР) позволяет [36] осуществлять обнаружение объекта, определять пеленг на БПЛА; определять класс (тип) БПЛА.

Средства АР являются пассивными по принципу действия и обладают следующими особенностями и достоинствами [42]:

- обеспечивают скрытность функционирования системы обнаружения и возможность работы в условиях интенсивного радиоэлектронного противодействия;

- обеспечивают достаточно надежное автоматическое обнаружение малоскоростных маловысотных БПЛА в условиях плохой оптической видимости, при сложных погодных условиях, в условиях сложных рельефов местности, при наличии застройки и в помещениях;

– имеют малые габаритные размеры, низкое энергопотребление и более высокие показатели по критерию «эффективность – стоимость» (в сравнении с радиолокационными и оптико-электронными средствами).

Акустические системы нашли применение в системах охраны территорий и объектов, в пограничных структурах и неплохо показали себя при обнаружении одиночных БПЛА в относительно незашумлённых условиях [36].

Основные недостатки акустических систем, которые ограничивают возможности их применения при обнаружении БПЛА, следующие [36]: сравнительно невысокая точность оценки координат БПЛА (в том числе вследствие рефракции распространения акустических волн в атмосфере); небольшие дальности обнаружения БПЛА: до 1 км по высоте и до 1,5 – 2 км по дальности.

В [39] приведены значения дальностей обнаружения БПЛА различных типов средствами АР: БПЛА с поршневым двигателем – до 2 км; вертолетный БПЛА с электрическим двигателем – 200 – 300 м; планерный БПЛА с электрическим двигателем – 100 – 200 м.

Таким образом, наилучшими поисковыми возможностями обладает радиолокационный метод, далее следуют по убывающей оптический (инфракрасный) и акустический методы. Зоны наблюдения различных методов и средств в комплексной системе графически могут быть представлены следующим образом [36] (рис. 3).

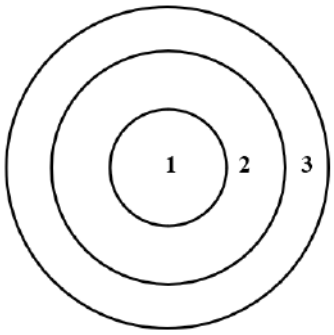
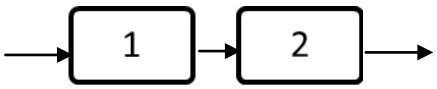


Рис. 3. Графическое представление зон обнаружения каналов комплексной системы обнаружения БПЛА: 1 – акустический канал; 2 – оптичекий канал; 3 – радиолокационный канал

Методы комплексной обработки сигналов с использованием целеуказания

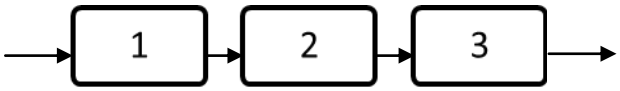
Одной из задач РЛС комплексной интегрированной системы наблюдения БПЛА является выдача координат и параметров движения целей на рубеже целеуказания с точностью, позволяющей средствам ОЭР произвести по данным целеуказания, полученным от РЛС, энергетическое обнаружение анализируемой цели без дополнительно поиска (допоиска), или, по крайней мере, ограничить зону допоиска до приемлемых пространственных объемов. Таким образом, происходит «завязывание» процесса обработки информации по каждой радиолокационной цели, выявленной РЛС, который включает все большие аппаратные, вычислительные и интеллектуальные ресурсы по мере приближения цели к охраняемому объекту, позволяя производить все более «тонкую» обработку поступающих на вход комплексной системы входных сигналов и извлекая из них все большее количество информации. В свою очередь цель, по мере приближения к охраняемому объекту, предоставляет, обеспечивает возможность для получения все большего количества информации, как бы втягиваясь в невидимую «информационную паутину».

Последовательное решение задач обнаружения и распознавания в комплексной интегрированной системе наблюдения БПЛА по мере приближения цели к охраняемому объекту отображено на рис. 4.



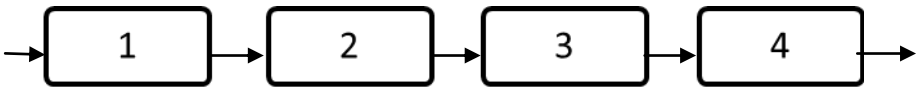
а

1 – энергетическое обнаружение в радиолокационном канале;
2 – распознавание в радиолокационном канале



б

1 – энергетическое обнаружение в радиолокационном канале;
2 – энергетическое обнаружение в оптическом канале;
3 – совместное распознавание по данным радиолокационного и оптического каналов



в

1 – энергетическое обнаружение в радиолокационном канале;
2 – энергетическое обнаружение в оптическом канале;
3 – энергетическое обнаружение в инфракрасном канале;
4 – совместное распознавание по данным радиолокационного, оптического и инфракрасного каналов

Рис. 4. Последовательность решения задач обнаружения и распознавания комплексной системой наблюдения БПЛА: *а* – в радиолокационном канале; *б* – в радиолокационном и оптическом каналах; *в* – в радиолокационном, оптическом и инфракрасном каналах

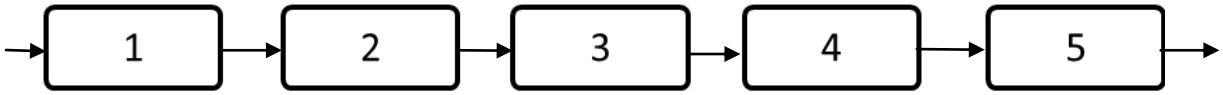
Последовательное выполнение задач обнаружения, оценки координат, целеуказания и распознавания по мере приближения цели в комплексной системе наблюдения БПЛА представлены на рис. 5.

В соответствии с представленными алгоритмами (рис. 4, 5) комплексируются каналы получения информации путем их объединения в комплексную систему, выполняющую совместную обработку полученной информации и обеспечивающую повышение основных показателей качества системы – помехозащищенности, надежности, точности измерений, вероятности правильного обнаружения и классификации (распознавания) целей [17, 23].

Многомодальная интеграция или многомодальное объединение в итоге уменьшает общую неопределенность и обеспечивает повышение точности, с которой признаки оцениваются системой. В этом случае реализуется наличие в сигналах каналов избыточной и взаимно дополняющей информации, избыточность информации также служит цели повышения надежности системы в случае появления аномальных ошибок, промахов или сбоев в каналах. Очень важно, что дополнительная информация из нескольких модальностей позволяет использовать признаки, которые невозможно однозначно воспринять и интерпретировать, имея лишь информацию от каждой модальности в отдельности. Также благодаря возможности реализовать параллельную обработку данных в используемых каналах несколько модальностей обеспечивают предоставление более оперативной информации. Подобное решение (обнаружение, распознавание), в принципе, можно получить и при использовании одного или меньшего количества информационных каналов, но для этого потребуется большее время для накопления информации.

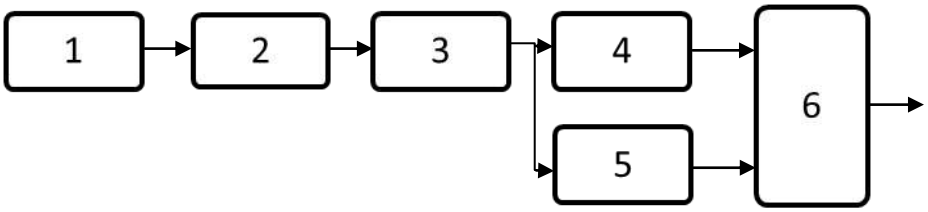
Объединение информации в комплексной системе, реализуемое в соответствии с алгоритмами (рис. 4, 5) возможно на уровне сигналов, на уровне признаков и на уровне решений [23, 32]. При этом могут быть реализованы следующие стратегии объединения данных:

- раннего объединения, реализуемые на уровне сигналов;
- раннего объединения, реализуемые на уровне признаков описания;
- позднего объединения, реализуемые на семантическом уровне принятия решения;
- гибридного объединения.



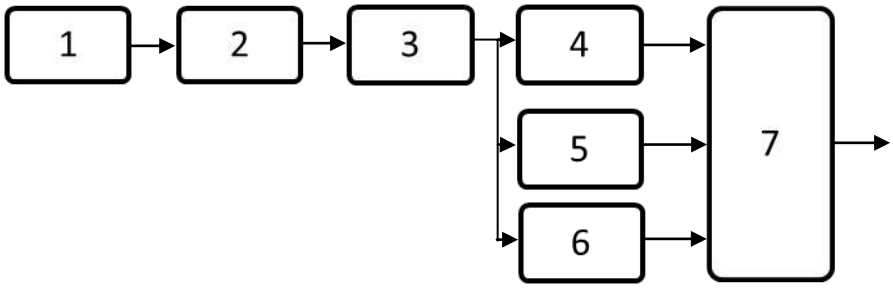
а

1 – энергетическое обнаружение в радиолокационном канале;
2 – оценка координат в радиолокационном канале;
3 – формирование целеуказания;
4 – энергетическое обнаружение в оптическом канале;
5 – совместное распознавание по данным радиолокационного и оптического каналов



б

1 – энергетическое обнаружение в радиолокационном канале;
2 – оценка координат в радиолокационном канале;
3 – формирование целеуказания;
4 – энергетическое обнаружение в оптическом канале;
5 – энергетическое обнаружение в инфракрасном канале;
6 – совместное распознавание по данным радиолокационного, оптического и инфракрасного каналов



в

1 – энергетическое обнаружение в радиолокационном канале;
2 – оценка координат в радиолокационном канале;
3 – формирование целеуказания;
4 – энергетическое обнаружение в оптическом канале;
5 – энергетическое обнаружение в инфракрасном канале;
6 – энергетическое обнаружение в акустическом канале;
7 – совместное распознавание по данным радиолокационного, оптического, акустического и инфракрасного каналов

Рис. 5. Последовательность выполнения задач обнаружения, оценки координат, целеуказания и распознавания комплексной системой наблюдения БПЛА: *а* – в радиолокационном и оптическом каналах; *б* – в радиолокационном, оптическом и инфракрасном каналах; *в* – в радиолокационном, оптическом, инфракрасном и акустическом каналах

Использование различных видов стратегии объединения, в частности стратегии гибридного объединения многомодальных сигналов информационных каналов комплексной интегрированной системы, позволяет производить эффективную обработку и объединение информации с учетом специфики решаемых данной системой задач и возможностей имеющихся в каналах технических средств.

В настоящее время открываются значительные возможности для объединения канальной информации в интегрированных системах при использовании нейронных сетевых технологий. Данные методы имеют ряд особенностей. В частности, объединение информационных каналов в этом случае осуществляется не на уровне признаков, формируемых в отдель-

ных концептах, а путем объединения имеющейся частной информации в единое мультимодальное семантическое представление (мультимодальная функция) [34].

Сигналы и результаты униполярного анализа в каналах при использовании нейронных сетей (НС) и раннего объединения сливаются до того, как соответствующие канальные представления детально изучены и сформированы соответствующие признаки. При использовании позднего слияния вначале осуществляется изучение канальной информации с помощью НС. В этом случае полученные оценки унимодальных функций образуют вектор оценок мультимодальной функции, которые далее являются входными данными для системы машинного обучения и интерпретации полученной многоканальной информации.

При использовании последовательного пространственного эшелонирования и целеуказаний в комплексной системе реализуется последовательное накопление информации из последовательно подключаемых каналов, далее осуществляется ее обработка с использованием нейросетевых либо традиционных технологий интерпретации и принятия решений.

Выводы

1. Анализ известных комплексных систем обнаружения БПЛА, реализованных в виде совокупности интегрированных информационных каналов, применяемых в них технических решений, методов и средств обработки многомодальных сигналов и изображений, показал, что известные системы и методы обработки информации не позволяют решать актуальные задачи на практике с необходимой эффективностью и требуется их дальнейшее усовершенствование.

Проблема эффективного обнаружения и противодействия БПЛА сегодня не решена, она является многогранной, сложной и требует системного подхода при ее решении.

2. Проанализированы информационные, энергетические и поисковые возможности методов и средств, входящих в состав комплексной системы обнаружения БПЛА, с целью организации целесообразной комплексной обработки сигналов с учетом естественного пространственного эшелонирования.

Показано, что наилучшими поисковыми возможностями обладает радиолокационный метод, далее следуют по убывающей оптический (инфракрасный) и акустический методы.

3. Синтезированы новые эффективные методы комплексной обработки многомодальных сигналов и изображений в интегрированной комплексной системе наблюдения беспилотных летательных аппаратов, построенные с учетом естественного пространственного эшелонирования различных информационных каналов и с использованием целеуказания. Показаны особенности объединения многомодальной информации с использованием нейросетевых технологий при использовании целеуказаний в комплексной системе.

4. Использование предложенных методов обработки и объединения многомодальной информации в комплексных интегрированных системах наблюдения БПЛА позволит осуществлять гибкое объединение разнородной информации, сигналов и изображений, получаемых в используемых каналах, с учетом возможностей имеющихся технических средств и специфики решаемых задач.

Список литературы:

1. Кошкин Р.П. Беспилотные авиационные системы. Москва : Стратегические приоритеты, 2016. 676 с.

2. Макаренко С. И., Тимошенко А. В., Васильченко А. С. Анализ средств и способов противодействия беспилотным летательным аппаратам. Ч. 1. Беспилотный летательный аппарат как объект обнаружения и поражения //Системы управления, связи и безопасности. 2020. № 1. С. 109-146. DOI: 10.24411/2410-9916-2020-10105.

3. Kartashov V.M., Oleynikov V.N, Sheyko S.A., Koryttsev I.V., Babkin S.I., Zubkov O.V. Peculiarities of small unmanned aerial vehicles detection and recognition // Telecommunications and Radio Engineering. 2019. Volume 78. Issue 9. P. 771-781.

4. Kartashov V. M., Oleynikov V. N., Sheyko S. A., Babkin S. I., Koryttsev I. V., Zubkov O. V., Anokhin M. A. Information characteristics of sound radiation of small unmanned aerial vehicles // Telecommunications and Radio Engineering. 2018, Vol.77. Iss. 10. pp. 915–924.

5. Карташов В.М., Олейников В.Н., Шейко С.А., Бабкин С.И., Корытцев И.В., Зубков О.В., Анохин М.А. Информационные характеристики звукового излучения малых беспилотных летательных аппаратов// Радиотехника. 2017. Вып. 191. С. 181-187.

6. Kartashov V., Oleynikov V., Zubkov O., Sheiko S. Optical detection of unmanned air vehicles on a video stream in a real-time // The Fourth International Conferenceon Information and Telecommunication Technologies and Radio Electronics (UkrMiCo'2019), 9-13 September 2019, Odessa, Ukraine, 4 p.

7. Oleksandr Sotnikov, Vladimir Kartashov, Oleksandr Tymochko, Oleg Sergiyenko, Vera Tyrsa, Paolo Mercorelli, Wendy Flores-Fuentes. Methods for Ensuring the Accuracy of Radiometric and Optoelectronic Navigation Systems of Flying Robots in a Developed Infrastructure. Chapter 16 // Machine Vision and Navigation; Editors: Sergiyenko**,** Oleg, Flores-Fuentes**,** Wendy**,** Mercorelli**,** Paolo; pp.537-578.

8. Oleynikov V. N , Zubkov O. V., Kartashov V. M., Korytsev I. V., Babkin S. I., Sheiko S. A. Investigation of detection and recognition efficiency of small unmanned aerial vehicles on their acoustic emission // Telecommunications and Radio Engineering, 2019, Volume 78, Issue 9; pp. 759-770.

9. Kartashov V., Oleynikov V., Koryttsev I., Zubkov O., Babkin S., Sheiko S. Processing and Recognition of Small Unmanned Vehicles Sound Signals. 2018 International Scientific-Practical Conference on Problems of Infocommunications // Science and Technology (PIC S and T 2018) – Proceedings, 31 January 2019; pp. 392-396.

10.Kartashov V., Oleynikov V., Koryttsev I., Sheyko S., Zubkov O., Babkin S., Selieznov I. Use of Acoustic Signature for Detection, Recognition and Direction Finding of Small Unmanned Aerial Vehicles // 2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), 25-29 Feb. 2020; pp. 1-4.

11.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, Iss. 9. P. 769-780.

12.Oleynikov V., Zubkov O., Kartashov V., Koryttsev I., Sheiko S., Babkin S. Experimental estimation of direction finding to unmanned air vehicles algorithms efficiency by their acoustic emission // 2019 International Scientific-Practical Conference: Problems of Infocommunications. Science and Technology (PIC S and T 2019) – Proceeding, 2019, pp. 175–178.

13.Semenets V.V., Kartashov V.M., Leonidov V.I.. Features of Acoustic Noise of Small Unmanned Aerial Vehicles // Telecommunications and Radio Engineering. 2020. Vol. 79, Iss. 11. P. 985-995. DOI: 10.1615/TelecomRadEng.v79.i11.80.

14.Тихонов В.А., Карташов В.М., Олейников В.М., Леонидов В.И., Тимошенко Л.П., Селезнев И.С., Рыбников Н.В. Обнаружение-распознавание беспилотных летательных аппаратов с использованием составной модели авторегрессии их акустического излучения // Вісник НТУУ «КПІ». Радіотехніка. Радіоапаратобудування. 2020. №81; С. 38-46.

15.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, Iss, 9. P. 769-780.

16.Kartashov V. M., Tikhonov V. A. , Voronin V. V. Features of Construction and Application of Complex Systems for the Atmosphere Remote Sounding // Telecommunications and Radio Engineering. 2017. Volume 78, Issue 8. P.743-749.

17.Карташов В.М., Олейников В.Н., Колендовская М.М., Тимошенко Л.П., Капуста А.И., Рыбников Н.В. Комплексирование изображений при обнаружении беспилотных летательных аппаратов // Радиотехника. 2020. Вып. 201. С.120-129.

18.Kartashov V.M., Tikhonov V.A., Voronin V.V., Tymoshenko L.P. Complex model of random signal in problems of acoustic sounding of atmosphere // Telecommunications and Radio Engineering. 2016. Vol. 75, Iss. 20. P. 1885-1892.

19.Developing and Applying Optoelectronics in Machine Vision**.** Oleg Sergiyenko and Julio C. Rodriguez-Quiñonez; 2016, IGI Global, 341 p.

20.Sytnik O., KartashovV. Methods and Algorithms for Technical Visionin Radar Introscopy. Chapter 13 // Optoelectronics in Machine Vision-Based Theories and Applications. IGI Global, 2019; pp. 373-391.

21.Дистанционные методы и средства исследования процессов в атмосфере Земли ; под ред. Б.Л. Кащеева, Е.Г. Прошкина, М.Ф. Лагутина. Харьков : Бизнес Информ, 2002. 426 с.

22.Карташов В.М. Модели и методы обработки сигналов систем радиоакустического и акустического зондирования атмосферы. Харьков : ХНУРЭ, 2011. 234 с.

23.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.

24.Сосулин Ю.Г. Теоретические основы радиолокации и радионавигации : учеб. пособие для вузов. Москва : Радио и связь, 1992. 304 с.

25.Карташов В.М. и др. Обработка сигналов в радиоэлектронных системах дистанционного мониторинга атмосферы. Харьков : ХНУРЭ, 2014. 312 с.

26.Koch W., Koller J., Ulmke M. Ground target tracking and road map extraction. ISPRS J. Photogramm. Remote Sens. 2006; 61:197–208. doi: 10.1016/j.isprsjprs.2006.09.013.

27.Hengy S., Laurenzis M., Schertzer S., Hommes A., Kloeppel F., Shoykhetbrod A., Geibig T., Johannes W., Rassy O., Christnacher F. Multimodal UAV detection: Study of various intrusion scenarios // Proceedings of the Electro-Optical Remote Sensing XI International Society for Optics and Photonics; Warsaw, Poland. 11–14 September 2017; p. 104340P.

28.Laurenzis M., Hengy S., Hammer M., Hommes A., Johannes W., Giovanneschi F., Rassy O., Bacher E., Schertzer S., Poyet J.M. An adaptive sensing approach for the detection of small UAV: First investigation of static sensor network and moving sensor platform // Proceedings of the Signal Processing, Sensor/Information Fusion, and Target Recognition XXVII International Society for Optics and Photonics; Orlando, FL, USA. 16–19 April 2018; p. 106460S.

29.Park S., Shin S., Kim Y., Matson E.T., Lee K., Kolodzy P.J., Slater J.C., Scherreik M., Sam M., Gallagher J.C., et al. Combination of radar and audio sensors for identification of rotor-type unmanned aerial vehicles // Proceedings of the 2015 IEEE SENSORS; Busan, Korea. 1–4 November 2015; pp. 1–4.

30.Charvat G.L., Fenn A.J., Perry B.T. The MIT IAP radar course: Build a small radar system capable of sensing range, Doppler, and synthetic aperture (SAR) imaging // Proceedings of the 2012 IEEE Radar Conference; Atlanta, GA, USA. 7–11 May 2012; pp. 0138–0144.

31.Liu H., Wei Z., Chen Y., Pan J., Lin L., Ren Y. Drone detection based on an audio-assisted camera array // Proceedings of the 2017 IEEE Third International Conference on Multimedia Big Data (BigMM); Laguna Hills, CA, USA. 19–21 April 2017; pp. 402–406.

32.Басов О.О., Карпов А.А. Анализ стратегий и методов объединения многомодальной информации // Обработка информации и управления. 2015. №2. С.7-14.

33.Карташов В.М., Куля Д.Н., Пащенко С.В. Алгоритм автосопровождения изменений информационного параметра сигнала радиоакустических систем // Восточно-европейский журнал передовых технологий. 2012. №4/9(58). С. 57-61.

34.Atrey P. K., Hossain M. A., Kankanhalli M. S. Multimoda Fusion for Multimedia Analysis: a Survey // Multimedia Systems. 2010. Vol. 16. Iss. 6. P. 345–379.

35.Countering rogue drones. FICCI Committee on Drones, EY, 2018; 31 p.

36. Ростопчин В. В. Ударные беспилотные летательные аппараты и противовоздушная оборона – проблемы и перспективы противостояния // Беспилотная авиация [Электронный ресурс]. 2020. URL: https://www.researchgate.net/publication/331772628_Udarnye_ bespilotnye_letatelny e_apparaty _i_protivovozdusnaa_oborona_-problemy_i_perspektivy_ protivostoania (дата обращения 18.10.2020).

37. Еремин Г. В., Гаврилов А. Д., Назарчук И. И. Малоразмерные беспилотники – новая проблема для ПВО // Отвага [Электронный ресурс]. 29.01.2015. № 6 (14). – URL: http://otvaga2004.ru/armiya-i-vpk/armiya-i-vpkvzglyad/malorazmernye-bespilotniki/ (дата доступа 18.10.2020).

38.Ананенков А. Е., Марин Д. В., Нуждин В. М., Расторгуев В. В., Соколов П. В. К вопросу о наблюдении малоразмерных беспилотных летательных аппаратов // Труды МАИ. 2016. № 91. С. 19.

39. Изделия и комплексы противодействия беспилотным летательным аппаратам [Доклад]. СПб. : АО «НИИ «Вектор», 2018. 51 с.

40. Годунов А. И., Шишков С. В., Бикеев Р. Р. Взаимосвязь машинного (технического) зрения с компьютерным зрением при идентификации малогабаритного беспилотного летательного аппарата // Труды международного симпозиума «Надежность и качество». 2015. Т. 1. С. 213-217.

41. Зайцев А. В., Назарчук И. И., Красавцев О. О., Кичулкин Д. А. Особенности борьбы с тактическими беспилотными летательными аппаратами // Военная мысль. 2013. № 5. С. 37-43.

42. Гейстер С. Р., Джеки А. М. Решение задачи обнаружения маловысотных легкомоторных летательных аппаратов путем использования акустических и сейсмических полей // Наука и военная безопасность. 2008. № 1. С. 42-46. URL: http://militaryarticle.ru/nauka-i-voennayabezopasnost/2008/12105-reshenie-zadachi-obnaruzhenija-malovysotnyh (дата обращения 18.10.2020).

43. Ситнік О.В., Карташов В.М. Радіотехнічні системи : навч. посібник. Харків : Сміт, 2009. 448 с.

44. Shirman Y.D., Manzhos V.N. The theory and technique of processing radar information against the background of interference. Moskva : Radio and communications, 1981. 416 p.

Поступила в редколлегию 30.10.2020

Сведения об авторах:

Карташов Владимир Михайлович – д-р техн. наук, профессор, заведующий кафедрой медиаинженерии и информационных радиоэлектронных систем, Харьковский национальный университет радиоэлектроники, Украина; e-mail: volodymyr.kartashov@nure.ua, ORCID: https://orcid.org/0000-0001-8335-5373

Олейников Владимир Николаевич – канд. техн. наук, доцент, профессор кафедры медиаинженерии и информационных радиоэлектронных систем, Харьковский национальный университет радиоэлектроники, Украина; e-mail: vladimir.oleinikov@nure.ua, ORCID: https://orcid.org/0000-0001-7197-9760

Леонидов Владимир Иванович – канд. техн. наук, с. н. с. кафедры биомедицинской инженерии, Харьковский национальный университет радиоэлектроники, Украина; e-mail:volodymyr.leonidov@nure.ua, ORCID: https://orcid.org/0000-0001-5218-3177

Воронин Виталий Валериевич – канд. техн. наук, преподаватель радиотехнических дисциплин, Светловодский политехнический коледж Центральноукраинского национального технического университета, Украина; e-mail: vvvoronin2016@gmail.com, ORCID: https://orcid.org/0000-0002-4495-9024

Капуста Анастасия Игоревна – аспирант кафедры медиаинженерии и информационных радиоэлектронных систем, Харьковский национальный университет радиоэлектроники, Украина; e-mail: anastasiia.kapusta@nure.ua, ORCID: https://orcid.org/0000-0003-2206-1552

Селезнёв Иван Сергеевич – аспирант кафедры медиаинженерии и информационных радиоэлектронных систем, Харьковский национальный университет радиоэлектроники, Украина, ORCID: https://orcid.org/0000-0002-0731-7540

Першин Евгений Васильевич – аспирант кафедры медиаинженерии и информационных радиоэлектронных систем, Харьковский национальный университет радиоэлектроники, Украина; e-mail: yevhenii.pershyn@nure.ua, ORCID: https://orcid.org/0000-0002-4573-9381

УДК 621.396.96:004.045 **DOI:10.30837/rt.2020.4.203.16**

І.В. СВИД, канд. техн. наук, І.І. ОБОД, д-р техн. наук,
Г.Е. ЗАВОЛОДЬКО, канд. техн. наук

ОПТИМІЗАЦІЯ ОБРОБКИ ДАНИХ В ЛІТАКОВИХ ВІДПОВІДАЧАХ СИСТЕМИ ІДЕНТИФІКАЦІЇ «СВІЙ-ЧУЖИЙ»

Вступ

Система ідентифікації «свій-чужий» [1, 2] забезпечує спостереження за повітряними об'єктами (ПО), обладнаними літаковими відповідачами (ЛВ) і забезпечує двосторонній зв'язок за каналом передачі даних між наземними станціями і повітряними об’єктами [3]. Система ідентифікації «свій-чужий» відноситься до основних інформаційних джерел як системи контролю повітряного простору [4], так і системи управління повітряним рухом [5]. Система ідентифікації «свій-чужий» повинна вирішувати завдання ідентифікації повітряного об'єкту за ознакою «свій-чужий» як в інтересах визначення ступеня небезпеки виявленого повітряного об'єкта, так і при безпосередньому застосуванні зброї. Рішення завдання радіолокаційної ідентифікації за ознакою «свій-чужий» полягає в ухваленні рішення про виявлення повітряного об'єкта системою ідентифікації «свій-чужий». Імітостійка (криптографічна) ідентифікація повітряних об'єктів, що реалізована в існуючих системах ідентифікації «свій-чужий» [1, 2], дозволяє однозначно вирішити питання за ознакою «свій-чужий» і є важливою умовою функціонування єдиного інформаційно-комунікаційного простору. Найбільш вразливим місцем в системах ідентифікації «свій-чужий», що істотно обмежує можливість ідентифікації повітряних об'єктів є літаковий відповідач [6 – 9]. Він побудований за принципом відкритої одноканальної системи масового обслуговування з відмовами [10, 11], що викликає труднощі при роботі останніх при значних щільностях потоків внутрісистемних завад [12, 13]. Така побудова літакового відповідача викликає суттєві недоліки в безпеці як його, так і безпеки всієї системи ідентифікації «свій-чужий». Це зазначається в значному числі робіт, зокрема в [14 – 16]. Використання ж єдиної частоти у запитальному каналі в системах, що розглядаються, призводить до високої щільності запитуючих сигналів і, як наслідок, до внутрістемних завад [17 – 18] значної інтенсивності. Зазначені фактори призводять до зниження якості обробки сигнальних даних. Так, в роботі [17] наводиться характеристика середовища щодо оцінки характеристик сучасних вторинних радіолокаційних приймачів спостереження. Основна увага приділяється параметрам, що надають точну характеристику явищ завад, які суттєво обмежують продуктивність даної системи. В роботі [18] розглядаються питання оптимального виявлення сигналів запиту (СЗ) при однакових рівнях як сигналів запиту, так і завад, які надходять на літаковий відповідач, що представляє собою ідеальний випадок.

Побудова ЛВ за принципом одноканальної системи обслуговування сигналів запиту з відмовами визначило часову паралізацію ЛВ на час обслуговування попереднього сигналу відповіді, що призводить до суттєвих обмежень відносної пропускної здатності ЛВ [10, 11], і це необхідно враховувати при оптимізації обробки даних в ЛВ.

Антенна система літакового відповідача утворена значною кількістю слабонаправлених антен [19 – 22], що розширює можливості щодо оптимізації обробки даних ЛВ за часовими і просторовими параметрами.

Наявність багатоканальності в прийомі сигналів запиту розширює структурні можливості при синтезі оптимальних виявлювачів сигналів запиту, зокрема при об'єднанні попередніх рішень в каналах виявлення сигналів запиту [23, 24]. Так, в існуючих ЛВ загалом реалізується квазіоптимальний виявлювач сигналів запиту під час багатоканального прийому з об'єднанням канальних рішень виявлення сигналів запиту.

При синтезі та аналізі оптимальної структури обробки сигнальних даних у літакових відповідачах систем ідентифікації «свій-чужий» враховується багатоканальність прийому сигналів запиту та обмеження відносної пропускної здатності літакового відповідача [25 – 28].

Синтез оптимальної структури обробки сигнальних даних в літакових відповідачах систем ідентифікації «свій-чужий»

Наявність багатоканальності в прийомі сигналів запиту зумовлює і багатоканальність структури детектора сигналів запиту. Це обумовлено наявністю значної кількості антен систем ідентифікації «свій-чужий» на повітряному об’єкті, які працюють на прийом сигналів запиту і також випромінюють сигнали відповіді (СВ). Зокрема, на винищувачах кількість антенних систем не менше чотирьох. Після порогових пристроїв і дешифраторів прийняті сигнали підсумовуються елементом об'єднання. При цьому слід враховувати, що параметри сигналів запиту, прийнятих різними антенними системами, суттєво відрізняються, що слід враховувати при реалізації виявлювачів сигналів запиту в ЛВ. Крім того, в існуючих алгоритмах обробки даних ЛВ об'єднанню підлягають попередні рішення про виявлення СЗ, здійснені дешифратором, тобто квазіоптимальним детектором. Однак, СЗ, як відомо [4, 5], мають кілька простих сигналів без внутріімпульсної модуляції, часова розстановка яких і визначає код СЗ. Ці обставини дозволяють розглядати питання оптимізації обробки в двох напрямках:

- виявлення СЗ з ваговим міжканальним об'єднанням канальних рішень про виявлення СЗ;
- виявлення СЗ з ваговим міжканальним об'єднанням канальних імпульсів СЗ.

Будемо вважати, що число каналів прийому сигналів запиту становить M, а кількість імпульсів, що утворюють сигнал запиту становить n, що є значністю коду сигналу запиту. Отримаємо загальний алгоритм виявлення сукупності одиночних рішень і, на основі отриманого алгоритму, розглянемо структури обробки сигналів запиту в ЛВ при зазначених вище напрямках оптимізації обробки.

У кожному каналі обробки СЗ в ЛВ прийняті сигнали, після оптимальної лінійної обробки і детектування, порівнюються в пороговому пристрої (ПП) з порогом виявлення, який визначає ймовірність хибної тривоги. Після ПП на подальшу обробку надходить реалізація $x_{ij}=1$, за умови, що в елементі часового дозволу $(i=\overline{1,M})$ і $(j=\overline{1,n})$, який відповідає аналізованому просторовому дозволу, відбулося перевищення порога; в іншому випадку $x_{ij}=0$. Для прийняття рішення про наявність або відсутність сигналу запиту під час спільної міжканальної обробки подається сукупність нулів та одиниць x_{ij}. В даному випадку очевидно, що x_{ij} – випадкова величина, яка підпорядковується розподілу Бернуллі

$$P\left(x_{ij}\right)=P_0P_{ij}^{x_{ij}}\left(1-P_0P_{ij}\right)^{1-x_{ij}}, \qquad (1)$$

де P_{ij} – ймовірність перевищення порога в ij-му каналі обробки сигнальних даних, P_0 – відносна пропускна здатність ЛВ. При відсутності сигналу $P_{ij}=F_{ij}$ – ймовірність хибної тривоги, а при наявності сигналу запиту $P_{ij}=D_{ij}$ – ймовірність виявлення.

Задачу оптимальної обробки сигнальних даних можна розглядати в різних постановках. В детекторі СЗ, що розглядається, можливе управління напругою порога спрацьовування вихідного порогового пристрою, а також напругою порога канальних порогових пристроїв. Отримаємо характеристики детектора СЗ при управлінні величиною порога на вихідному ПП. Імовірність помилкової тривоги й правильного виявлення СЗ в каналах обробки будемо вважати заданими (хоча і довільні).

Припустимо, що на вхід пристрою спільної обробки прийнятих сигналів надходить наступна сукупність випадкових величин x_{ij}. Спільні розподіли ймовірностей всіх можливих комбінацій x_{ij} як у відсутності, так і при наявності сигналу запиту (гіпотези H_0 і H_1), тобто $P\left(x_{ij}\middle|H_0\right)$ і $P\left(x_{ij}\middle|H_1\right)$ довільні, проте відомі. В цьому випадку для кожної конкретної сукупності можна сформувати відношення правдоподібності у вигляді

$$\Lambda = P\left(x_{ij}\middle|H_1\right)\Big/P\left(x_{ij}\middle|H_0\right). \tag{2}$$

Шляхом порівняння відношення правдоподібності Λ із заданим порогом, який визначається виходячи з допустимої ймовірності хибної тривоги, забезпечується оптимальне, за критерієм Неймана – Пірсона, рішення про наявність або відсутність сигналу.

Припускаючи незалежність шумів у каналах обробки даних можна записати

$$P(x_{ij}\mid H_0) = \prod_{i=1,\,j=1}^{M,n} D_{ij}^{x_{ij}}\left(1-D_{ij}\right)^{1-x_{ij}}. \tag{3}$$

Можна припустити, що при впливі корисного сигналу перевищення порога виявлення в каналах обробки – незалежні події. В цьому випадку можна записати

$$P(x_{ij}\mid H_1) = \prod_{i=1,\,j=1}^{M,n} D_{ij}^{x_{ij}}\left(1-D_{ij}\right)^{1-x_{ij}}. \tag{4}$$

З урахуванням виразів (3) і (4) вираз (2) можна записати в наступному вигляді

$$\Lambda = \prod_{i=1,\,j=1}^{M,n} D_{ij}^{x_{ij}}\left(1-D_{ij}\right)^{1-x_{ij}} \Bigg/ \prod_{i=1,\,j=1}^{M,n} D_{ij}^{x_{ij}}\left(1-D_{ij}\right)^{1-x_{ij}}. \tag{5}$$

Здійснивши логарифмування виразу (5) отримуємо

$$L = \ln\Lambda = \sum_{i=1,\,j=1}^{M,n} x_{ij}\left(\ln D_{ij} - \ln F_{ij}\right) + \left(1-x_{ij}\right)\left[\ln\left(1-D_{ij}\right) - \ln\left(1-F_{ij}\right)\right]. \tag{6}$$

Якщо позначити множники при x_{ij} у виді

$$Q_{ij} = \ln D_{ij} - \ln F_{ij} - \ln\left(1-D_{ij}\right) + \ln\left(1-F_{ij}\right) = D_{ij}\left(1-F_{ij}\right)\Big/\left(1-D_{ij}\right)F_{ij} \tag{7}$$

і відкинути доданки, що не залежать від реалізацій x_{ij}, отримаємо оптимальний за критерієм Неймана – Пірсона алгоритм виявлення сигналів запиту при об'єднанні даних попередніх рішень виявлення сигналів або імпульсів всіх каналів обробки ЛВ

$$L = \sum_{i=1}^{M}\sum_{j=1}^{n} Q_{ij}x_{ij} \underset{<}{\overset{>}{}} z_0, \tag{8}$$

де z_0 – поріг, який визначає вихідну ймовірність помилкової тривоги F.

Таким чином, оптимальна спільна обробка СЗ зводиться до вагового підсумовування одиниць і нулів x_{ij}, які відображають прийняті в каналах обробки даних попередні рішення. Вагові коефіцієнти, що визначаються відповідно до виразу (7), підвищують роль того каналу обробки даних, де вища ймовірність правильного виявлення D_{0ij} і нижче ймовірність хибної

тривоги F_{0ij}. Вагові коефіцієнти (7) є функцією як відношення сигнал/шум, так і рівня шумів в різних каналах обробки ЛВ.

Так як x_{ij} може бути 0 або 1, тоді ліва частина виразу (8) є сумою $k < Mn$ вагових коефіцієнтів Q_{ij} та може приймати тільки певні дискретні значення. Значення порога z_0 в цьому випадку буде лежати в межах $0 < z_0 < \sum_{i=1}^{M} \sum_{j=1}^{n} Q_{ij}$, для того, з одного боку, щоб завжди не приймалося рішення про виявлення СЗ, а з іншого боку – тривіальне рішення про пропуск СЗ.

Якщо розглядати ситуацію, коли всі вагові коефіцієнти Q_{ij} різні й сума будь-якої групи Q_{ij} не співпадає з сумою будь-якої іншої їх групи, то при різних комбінаціях значень x_{ij} для розглянутого випадку можливі тільки $2^M - 1$ різних правил виявлення СЗ.

Зазначимо, що на практиці підсумовування складових імпульсів СЗ в каналах обробки здійснюється без вагових коефіцієнтів через припущення про однакові відношення сигнал/шум і рівня завад в каналі обробки. Це дещо спрощує алгоритм обробки СЗ. Підсумовування без ваг нулів і одиниць в каналах обробки і заміна виявлювача СЗ дешифратором не призводить до суттєвих втрат в пороговому відношенні сигнал/шум.

При зазначених припущеннях вираз (8) можна записати як:

- при міжканальному злитті результатів виявлення СЗ

$$L = \sum_{i=1}^{M} Q_i \times \left(x_i = \prod_{j=1}^{n} x_j \right) \underset{<}{>} z_0, \tag{9}$$

- при міжканальному злитті результатів виявлення складових імпульсів СЗ

$$L = \prod_{j=1}^{n} x_j = \left(\sum_{i=1}^{M} Q_i x_i \underset{<}{>} z_0 \right). \tag{10}$$

Отримані вирази (9) і (10) дозволяють реалізувати структури обробки даних СЗ для зазначених ситуацій міжканального злиття попередніх канальних рішень про виявлення сигналів запиту або імпульсних складових сигналів запиту. У синтезованих виявлювачах є три порогових пристрої: перший – пороговий пристрій з аналоговим порогом, де здійснюється виявлення імпульсів СЗ, другий – в дешифраторі (цифровий поріг) і третій – при виявленні об'єднаних імпульсів (сигналів) (цифровий поріг).

Отже, оптимізація обробки СЗ в ЛВ зводиться до вибору для спільної обробки даних одного з вирішальних правил, яке задовольняє алгоритму (8), (9) та (10), а також до установки однакових відносних порогів в каналах обробки СЗ ЛВ, які забезпечують такі значення F_i, що при обраному вирішальному правилі дають необхідне значення результуючої ймовірності F_i.

Аналіз оптимальної структури обробки даних в літакових відповідачах систем ідентифікації «свій-чужий»

Розрахунок показників якості обробки даних СЗ відповідно до виразів (9) і (10) відносно складний і викликає деякі труднощі. Складність викликана необхідністю розгляду відмінностей завадових коливань і відношень сигнал/шум в кожному з каналів обробки даних. У зв'язку з цим розглянемо ситуацію, при якій можна вважати, що в кожному каналі обробки відношення сигнал/шум однакові. При таких умовах вагові коефіцієнти внутріканального і міжканального злиття однакові, а розрахункові вирази для показників

якості виявлення кілька спрощуються. При розрахунках будемо припускати, що число просторових каналів обробки даних становить M .

Розрахунки виявлення СЗ в ЛВ при значності коду запиту $n=3$ представлені на рис. 1, 2, а для $n=2$ – на рис. 3, 4. Неперервні криві визначають зазначені залежності для міжканального злиття результатів виявлення СЗ, а пунктирні – для міжканального злиття результатів виявлення складових імпульсів СЗ. Розрахунки отримані при $F=10^{-4}$. Число просторово-рознесених каналів обробки даних M склало 2, 3, 4. Представлені залежності показують, що міжканальне злиття результатів виявлення складових імпульсів СЗ дещо краще порівняно з міжканальним злиттям результатів виявлення СЗ.

На рис. 1 представлена залежність $D=f(q,n=3,M,P_0=1)$. Представлені залежності показують, що міжканальне злиття результатів виявлення складових імпульсів СЗ більш переважне. Так при $q=2,8$ ймовірність виявлення сигналів запиту в ЛВ становить відповідно 0,6 $(M=2)$; 0,73 $(M=3)$ і 0,81 $(M=4)$, в той час як для міжканального злиття результатів виявлення СЗ ці ймовірності відповідно дорівнюють 0,5 $(M=2)$; 0,61 $(M=3)$ і 0,68 $(M=4)$.

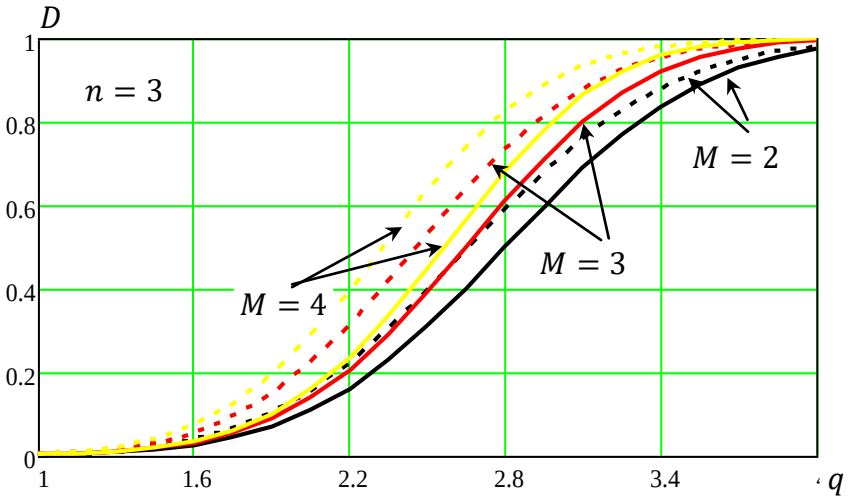


Рис. 1. Виявлення сигналів запиту в літаковому відповідачі при *n*=3

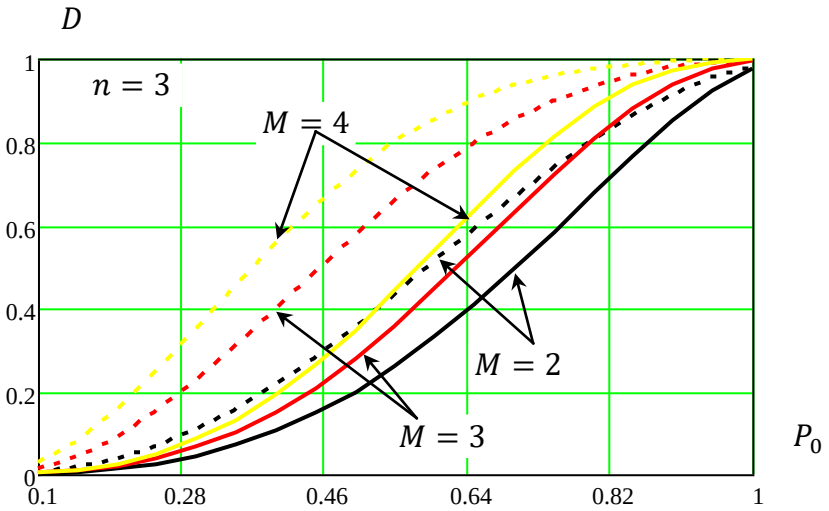


Рис. 2. Виявлення сигналів запиту в літаковому відповідачі при *n*=3

На рис. 2 представлена залежність $D = f(P_0, n = 3, M, q = 4)$. Представлені залежності показують, що міжканальне злиття результатів виявлення складових імпульсів СЗ також більш переважне. Дійсно, при $P_0 = 0,64$ ймовірність виявлення СЗ в ЛВ становить відповідно 0,58 $(M = 2)$; 0,79 $(M = 3)$ и 0,9 $(M = 4)$, в той час як для міжканального злиття результатів виявлення СЗ ці ймовірності відповідно рівні 0,4 $(M = 2)$; 0,52 $(M = 3)$ і 0,61 $(M = 4)$.

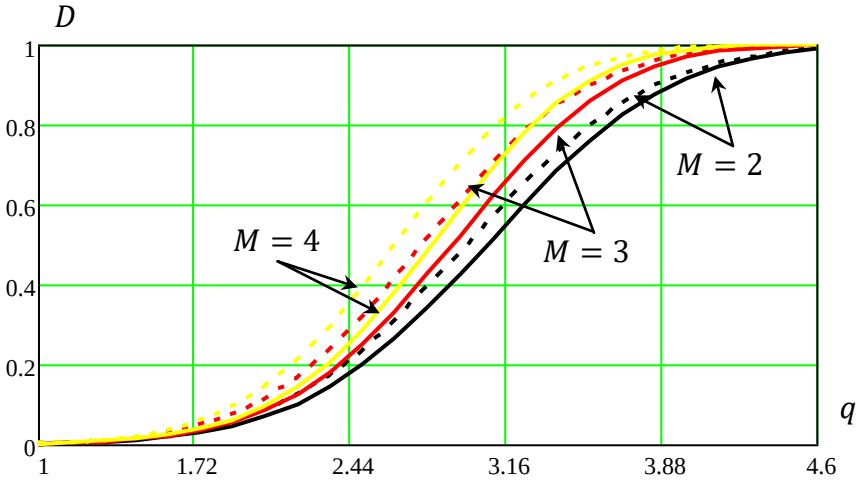


Рис. 3. Виявлення сигналів запиту в літаковому відповідачі при *n*=2

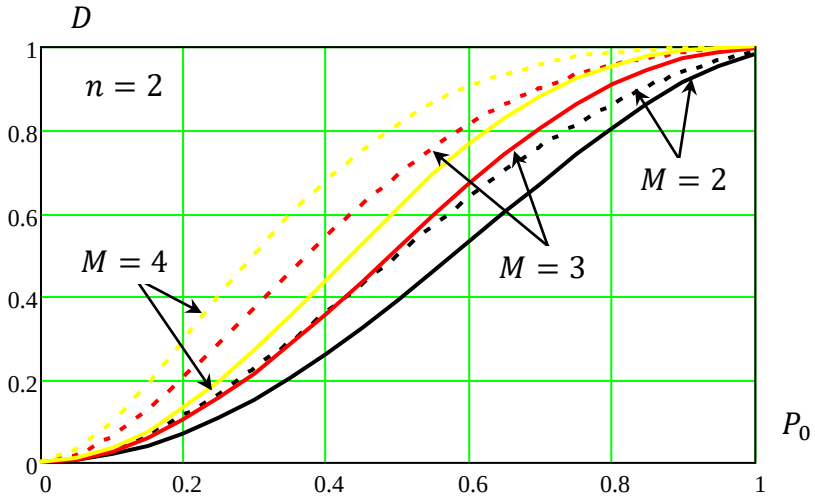


Рис. 4. Виявлення сигналів запиту в літаковому відповідачі при *n*=2

На рис. 3 представлена залежність $D = f(q, n = 2, M, P_0 = 1)$. Представлені залежності показують, що міжканальне злиття результатів виявлення складових імпульсів СЗ більш переважне. Так, при $q = 3,16$ ймовірність виявлення сигналів запиту в ЛВ становить відповідно 0,6 $(M = 2)$; 0,74 $(M = 3)$ і 0,81 $(M = 4)$, в той час як для міжканального злиття результатів виявлення СЗ ці ймовірності відповідно дорівнюють 0,55 $(M = 2)$; 0,62 $(M = 3)$ і 0,71 $(M = 4)$.

На рис. 4 представлена залежність $D = f(P_0, n = 3, M, q = 4,5)$. Представлені залежності показують, що міжканальне злиття результатів виявлення складових імпульсів СЗ також більш переважне. Дійсно, при $P_0 = 0,6$ ймовірність виявлення сигналів запиту в ЛВ становить відповідно 0,62 $(M = 2)$; 0,81 $(M = 3)$ і 0,92 $(M = 4)$, в той час як для міжканального злиття результатів виявлення СЗ ці ймовірності відповідно дорівнюють 0,54 $(M = 2)$; 0,67 $(M = 3)$ і 0,77 $(M = 4)$.

Висновки

Отримані результати дозволяють зробити наступні висновки:

- міжканальне об'єднання даних результатів виявлення складових імпульсів сигналу запиту дозволяє отримати переваги в пороговому відношенні сигнал/шум в порівнянні з міжканальним об'єднанням даних результатів виявлення сигналів запиту, тобто існуючим алгоритмом злиття результатів виявлення сигналів запиту, так як дозволяють підвищити якість виявлення сигналів запиту і знизити залежність ймовірності виявлення сигналів запиту від відносної пропускної здатності літакового відповідача;
- збільшення значності коду використовуваних сигналів запиту систем ідентифікації «свій-чужий» дозволяє підвищити ймовірність виявлення їх в літаковому відповідачі;
- вплив відносної пропускної здатності літакового відповідача більше відчувається при збільшенні значності коду сигналу запиту.

Список літератури:

1. STANAG 4193 Document, Technical Characteristics Of IFF Mk X And Mk XII Interrogators And Transponders (Part V) – Technical Description Of The MkXII System, NATO Standard, 2016.
2. Маляренко А.С. Системы вторичной радиолокации для управления воздушным движением и государственного радиолокационного опознавания : справочник. Харьков: ХУПС, 2007. 78 с.
3. Uzan S. Turan, and S. A. Colak. IFF system simulator design based on DSP // 2016 24th Signal Processing and Communication Application Conference, SIU 2016 – Proceedings, 2016, pp. 1-4.
4. Stevens Brian L., Frank L. Lewis, and Eric N. Johnson. Aircraft control and simulation: dynamics, controls design, and autonomous systems. John Wiley & Sons, 2015.
5. Benelli G., Giuli D., Mese E. and Pardini S. Characterization of ATC environment for performance evaluation of modern SSR systems // 29th IEEE Vehicular Technology Conference, Arlington Heights, Illinois, USA, 1979, pp. 370-377, doi: 10.1109/VTC.1979.1622720.
6. 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.
7. Martin Strohmeier. Large-Scale Analysis of Aircraft Transponder Data // IEEE Aerospace and Electronic Systems Magazine (Volume: 32, Issue: 1, January 2017). P. 42 – 44. doi: 10.1109/MAES.2017.160149.
8. Mauro Leonardi; Davide Di Fausto. Secondary Surveillance Radar Transponders classification by RF fingerprinting // 2018 19th International Radar Symposium (IRS). doi: 10.23919/IRS.2018.8448244.
9. David S. and Vitolo A. J., Airborne IFF transponder antenna system with Omni and steerable cardioid patterns, Aug. 1970, pp. 279-283.
10. 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), Lviv, Ukraine, 2019, pp. 73-77. doi: 10.1109/UKRCON.2019.8879812.
11. Obod I., Svyd I., Maltsev O. and Bakumenko B. Comparative Analysis of Noise Immunity Systems Identification Friend or Foe // 2020 IEEE 40th International Conference on Electronics and Nanotechnology (ELNANO), Kyiv, Ukraine, 2020, pp. 751-756. doi: 10.1109/ELNANO50318.2020.9088856.
12. NTIA, Compendium for 960–1164 MHz. NTIA, 2014.
13. Otsuyama T., Honda 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), Singapore, 2018, pp. 71-71. doi: 10.1109/ISEMC.2018.8394048.
14. Pollack J. and Ranganathan P. Aviation Navigation Systems Security: ADS-B, GPS, IFF // International Conference on Security & Management, SAM'18, International Conference on Security & Management, SAM'18, Las Vegas, Nevada, USA, 2018, pp. 129-135.

15. Strelnytskyi O., Svyd I., Obod I., Maltsev O., Voloshchuk O. and Zavolodko G. Assessment Reliability of Data in the Identification Friend or Foe Systems // 2019 IEEE 39th International Conference on Electronics and Nanotechnology (ELNANO), Kyiv, Ukraine, 2019, pp. 728-731, doi: 10.1109/ELNANO.2019.8783397.

16. Svyd I., Obod I., Maltsev O., Strelnytskyi O., Zubkov O. and Zavolodko G. Method of Increasing the Identification Friend or Foe Systems Information Security // 2019 3rd International Conference on Advanced Information and Communications Technologies (AICT), Lviv, Ukraine, 2019, pp. 434-438, doi: 10.1109/AIACT.2019.8847853.

18. Federal Aviation Administration, DOT, "Automatic Dependent Surveillance-Broadcast (ADS-B) Out Performance Requirements to Support Air Traffic Control (ATC) Service; Technical Amendment. Final rule; technical amendment // Federal Aviation Administratio, Renton, Washington, 2015.

19. Svyd I., Obod I., Maltsev O., Shtykh I., Maistrenko G. and Zavolodko G. Comparative Quality Analysis of the Air Objects Detection by the Secondary Surveillance Radar // 2019 IEEE 39th International Conference on Electronics and Nanotechnology (ELNANO), Kyiv, Ukraine, 2019, pp. 724-727, doi: 10.1109/ELNANO.2019.8783539.

20. Sharifi-Tehrani O., Sadeghi A. and Razavi S. M. J. Design and Simulation of IFF/ATC Antenna for Unmanned Aerial Vehicle // Majlesi Journal of Mechatronic Systems, vol. 6, no. 1, Jun. 2017.

21. Kolosowski W., Sedek E., Borejko M. and Jeziorski A. Monopulse IFF antennas. // MIKON 2008 – 17th International Conference on Microwaves, Radar and Wireless Communications, Wroclaw, 2008, pp. 1-4.

22. Coleman H. and Wright B. A compact flush-mounting antenna with direction finding and steerable cardioid pattern capability // IEEE Transactions on Antennas and Propagation, vol. 32, no. 4, pp. 412-414, 1984. doi: 10.1109/tap.1984.1143319.

23. Obod I., Svyd I., Maltsev O., Vorgul O., Maistrenko G. and Zavolodko G. Optimization of the Quality of Information Support for Consumers of Cooperative Surveillance Systems. In: Radivilova T., Ageyev D., Kryvinska N. (eds) Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies, vol 48. Springer, Cham, pp. 133-155, 2021. doi: 10.1007/978-3-030-43070-2_8.

24. Obod I., Svyd I., Maltsev O., Zavolodko G., Pavlova D. and Maistrenko G. Fusion the Coordinate Data of Airborne Objects in the Networks of Surveillance Radar Observation Systems. In: Radivilova T., Ageyev D., Kryvinska N. (eds) Data-Centric Business and Applications // Lecture Notes on Data Engineering and Communications Technologies, vol 48. Springer, Cham, pp. 731-746, 2021. doi: 10.1007/978-3-030-43070-2_31.

25. Poornima P., Roja Reddy B. and Anantha Murthy B. G. Design and Simulation of Two-Chain Monopulse Receiver for IFF Radar Application // 2018 3rd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), Bangalore, India, 2018, pp. 1114-1118. doi: 10.1109/RTEICT42901.2018.9012646.

26. 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), Kyiv, Ukraine, 2020, pp. 336-340. doi: 10.1109/DESSERT50317.2020.9125040.

27. Svyd, I.V., Obod, A.I., Zavolodko, G.E., Melnychuk, I.M., Wójcik, W., Orazalieva, S., Ziyatbekova, G. Assessment of information support quality by "friend or foe" identification systems // PRZEGLĄD ELEKTROTECHNICZNY, vol. 1, no. 4, pp. 129-133, 2019. doi: 10.15199/48.2019.04.22.

28. Svyd I., Obod I., Maltsev O., Shtykh I. and ZavolodkoG. 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), Polyana, Ukraine, 2019, pp. 1-4, doi: 10.1109/CADSM.2019.8779322.

Надійшла до редколегії 28.30.2020

Відомості про авторів:

Свид Ірина Вікторівна – кандидат технічних наук, доцент, завідувач кафедри мікропроцесорних технологій і систем, Харківський національний університет радіоелектроніки, Україна; email: iryna.svyd@nure.ua, ORCID: http://orcid.org/0000-0002-4635-6542

Обод Іван Іванович – доктор технічних наук, професор, професор кафедри мікропроцесорних технологій і систем, Харківський національний університет радіоелектроніки, Україна; email: ivan.obod@nure.ua; ORCID: https://orcid.org/0000-0002-9898-0937

Заволодько Ганна Едвардівна – кандидат технічних наук, доцент, докторант кафедри мікропроцесорних технологій і систем, Харківський національний університет радіоелектроніки, Україна; email: ganna.zavolodko@nure.ua; ORCID: https://orcid.org/0000-0003-0000-8910

УДК 537.862 **DOI:10.30837/rt.2020.4.203.17**

М.И. ДЗЮБЕНКО, д-р физ.-мат. наук, В.А. МАСЛОВ, д-р физ.-мат. наук,
В.П. РАДИОНОВ, канд. физ.-мат. наук, А.А. ФОМИН

СПОСОБЫ РЕГУЛИРОВКИ ОБРАТНОЙ СВЯЗИ В ЛАЗЕРАХ ТЕРАГЕРЦЕВОГО ДИАПАЗОНА

Введение

Оптимальный коэффициент обратной связи является важным условием высокой эффективности лазерной генерации. Максимальная эффективность лазера, как и любого генератора, достигается только при оптимальной обратной связи. При увеличении доли излучения, выводимого из резонатора, снижается доля стимулированного излучения и увеличивается доля спонтанного излучения, вплоть до того, что лазерная генерация может вообще не возникать. Уменьшение доли выводимого излучения может привести к насыщению активного вещества и к увеличению потерь в резонаторе. Оптимум обратной связи зависит, прежде всего, от усиления и потерь в резонаторе и от его размеров. В большинстве схем лазерных резонаторов обратная связь обеспечивается подбором коэффициента пропускания выходного зеркала путем его замены, что чревато нарушением юстировки резонатора. К тому же, из-за дискретности параметров зеркал трудно точно подобрать оптимум. Но даже тщательно подобранное зеркало не может быть оптимальным на всех режимах работы, поскольку усиление и потери в резонаторе могут изменяться в процессе работы лазера. Становится очевидным преимущество плавного изменения обратной связи, что позволяет обеспечить максимальную эффективность генерации на всех режимах работы лазера. В лазерах терагерцевого (ТГц) диапазона имеется ряд особенностей, которые необходимо учитывать при выборе схем регулировки обратной связи. В качестве выходных зеркал в них используются металлические решетки и металлические зеркала с отверстиями. Для компенсации высокой дифракционной расходимости в ТГц лазерах широко используются волноводные резонаторы с диэлектрическими волноводами круглого сечения.

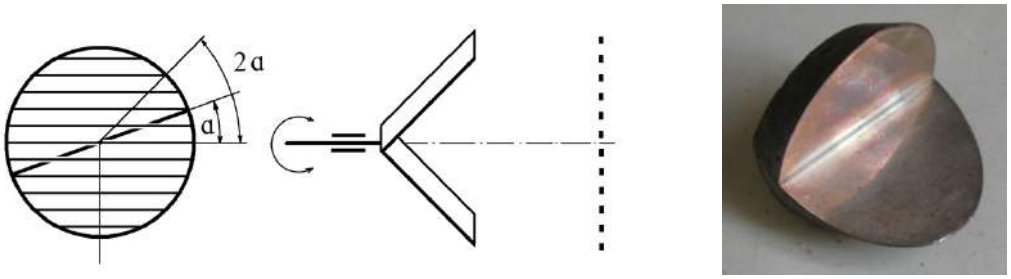
Цель работы - сравнительный анализ лазерных резонаторов ТГц диапазона с плавной регулировкой обратной связи и выработка рекомендаций по их использованию.

Схемы открытых резонаторов с плавной регулировкой обратной связи

Простейшим способом регулировки обратной связи в лазере является использование дополнительного подвижного зеркала, помещенного на пути излучения в резонаторе под углом к направлению его распространения [1]. Поворотом зеркала изменяется вывод излучения из резонатора. Однако элементы механизма перемещения зеркала вносят потери в резонатор, а направление выходного пучка излучения изменяется при регулировке, что затрудняет коммутацию лазера с трактом передачи излучения.

Оригинальная схема регулировки применена в ТГц лазере с выходным зеркалом в виде одномерной металлической решетки [2]. В качестве второго зеркала резонатора использовано двугранное 90˚ зеркало, типа призмы полного внутреннего отражения ПВО (рис.1). Ребро двугранного зеркала расположено перпендикулярно к оси резонатора. Одно из зеркал снабжено механизмом поворота вокруг оси резонатора. С помощью поворота этого зеркала осуществляется регулировка вывода излучения из резонатора. Принцип регулировки связи основан на известном свойстве двугранного 90° отражателя изменять поляризацию падающего на него излучения. Если на двугранный отражатель падает линейно поляризованное излучение, вектор напряженности электрического поля которого расположен под углом $+\alpha$ к ребру отражателя, то вектор напряженности отраженного

излучения будет расположен под углом -α к ребру отражателя, следовательно, повернут на угол 2α относительно вектора напряженности падающего излучения.



а *б*

Рис. 1. Схема лазерного резонатора с плавной регулировкой вывода излучения – *а*; внешний вид двугранного зеркала – *б*

В положении, когда ребро двугранного зеркала параллельно проводникам решетки (или перпендикулярно, но при этом потери на зеркале несколько выше), излучение линейно поляризовано, а вектор напряженности электрического поля перпендикулярен проводникам решетки. В этом случае из резонатора выводится минимальная часть излучения, задаваемая коэффициентом пропускания решетки. При повороте двугранного отражателя лазерное излучение приобретает эллиптическую поляризацию, в нем появляется ортогональная составляющая, для которой решетка практически прозрачна – вывод излучения из резонатора увеличивается. Возрастание вывода излучения происходит до положения, когда ребро двугранного зеркала окажется под углом 45° к проводникам решетки. Таким образом, можно изменять обратную связь в широких пределах и получать оптимальную обратную связь. Следует отметить, что для получения оптимума связи необходимо подбирать такую решетку, чтобы в положении минимального вывода излучения через нее выводилось излучения несколько меньше, чем требуется для оптимальной связи.

Регулировку вывода излучения в такой схеме можно осуществлять либо поворотом двугранного зеркала, либо поворотом решетки. Поворот двугранного зеркала, казалось бы, осуществлять технически проще. Однако при этом следует учитывать, что ось поворота должна быть строго перпендикулярна к ребру двугранного зеркала и расположена строго под углом 45° к обеим его граням. Не соблюдение этих требований приводит к нарушению юстировки резонатора в процессе регулировки.

Такая схема лазерного резонатора может использоваться как измерительный инструмент для сравнения потерь, вносимых решетками, которые являются выходным зеркалом [3], а также для определения коэффициентов пропускания этих решеток и вносимого ими фазового сдвига [4]. Критерием оценки вносимых потерь является мощность лазерного излучения в режиме оптимальной связи. Чем выше мощность излучения, тем меньшие потери вносит решетка, используемая в качестве выходного зеркала. Коэффициент пропускания, вносимый решеткой, рассчитывается на основании экспериментальных зависимостей мощности ортогональных составляющих лазерного излучения от угла поворота двугранного зеркала, а фазовый сдвиг - на основании снятых поляризационных диаграмм.

Однако недостатком резонаторов, содержащих решетки, является то, что они имеют существенные ограничения по мощности излучения. В мощных лазерах целесообразно использовать металлические зеркала, которые способны выдерживать высокие мощности излучения.

Для резонаторов с металлическими зеркалами разработаны оригинальные способы регулировки обратной связи. Например, в резонаторе, образованном двугранным 90˚ зеркалом типа призмы ПВО и зеркалом с выводным отверстием, удается осуществить регулировку связи путем смещения одного из зеркал [5]. Для этого можно перемещать зеркало с отверстием в направлении перпендикулярном оси резонатора или поворачивать двугранное зерка-

ло вокруг оси резонатора (в этом случае требуется, чтобы отверстие в выходном зеркале было выполнено не по центру, а со смещением). На рис. 2 приведена схема регулировки путем перемещения выходного зеркала.

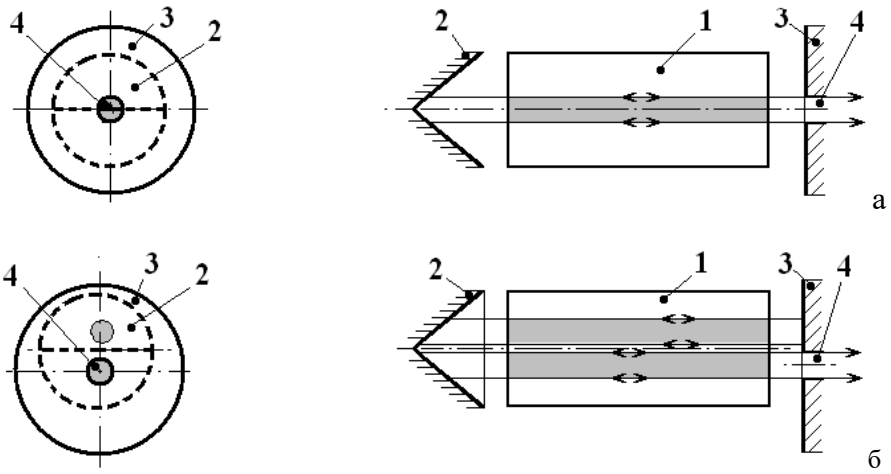


Рис. 2. Схема резонатора, содержащего двугранное 90˚ зеркало, с плавной регулировкой вывода излучения путем перемещения выходного зеркала с отверстием

В лазерном резонаторе используется активный элемент 1 круглого сечения. Резонатор образован двумя зеркалами 2, 3, размещенными по обе стороны от активного элемента 1. Зеркало 2 является двугранным с углом между гранями 90^0. Зеркало 3 имеет плоскую или слегка вогнутую отражающую поверхность, и в нем имеется отверстие связи 4. Регулировка вывода излучения осуществляется путем перемещения зеркала 3 перпендикулярно оси резонатора. В случае, когда центр отверстия 4 находится напротив ребра двугранного зеркала 2 (рис. 2, *а*), из резонатора выводится минимальная часть излучения, попадающая в заштрихованную зону. Эта зона ограничена цилиндром, имеющим основание, равное контуру отверстия 4 в зеркале связи 3, и высоту, равную расстоянию между зеркалами резонатора. Излучение, не попадающее в зону отверстия 4, испытывает многократные переотражения и усиливается в активном веществе 1. В случае, когда зеркало 3 является плоским, излучение из зоны многократного отражения попадает в зону вывода в результате дифракционной расходимости. Дифракционная связь между двумя этими зонами пропорциональна площади границы между ними, т.е. боковой поверхности цилиндра с основанием, равным контуру отверстия 4 в зеркале 3. В случае применения вогнутого зеркала 3, излучение концентрируется к оси резонатора. При этом увеличивается плотность излучения в зоне отверстия и вывод энергии через него.

При смещении отверстия связи 4 относительно ребра двугранного зеркала 2 увеличивается объем зоны, попав в которую, излучение выводится из резонатора. Одновременно увеличивается площадь границы между зоной вывода и зоной многократного отражения. Это вызывает увеличение дифракционной связи между двумя этими зонами, а следовательно, увеличивается доля выводимого из резонатора излучения. Максимальная доля излучения выводится из резонатора в случае, когда отверстие полностью проецируется на одну из граней двугранного зеркала 2 (рис. 2, *б*). В этом случае объем зоны вывода излучения увеличивается примерно в два раза по сравнению с вариантом, изображенным на рис. 2, *а*. Пропорционально увеличивается связь резонатора с внешним пространством, а следовательно, и доля выводимого излучения. Нагруженная добротность резонатора при этом уменьшается, причем потери увеличиваются в основном за счет потерь на связь, т.е. за счет увеличения «полезного» излучения. Энергетически это эквивалентно увеличению сечения выводного отверстия, но сечение выводного пучка излучения при всех положениях зеркал не изменяется и остается

равным сечению выводного отверстия 4. Естественно, что для получения оптимума связи необходимо, чтобы через выводное отверстие 4 в положении минимального вывода излучения (рис. 2, *а*) выводилось несколько меньше энергии, чем требуется для получения оптимальной связи.

Однако при перемещении зеркал может нарушаться юстировка резонатора, особенно если регулировка осуществляется поворотом двугранного зеркала.

Проблема нарушения юстировки резонатора при регулировке связи существенно нивелирована в резонаторе [6], в котором вместо двугранного зеркала использован трехгранный 90˚ уголковый отражатель. Благодаря известным свойствам такого отражателя возврат луча в обратном направлении не зависит от угла падения. Такой отражатель практически не требует юстировки. Схема регулировки аналогична схеме, изображенной на рис. 2. Однако в волноводных резонаторах регулировку можно осуществлять только путем смещения плоского зеркала. Вершина трехгранного зеркала (для минимизации потерь в резонаторе) должна быть расположена строго на оси круглого сечения волновода. Принцип регулировки не изменяется – минимальная часть излучения выводится, когда центр выводного отверстия проецируется на вершину трехгранного зеркала. При смещении центра выводного отверстия относительно вершины трехгранного зеркала происходит увеличение вывода излучения. Увеличение происходит при перемещении до расстояния, равного примерно радиусу отверстия связи. Однако потери излучения на трехгранном зеркале несколько выше, вследствие трех отражений от его граней. Кроме того, вблизи его ребер (как и у двугранного отражателя) присутствует зона повышенных потерь. Это обусловлено неидеальностью изготовления граней и волновыми свойствами излучения.

Значительно уменьшить потери излучения позволяет применение в резонаторе конического зеркала с углом при вершине 90^0 [7]. Коническое зеркало (рис. 3), так же как и трехгранный уголковый отражатель, не требует тщательной юстировки и вносит меньше потерь в резонатор благодаря отсутствию ребер и благодаря тому, что имеет всего лишь два отражения от его поверхности. Схема регулировки при использовании конического зеркала аналогична схеме, изображенной на рис. 2. Регулировка осуществляется путем смещения плоского зеркала с отверстием в направлении перпендикулярно оси резонатора. Вершина конического зеркала должна быть расположена на оси резонатора. Особенно это актуально для волноводных резонаторов.

Существенным достоинством конического зеркала является то, что если угол при его вершине выполнить несколько меньше 90^0, такое зеркало приобретает фокусирующие способности. Это позволяет снизить дифракционные потери в резонаторе и повысить концентрацию излучения в зоне выводного отверстия. Следовательно, в резонаторе не нужно использовать второе вогнутое зеркало, оно может быть плоским, что значительно проще в изготовлении.

Рис. 3. Коническое зеркало с углом при вершине 90^0

Однако на вершине конического зеркала все же имеется зона повышенных потерь, обусловленная неидеальностью изготовления зеркала и волновыми свойствами излучения. Устра-

нить эти потери позволяет резонатор с двухсторонним выводом излучения (рис. 4), в котором использовано 90˚коническое зеркало с центральным выводным отверстием [8]. В лазерном резонаторе используется активный элемент 1 круглого сечения. Резонатор образован двумя зеркалами 2 и 3, размещенными по обе стороны от активного элемента 1. Зеркало 2 является коническим с углом при вершине 90^0 или несколько меньше. Оно размещено строго по оси активного элемента 1, а зеркало 3 имеет плоскую отражающую поверхность, и в нем имеется отверстие связи 4. В такой схеме основной регулируемый вывод излучения осуществляется через отверстие 4 в подвижном плоском зеркале 3, которое перемещается перпендикулярно оси резонатора. Через отверстие 5 в коническом зеркале 2 вывод излучения не регулируется, а это излучение подается на приборы контроля и управления лазером. Излучение в зону отверстий 4, 5 попадает благодаря дифракции. Если коническое зеркало 2 имеет угол при вершине меньше 90^0, то это повышает концентрацию энергии в зоне отверстий и одновременно снижает дифракционные потери в резонаторе. Отверстие 5 в центре конического зеркала 2 позволяет устранить зону повышенных потерь. Часть излучения, которая бы имела повышенные потери, теперь выводится через отверстие и используется для контроля и управления лазером. В предыдущих схемах для контроля и управления лазером используется часть энергии, отобранная от основного лазерного пучка. Таким образом, дополнительный канал вывода излучения позволяет повысить общий КПД лазерной установки. Естественно, что для обеспечения оптимальной связи требуется, чтобы в положении минимального вывода излучения (рис. 4, *а*) из резонатора через оба отверстия выводилось немного меньше энергии, чем требуется для обеспечения оптимума.

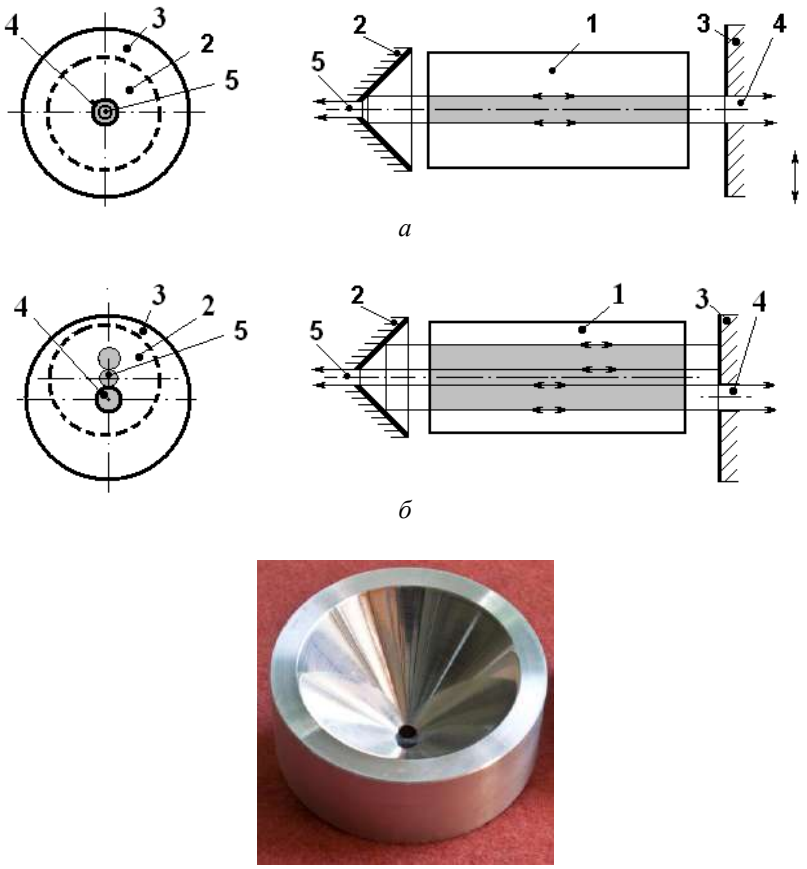


Рис. 4. Схема резонатора с плавной регулировкой, содержащая коническое 90˚ зеркало с дополнительным каналом не регулируемого вывода излучения (*а, б*). Внешний вид конического зеркала с отверстием (*в*)

Выводы

Приведен краткий обзор и сравнительный анализ открытых резонаторов лазеров ТГЦ диапазона длин волн с плавной регулировкой связи с внешним пространством. Рассмотрены как давно известные и широко используемые, так и новейшие схемы лазерных резонаторов. Плавную регулировку обратной связи можно реализовать при использовании в качестве выходных отражателей резонатора как металлических зеркал с отверстиями, так и одномерных проволочных решеток. Проведен анализ преимуществ и недостатков каждой из рассмотренных схем. Показано, что их применение позволяет получать оптимальную обратную связь в процессе роботы лазеров и добиваться высокой эффективности лазеров на всех энергетических режимах. Особенно это полезно для лазеров на активных средах, имеющих несколько линий излучения с различными коэффициентами усиления. Существенным преимуществом приведенных схем является их относительная простота изготовления, что позволяет переоборудовать лазеры, которые уже используются.

Список литературы:

1. Свейн Д. Устройство для регулирования связи на выходе лазера в дальней ИК области // Приборы для научных исследований. 1972. №7. С.86.

2. Каменев Ю.Е., Кулешов Е.М. Волноводный HCN лазер с регулируемой связью // Квантовая электроника. 1990. Т.17, №1. С. 58-59.

3. Дзюбенко М.И., Каменев Ю.Е., Радионов В.П., Литвина З.Ю. Резонаторный способ определения потерь в одномерных металлических решетках в терагерцевом диапазоне // Радиофизика и электроника. 2018. Т. 23. № 2. С. 69-75.

4. Дзюбенко М.И., Каменев Ю.Е., Масалов С.А., Радионов В.П. Измерение электродинамических характеристик металлических ленточных решеток в терагерцевом диапазоне // Радиофизика и электроника. 2019, 24(2). С. 78-85.

5. Патент на винахід України № 91610 від 10.08.2010 «Лазер з плавним регулюванням випромінювання з резонатора» : авт. Кісельов В.К., Радіонов В.П.

6. Патент на винахід України №105802 від 25.06.2014 «Лазер з плавним регулюванням виведевиведення випромінювання з резонатора» : авт. Кісельов В.К., Радіонов В.П.

7. Патент на винахід України №110672 від 25.01.2016 «Лазер з плавним регулюванням виведення випромінювання з резонатора» : авт. Радіонов В.П., Маслов В.О.

8. Патент на винахід України №114127 від 25.04.2017 «Лазер з плавним регулюванням виведення випромінювання з резонатора» : авт. Дзюбенко М.І., Маслов В.О. Радіонов В.П.

Поступила в редколлегию 11.10.2020

Сведения об авторах:

Дзюбенко Михаил Иванович – д-р физ.-мат. наук, профессор, заведующий отделом, Институт радиофизики и электроники им. А.Я. Усикова НАН Украины; профессор кафедры физических основ электронной техники, Харьковский национальный университет радиоэлектроники, Украина; e-mail:mid41@ukr.net, ORCID: https://orcid.org/0000-0002-9227-5604

Маслов Вячеслав Александрович – д-р физ.-мат. наук, профессор, заведующий кафедрой квантовой радиофизики, Харьковский национальный университет имени В.Н. Каразина, Украина; e-mail: v.a.maslov@karazin.ua, ORCID: https://orcid.org/0000-0001-7743-7006

Радионов Владимир Петрович – канд. физ.-мат. наук, старший научный сотрудник, Институт радиофизики и электроники им. А.Я. Усикова НАН Украины, Украина; e-mail: radsvet@ukr.net

Фомин Александр Александрович – аспирант, Харьковский национальный университет радиоэлектроники, Украина; e-mail: oleksandr.fomin@nure.ua

УДК 537.226.3 **DOI:10.30837/rt.2020.4.203.18**

Б.В. ЖУКОВ, канд. техн. наук, С.И. БОРБУЛЕВ

ОДНОРЕЗОНАТОРНОЕ СВЧ УСТРОЙСТВО ДЛЯ КОНТРОЛЯ ДИЭЛЕКТРИЧЕСКОЙ ПРОНИЦАЕМОСТИ ЖИДКИХ ГОРЮЧЕ-СМАЗОЧНЫХ МАТЕРИАЛОВ

Введение

Помимо двухрезонаторных [1, 2] для контроля диэлектрической проницаемости горюче-смазочных материалов (ГСМ) могут применяться однорезонаторные СВЧ устройства [3]. Основное преимущество двухрезонаторных диэлектрометров заключается в возможности текущего сопоставления комплексной диэлектрической проницаемости исследуемого образца с его эталоном, что необходимо, например, на технологических линиях в процессе производства ГСМ. При проведении экспресс-анализа в полевых условиях в синхронном сопоставлении обычно нет необходимости, что позволяет использовать для контроля комплексной диэлектрической проницаемости ГСМ однорезонаторный вариант исполнения СВЧ датчика диэлектрометра. Использование только одного резонатора упрощает СВЧ датчик диэлектрометра, снижает его массогабаритные параметры, однако приводит к изменению самого процесса измерения комплексной диэлектрической проницаемости жидких ГСМ и анализа результатов на комплексной плоскости.

В работе рассмотрены особенности построения и настройки СВЧ датчика однорезонаторного диэлектрометра, предназначенного для экспресс-анализа комплексной проницаемости ГСМ типа бензины, керосины, дизельные топлива, моторные и трансформаторные масла.

Основная часть

На рис. 1 приведена упрощенная структурная схема однорезонаторного СВЧ диэлектрометра, в состав которого входит СВЧ датчик, управляющий процессор, индикатор, клавиатура, банк хранения данных, усилитель и делитель частоты сигнала действительной части комплексной диэлектрической проницаемости.

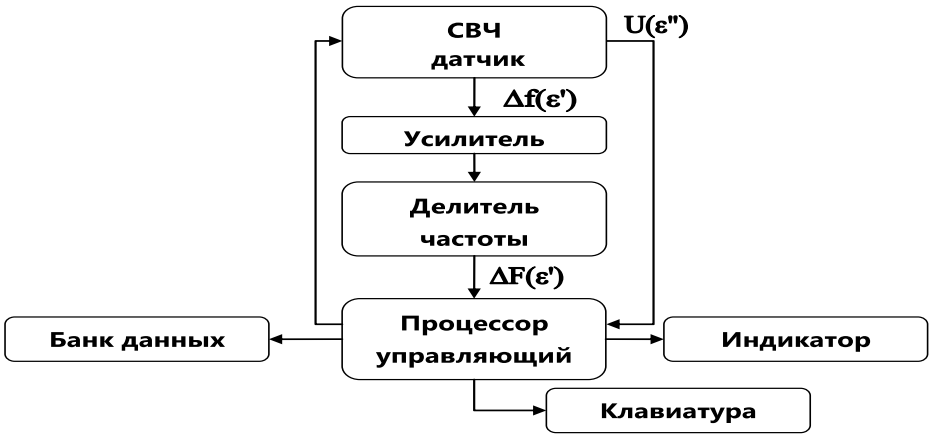


Рис. 1. Диэлектрометр однорезонаторный

Структурная схема СВЧ датчика однорезонаторного диэлектрометра представлена на рис. 2. В состав датчика входит генератор, управляемый с варикапом перестройки его частоты; генератор опорный с устройством подстройки его частоты,; первый и второй аттенюаторы, предназначенные для снижения взаимного влияния генераторов друг на друга; смеситель, с выхода которого сигнал разностной частоты $\Delta f(\varepsilon')$ поступает на вход усилителя и делителя частоты (см. рис. 1) канала измерения действительной части комплексной диэлектрической проницаемости исследуемого диэлектрика $\Delta F(\varepsilon')$, а также измерительный резонатор

и детектор сигнала мнимой части $U(\varepsilon^{"})$ комплексной диэлектрической проницаемости исследуемого диэлектрик с устройством его согласования с волноводным трактом.

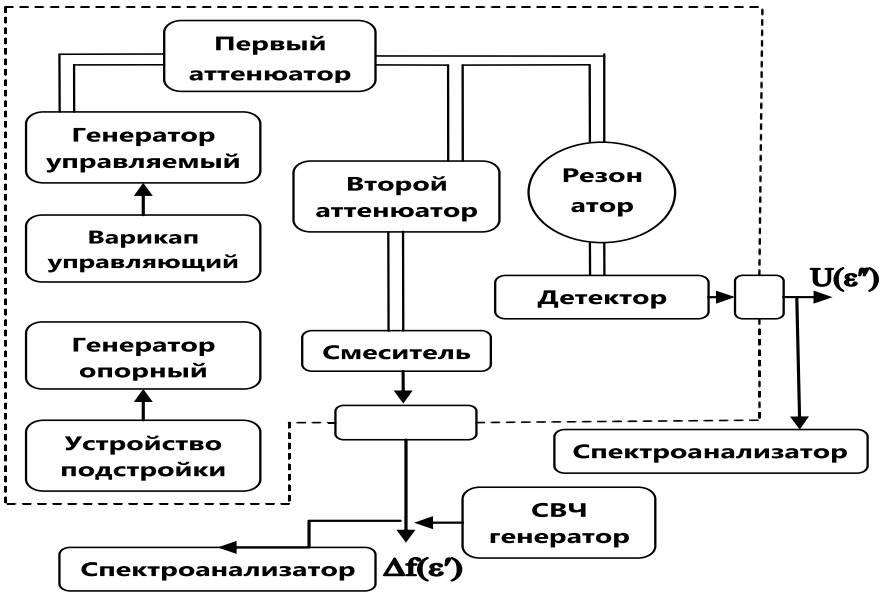


Рис. 2. СВЧ датчик

Конструктивно СВЧ датчик выполнен в виде параллелепипеда, внутри которого размещены волноведущие тракты, резонатор, генераторы, смесительный и детекторный диоды и аттенюаторы. Размещение обоих генераторов внутри единого массивного корпуса совместно с общим для них источником питания и использование относительного метода измерения обусловливает кратковременную нестабильность измерения параметров комплексной диэлектрической проницаемости на уровне до (10^{-4}...10^{-5}). Нижняя часть корпуса СВЧ датчика приведена на рис. 3.

Для измерения комплексной диэлектрической проницаемости исследуемого образца необходимо выполнить калибровку по пустой кювете, затем произвести измерение параметров исследуемого образца и анализ полученных результатов на комплексной плоскости.

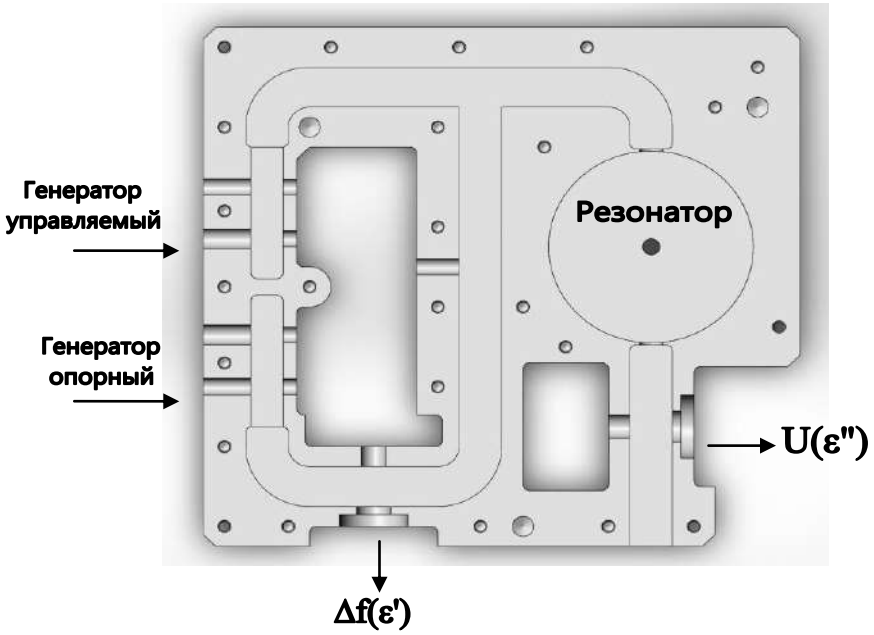


Рис. 3. Корпус СВЧ датчика

Для исследования отличий заданного образца от его эталона последовательно во времени необходимо выполнить калибровку по пустой кювете, измерение параметров образца, параметров эталона, а затем проанализировать полученные результаты на комплексной плоскости.

Первоначальная настройка СВЧ датчика

Проведению измерений предшествует этап первоначальной настройки СВЧ датчика. В процессе проведения первоначальной настройки:

- проводится оценка диапазона возможной механической перестройки резонансной частоты измерительного резонатора. Для этого внешний СВЧ генератор стандартных сигналов подключается к технологическому разъему смесителя (см. рис. 2), а спектроанализатор – к технологическому разъему детектора. Для положений элемента подстройки резонатора, соответствующих минимальной и максимальной частотам резонатора, по сигналу генератора, прошедшему через резонатор, определяется его частотный диапазон. Измерения проводятся при выключенных опорном и управляемом генераторах и установленной в резонаторе пустой кювете;
- при включенном питании управляемого генератора с помощью спектроанализатора, подключенного к технологическому разъему смесителя, осуществляется оценка диапазона перестройки его частоты, который должен располагаться внутри частотного диапазона перестройки резонатора. Кроме того, проводится контроль спектра сигнала в полосе его перестройки;
- при включенном питании опорного генератора с помощью спектроанализатора, подключенного к технологическому разъему смесителя (см. рис. 2), осуществляется контроль спектра сигнала в полосе его перестройки; а также диапазона перестройки его частоты, который должен располагаться вне частотного диапазона перестройки резонатора;
- при включенном управляемом генераторе с помощью спектроанализатора, подключенного к технологическому разъему детектора (см. рис. 2), осуществляется контроль возможности настройки резонатора, нагруженного пустой кюветой, на частоту близкую к максимальной частоте управляемого генератора;
- при включенном управляемом генераторе с помощью спектроанализатора, подключенного к технологическому разъему детектора (см. рис. 2), осуществляется контроль возможности настройки резонатора, нагруженного образцом ГСМ с максимальной диэлектрической проницаемостью;

В результате первоначальной настройки выполняется подготовка СВЧ датчика к проведению измерений, а именно – устанавливаются начальные частоты управляемого и опорного генераторов и проверяется максимальный электронной перестройки частоты управляемого генератора. После завершения первоначальной настройки СВЧ датчика и его подключения к управляющему процессору диэлектрометр готов к выполнению измерений.

Калибровка по пустой кювете

После установки в резонаторе пустой (без образца) кюветы с помощью клавиатуры выбирается режим “калибровка”. По этой команде в управляющем процессоре блока обработки информации (см. рис. 1) вырабатывается команда начала программной перестройки частоты управляемого генератора от её максимального до минимального значений. Об этой команде управляющий процессор вырабатывает сигнал управления частотой, который поступает на управляющий вход управляемого генератора. С выхода управляемого генератора перестраиваемый по частоте сигнал $f_{\text{упр}}$ через первый аттенюатор поступает на вход измерительного резонатора и вход второго аттенюатора, с выхода которого он поступает на сигнальный вход смесителя.

Когда частота сигнала управляемого генератора попадает в полосу пропускания измерительного резонатора, на его выходе появляется сигнал, поступающий на вход детектора, с выхода которого продетектированный сигнал $U(\varepsilon'')$ поступает на вход управляющего про-

цессора для измерения мнимой части диэлектрической проницаемости ε'', где он преобразуется аналого-цифровым преобразователем в цифровой код и используется для дальнейшей обработки.

Одновременно с перестраиваемым по частоте сигналом управляемого генератора $f_{\text{упр}}$ на гетеродинный вход смесителя подается сигнал опорного генератора $f_{\text{оп}}$. Сигнал разностной частоты $\Delta f(\varepsilon') = \left| f_{\text{упр}} - f_{\text{оп}} \right|$ с выхода смесителя поступает на вход усилителя, где усиливается до необходимой величины и подается на вход делителя частоты. С выхода делителя частоты сигнал разностной частоты $\Delta F(\varepsilon') = \Delta f(\varepsilon') / \hat{E}$, где К – коэффициент деления делителя, поступает на вход управляющего процессора для измерения разностной частоты несущей информацию о величине действительной части ε' диэлектрической проницаемости пустой кюветы.

После появления сигнала на входе измерения ε'' управляющий процессор переходит в режим поиска максимальной величины этого сигнала, соответствующей настройке частоты управляемого генератора на резонансную частоту измерительного резонатора. В процессе поиска производится регистрация в оперативной памяти управляющего процессора разностной частоты $\Delta F(\varepsilon')$, поступающей на вход измерения ε', и величины сигнала $U(\varepsilon'')$, поступающего на второй вход измерения ε''. В оперативной памяти управляющего процессора регистрируются максимальная величина сигнала $U_O^{\max}$ и соответствующее ей значение разностной частоты $\Delta F_O^{\max}$, несущие информацию о диэлектрической проницаемости пустой кюветы.

Результаты вычислений $\Delta F_O^{\max}$ и $U_O^{\max}$ также выводятся на индикатор для визуального анализа и принятия решения о пригодности кюветы для проведения измерений. Управление частотой управляемого генератора продолжается до достижения нижней границы частоты перестройки, после чего процесс перестройки прекращается. Для снижения влияния разброса параметров кювет на результат измерения параметров диэлектриков калибровка должна проводиться непосредственно перед каждым исследованием.

На рис. 4 приведены результаты измерения комплексной диэлектрической проницаемости для пяти пустых кювет. Они подтверждают необходимость проведения калибровки перед каждым измерением, так как разброс величин действительных и мнимых частей образцов кювет могут превышать несколько процентов.

Измерение параметров исследуемого образца. Анализ результатов измерений

После установки в резонаторе кюветы с образцом исследуемого ГСМ с помощью клавиатуры выбирается режим “измерение”. По этой команде управляющий процессор, аналогично режиму «калибровка», выполняет измерения $\Delta F_{\text{обр}}^{\max}$ и $U_{\text{обр}}^{\max}$, величины которых выводятся на индикатор и записываются в его оперативную память.

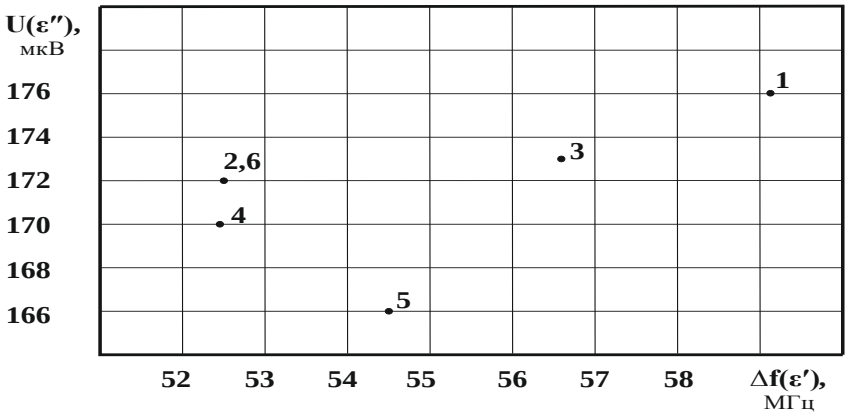


Рис. 4. Параметры пустых кювет

Анализ результатов измерений выполняется после включения режима «анализ». В этом режиме управляющий процессор вычисляет величины $\Delta F_{\text{обр}} = \Delta F_{\text{обр}}^{\max} - \Delta F_{O}^{\max}$ и $\delta U_{\text{обр}} = U_{\text{обр}}^{\max} / U_{O}^{\max}$, которые характеризуют реальную комплексную диэлектрическую проницаемость образца ГСМ. Результаты вычисления представляются на комплексной плоскости индикатора и записываются в банк данных устройства.

Измерения относительно эталона

Режим “Эталон” позволяет исследовать отличие исследуемого образца от его эталона. С этой целью последовательно определяется пригодность пустой кюветы для проведения исследований. Далее определяются параметры $\Delta F_{\text{этал}}^{\max}$ и $U_{\text{этал}}^{\max}$ эталона и параметры $\Delta F_{\text{обр}}^{\max}$ и $U_{\text{обр}}^{\max}$ исследуемого образца, а затем величины $\Delta F = \Delta F_{\text{обр}}^{\max} - \Delta F_{\text{этал}}^{\max}$ и $\delta U = U_{\text{обр}}^{\max} / U_{\text{этал}}^{\max}$, характеризующие отличие исследуемого образца от эталона.

Выводы

Однорезонаторный диэлектрометр обеспечивает возможность измерения комплексной диэлектрической проницаемости жидких ГСМ с последующим анализом результатов на комплексной плоскости. Он также обеспечивает возможность сопоставления полученных результатов измерения комплексной диэлектрической проницаемости образца ГСМ с его эталоном.

Конструктивное исполнение однорезонаторного СВЧ датчика в виде параллелепипеда позволяет выполнять его комплексную настройку перед проведением измерений.

Список литературы:

1. Жуков Б.В. СВЧ диэлектрометр для экспресс-анализа октановых чисел автомобильных топлив // Датчики и системы. 2008. № 11. с.15-17.

2. Патент РФ 2163373 G01N 22/00, 33/22. Устройство для измерения параметров жидких топлив // Бюл. 2001. №5.

3. Б.В. Жуков, С.І. Борбульов/ Оперативный контроль параметров жидких горюче-смазочных материалов // Радиотехника. 2019. Вып. 196. С. 62-69.

Поступила в редколлегию 05.11.2020

Сведения об авторах:

Жуков Борис Владимирович – канд. техн. наук, старший научный сотрудник отдела физических основ радиолокации доцент, Институт радиофизики и электроники им. А.Я. Усикова НАН Украины, Украина; e-mail: zhukov@ire.kharkov.ua

Борбулев Станислав Игоревич – Институт современной обработки металлов, соискатель Института радиофизики и электроники им. А.Я. Усикова НАН Украины; Украина; e-mail: Stanislav.borbulev@gmail.com

УДК 537.86 **DOI:10.30837/rt.2020.4.203.19**

А.И. КОЗАРЬ, д-р физ.-мат. наук

РАССЕЯНИЕ ЭЛЕКТРОМАГНИТНЫХ ВОЛН ДИСКРЕТНЫМ ОКТАЭДРОМ ИЗ РЕЗОНАНСНЫХ СФЕР

Введение

Здесь рассматривается случай, эквивалентный рентгеновской оптике кристаллов, когда $a/\lambda' << 1$ и может быть $a/\lambda_g \sim 1; d,h,l/\lambda' \sim 1$, где a – радиус сфер; λ', λ_g – длины рассеиваемой волны вне и внутри сфер; d,h,l – постоянные решетки. Решение задачи получено на основе интегральных уравнений электродинамики Фредгольма 2-го рода, с нелокальными граничными условиями [1 – 3].

Найденные в работе выражения для метакристалла в форме октаэдра можно использовать для изучения рассеянных кристаллом полей в зонах Френеля и Фраунгофера, а также для изучения его внутреннего поля.

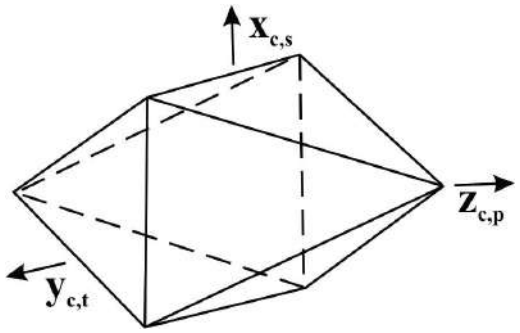


Рис. 1. Геометрия задачи

Основная часть

Рассмотрим сложную пространственную решетку метакристалла, состоящую из C ромбических подрешеток $c\left(c \in C\right)$. Эти подрешетки порождаются координатным представлением, которое в прямоугольной декартовой системе координат имеет вид (рис. 1):

$$\begin{aligned} x_{c,s} &= [s - 0,5\{(-1)^s - 1\}]d - (-1)^{s-1} x_{c,s=0} \\ s &= 0, \pm 1, \pm 2, ..., \pm\left(|p_{\max}| - |p|\right), \\ y_{c,t} &= [t - 0,5\{(-1)^t - 1\}]h - (-1)^{t-1} y_{c,t=0} \\ t &= 0, \pm 1, \pm 2, ..., \pm\left(|p_{\max}| - |p|\right), \\ z_{c,p} &= [p - 0,5\{(-1)^p - 1\}]l - (-1)^{p-1} z_{c,p=0} \\ p &= 0, \pm 1, \pm 2, ..., \pm|p_{\max}|, \end{aligned} \tag{1}$$

где величины d, h, l определяются условиями $x = 0, x = d; y = 0, y = h; z = 0, z = l$, а $x_{c,s=0}, y_{c,t=0}, z_{c,p=0}$ – координаты узла, порождающего подрешетку c и находящегося внутри области элементарной ячейки решетки

$$\begin{aligned} 0 \le x_{c,s=0} \le d, \\ 0 \le y_{c,t=0} \le h, \\ 0 \le z_{c,p=0} \le l. \end{aligned} \tag{2}$$

Координаты $x_{c,s}, y_{c,t}, z_{c,p}$ – определяют положение узлов подрешетки c вне пределов области (2) и являются функциями координат $x_{c,s=0}, y_{c,t=0}, z_{c,p=0}$. Каждому узлу подрешетки c (1) сопоставляется упорядоченная тройка чисел – $c\left(p,s,t\right)$, выделенный узел решетки будем обозначать – $c'\left(p',s',t'\right)$. Задавая максимальные значения для чисел $\left(p,s,t\right)$ в (1), можно рассматривать ограниченные дискретные решетки.

Ячейку решетки формируют из узлов внутри области (2), которую повторит за пределами области (2) координатное представление (1) в виде пространственной решетки.

Расстояние между узлами определим (1)

$$r_{c'(p',s',t'),c(p,s,t)} = \sqrt{\left(x_{c',s'} - x_{c,s}\right)^2 + \left(y_{c',t'} - y_{c,t}\right)^2 + \left(z_{c',p'} - z_{c,p}\right)^2}. \quad (3)$$

В узлы подрешеток (1) помещаются центры сфер с комплексными диэлектрической и магнитной проницаемостями $\varepsilon_{c(p,s,t)}, \mu_{c(p,s,t)}$, радиусами $a_{c(p,s,t)}$, объемами $V_{c(p,s,t)}$, которые дальше будем обозначать – ε_c, μ_c, a_c, V_c. Сферы решетки находятся в среде с комплексными диэлектрической и магнитной проницаемостями ε_0, μ_0.

Для решения подобных задач удобно использовать интегральные уравнения электродинамики с нелокальными граничными условиями [1, 2], и решать задачу будем в два этапа. На первом этапе найдем внутреннее поле рассеивающих сфер, а на втором – поле, рассеянное пространственной решеткой сфер.

Рассеянное решеткой поле по известному внутреннему полю рассеивателей определим через электрический $\vec{\Pi}^э$ и магнитный $\vec{\Pi}^м$ потенциалы Герца:

$$\begin{aligned} \vec{E}_{расс} &= \left(\nabla\nabla + k^2\varepsilon_0\mu_0\right)\vec{\Pi}^э - ik\mu_0\left[\nabla, \vec{\Pi}^м\right], \\ \vec{H}_{расс} &= \left(\nabla\nabla + k^2\varepsilon_0\mu_0\right)\vec{\Pi}^м + ik\varepsilon_0\left[\nabla, \vec{\Pi}^э\right]. \end{aligned} \quad (4)$$

Потенциалы Герца рассеянного поля отдельными сферами представим в виде

$$\begin{aligned} \vec{\Pi}^э_{c(p,s,t)}\left(\vec{r},t\right) &= \frac{1}{4\pi}\int_{V_c}\left(\frac{\varepsilon_{сэф}}{\varepsilon_0} - 1\right)\vec{E}^0_{c(p,s,t)}\left(\vec{r}',t\right) f_c\left(\left|\vec{r} - \vec{r}'\right|\right)dV, \\ \vec{\Pi}^м_{c(p,s,t)}\left(\vec{r},t\right) &= \frac{1}{4\pi}\int_{V_c}\left(\frac{\mu_{сэф}}{\mu_0} - 1\right)\vec{H}^0_{c(p,s,t)}\left(\vec{r}',t\right) f_c\left(\left|\vec{r} - \vec{r}'\right|\right)dV, \end{aligned} \quad (5)$$

где $\vec{E}^0_{c(p,s,t)}\left(\vec{r}',t\right), \vec{H}^0_{c(p,s,t)}\left(\vec{r}',t\right)$ – внутренние поля рассеивателя, V_c – объем рассеивателя; функция $f\left(\left|\vec{r} - \vec{r}'\right|\right)$ является решением уравнения

$$\Delta f\left(\left|\vec{r} - \vec{r}'\right|\right) + k^2\varepsilon_0\mu_0 f\left(\left|\vec{r} - \vec{r}'\right|\right) = -4\pi\delta\left(\left|\vec{r} - \vec{r}'\right|\right),$$

удовлетворяющего условию излучения на бесконечности и имеет вид

$$f\left(\left|\vec{r} - \vec{r}'\right|\right) = \frac{e^{-ki\sqrt{\varepsilon_0\mu_0}\left|\vec{r} - \vec{r}'\right|}}{\left|\vec{r} - \vec{r}'\right|}. \quad (6)$$

Можно показать, что для точек вне сферы ($r > r'$) интеграл по объему сферы от функции Грина (6) имеет вид

$$W_{c(p,s,t)}\left(\vec{r}\right) = \int_{V_c}\frac{e^{-ik\sqrt{\varepsilon_0\mu_0}\left|\vec{r} - \vec{r}'\right|}}{\left|\vec{r} - \vec{r}'\right|}dV = \frac{4\pi}{k_1^3}\left(\sin k_1 a_c - k_1 a_c \cos k_1 a_c\right)\frac{e^{-ik_1 r}}{r}, \quad (7)$$

где $k_1 = k\sqrt{\varepsilon_0\mu_0}, k = 2\pi/\lambda_0$, r – определяет расстояние от центра до точек вне сферы.

Поля представим в виде

$$\vec{E}\left(\vec{r},t\right) = \vec{E}\left(\vec{r}\right)e^{i\omega t}, \vec{H}\left(\vec{r},t\right) = \vec{H}\left(\vec{r}\right)e^{i\omega t}.$$

Будем считать, что вне сфер $a_c/\lambda << 1$, но внутри сферы возможен резонансный случай $a_c/\lambda_g \sim 1$, где $\lambda = \lambda_0/\sqrt{\varepsilon_0\mu_0}$ – длина волны вне сферы, а $\lambda_g = \lambda_0/\sqrt{\varepsilon_c\mu_c}$ – длина волны в сфере.

Внутреннее поле $c'(p',s',t')$ сферы найдем из системы квазистационарных неоднородных уравнений, которые построим, опираясь на интегральные уравнения [2]. Входящее в эту систему неоднородное уравнение для внутреннего электрического поля произвольной сферы $c'(p',s',t')$ имеет вид

$$\vec{E}_{0c'(p',s',t')}(\vec{r}',t)=\left(\left\{\frac{\left(\varepsilon_{c\text{эф}}+2\varepsilon_0\right)+\theta_{1c}^2\varepsilon_{c\text{эф}}+\theta_{1c}^2\left(\varepsilon_{c\text{эф}}+2\varepsilon_0\right)}{3\varepsilon_0}\right\}\times\right.$$

$$\times\vec{E}^0_{c'(p',s',t')}(\vec{r}',t)-\sum_p\sum_s\sum_t\left\{\left(\nabla\nabla+k^2\varepsilon_0\mu_0\right)\times\frac{1}{4\pi}\left(\frac{\varepsilon_{c'\text{эф}}}{\varepsilon_0}-1\right)W^{\text{э}}_{c'(p,s,t)}(\vec{r})\vec{E}^0_{c'(p,s,t)}(\vec{r}',t)-\right.$$

$$c'(p,s,t)\neq c'(p',s',t')$$

$$\left.\left.-ik\mu_0\left[\nabla,\frac{1}{4\pi}\left(\frac{\mu_{c'\text{эф}}}{\mu_0}-1\right)W^{\text{м}}_{c'(p,s,t)}(\vec{r})\vec{H}^0_{c'(p,s,t)}(\vec{r}',t)\right]\right\}\right)-$$

$$-\sum_{c=1}^{C}\left(\sum_p\sum_s\sum_t\left\{\left(\nabla\nabla+k^2\varepsilon_0\mu_0\right)\frac{1}{4\pi}\left(\frac{\varepsilon_{c\text{эф}}}{\varepsilon_0}-1\right)\times W^{\text{э}}_{c(p,s,t)}(\vec{r})\vec{E}^0_{c(p,s,t)}(\vec{r}',t)-ik\mu_0\times\right.\right.$$

$$(c\neq c')$$

$$\left.\left.\times\left[\nabla,\frac{1}{4\pi}\left(\frac{\mu_{c\text{эф}}}{\mu_0}-1\right)W^{\text{м}}_{c(p,s,t)}(\vec{r})\vec{H}^0_{c(p,s,t)}(\vec{r}',t)\right]\right\}\right), \qquad (8)$$

где $\vec{E}_{0c'(p',s',t')}(\vec{r}',t)$ и $\vec{E}^0_{c'(p',s',t')}(\vec{r}',t)$, $\vec{H}^0_{c'(p',s',t')}(\vec{r}',t)$ – поле падающей волны и внутреннее поле $c'(p',s',t')$ сферы, а $\vec{E}_{c(p,s,t)}(\vec{r}',t),\vec{H}_{c(p,s,t)}(\vec{r}',t)$ – внутренние поля остальных сфер.

Величины $W^{\text{э}}_{c(p,s,t)}(\vec{r}'),W^{\text{м}}_{c(p,s,t)}(\vec{r}')$, $\varepsilon_{c\text{эф}}$, $\mu_{c\text{эф}}$ имеют вид (3, 7, 8)

$$W^{\text{м}}_{c(p,s,t)}=W^{\text{э}}_{c(p,s,t)}(\vec{r}')=\frac{4\pi}{k_1^3}\left(\sin k_1a_c-k_1a_c\cos k_1a_c\right)\times\frac{e^{-ik_1r_{c'(p',s',t'),c(p,s,t)}}}{r_{c'(p',s',t'),c(p,s,t)}},$$

$$\varepsilon_{c\text{эф}}=\varepsilon_cF\left(ka_c\sqrt{\varepsilon_c\mu_c}\right), \qquad (9)$$

$$\mu_{c\text{эф}}=\mu_cF\left(ka_c\sqrt{\varepsilon_c\mu_c}\right),$$

где

$$F\left(ka_c\sqrt{\varepsilon_c\mu_c}\right)=\frac{2\left(\sin ka_c\sqrt{\varepsilon_c\mu_c}-ka_c\sqrt{\varepsilon_c\mu_c}\cos ka_c\sqrt{\varepsilon_c\mu_c}\right)}{\left(k^2a_c^2\varepsilon_c\mu_c-1\right)\sin ka_c\sqrt{\varepsilon_c\mu_c}+ka_c\sqrt{\varepsilon_c\mu_c}\cos ka_c\sqrt{\varepsilon_c\mu_c}}.$$

Уравнение для внутреннего магнитного поля сферы $c'(p',s',t')$ имеет вид аналогичный уравнению (8), если в нем произвести замену электрических величин на магнитные.

Уравнения (8) представляют алгебраическую систему $2N=2\sum_{c=1}^{C}N_c$ векторных неоднородных уравнений, где N– общее число сфер решетки, а N_c – число сфер подрешетки c. Решение этой системы уравнений для сферы $c'(p',s',t')$ имеет вид:

$$\vec{E}^{0}_{c'(p',s',t')}(\vec{r}',t)=\frac{1}{\Delta^{эм}}\sum_{c=1}^{C}\left(\sum_{u}\left[\hat{g}^{эи'}_{u}\vec{E}_{0c(p,s,t)}(\vec{r}',t)+\hat{\beta}^{эи'}_{u}\vec{H}_{0c(p,s,t)}(\vec{r}',t)\right]\right),$$
$$\vec{H}^{0}_{c'(p',s',t')}(\vec{r}',t)=\frac{1}{\Delta^{эм}}\sum_{c=1}^{C}\left(\sum_{u}\left[\hat{\beta}^{ми'}_{u}\vec{H}_{0c(p,s,t)}(\vec{r}',t)+\hat{g}^{ми'}_{u}\vec{E}_{0c(p,s,t)}(\vec{r}',t)\right]\right), \quad (10)$$

$\Delta^{эм}$ – детерминант основной матрицы системы уравнений (8).

Потенциалы Герца (4), рассеянного сферами решетки поля можно представить, учитывая (9) и (10), в виде суперпозиции потенциалов Герца отдельных сфер решетки (5)

$$\vec{\Pi}^{э}(\vec{r},t)=\sum_{c=1}^{C}\left[\sum_{p}\sum_{s}\sum_{t}\frac{1}{k_1^3}\left(\sin k_1a_c-k_1a_c\cos k_1a_c\right)\times\left(\frac{\varepsilon_{сэф}}{\varepsilon_0}-1\right)\vec{E}^{0}_{c(p,s,t)}(\vec{r}',t)\frac{e^{-ik_1r_{c(p,s,t)}}}{r_{c(p,s,t)}}\right],$$
$$\vec{\Pi}^{м}(\vec{r},t)=\sum_{c=1}^{C}\left[\sum_{p}\sum_{s}\sum_{t}\frac{1}{k_1^3}\left(\sin k_1a_c-k_1a_c\cos k_1a_c\right)\times\left(\frac{\mu_{сэф}}{\mu_0}-1\right)\vec{H}^{0}_{c(p,s,t)}(\vec{r}',t)\frac{e^{-ik_1r_{c(p,s,t)}}}{r_{c(p,s,t)}}\right]. \quad (11)$$

$$\text{Здесь } r_{c(p,s,t)}=\sqrt{\left(x-x_{c,s}\right)^2+\left(y-y_{c,t}\right)^2+\left(z-z_{c,p}\right)^2}, \quad (12)$$

где координаты (x,y,z) – точка наблюдения рассеянного поля вне сфер решетки, координаты $\left(x_{c,s},y_{c,t},z_{c,p}\right)$ – точка нахождения центра рассеивающей сферы (1). Тогда, учитывая (10), (11), из (4) найдем искомое рассеянное сферами решетки поле

$$\vec{E}_{расс}=\sum_{c=1}^{C}\left[\sum_{p}\sum_{s}\sum_{t}\frac{1}{k_1^3}\left(\sin k_1a_c-k_1a_c\cos k_1a_c\right)\times\right.$$
$$\left.\times\left\{\left(\frac{\varepsilon_{сэф}}{\varepsilon_0}-1\right)\hat{L}_c\vec{E}^{0}_{c(p,s,t)}(\vec{r}')-ik\mu_0\left(\frac{\mu_{сэф}}{\mu_0}-1\right)\times\hat{P}_c\vec{H}^{0}_{c(p,s,t)}(\vec{r}')\right\}e^{i\left(wt-k_1r_{c(p,s,t)}\right)}\right], \quad (13)$$
$$\vec{H}_{расс}=\sum_{c=1}^{C}\left[\sum_{p}\sum_{s}\sum_{t}\frac{1}{k_1^3}\left(\sin k_1a_c-k_1a_c\cos k_1a_c\right)\times\right.$$
$$\left.\times\left\{\left(\frac{\mu_{сэф}}{\mu_0}-1\right)\hat{L}_c\vec{H}^{0}_{c(p,s,t)}(\vec{r}')+ik\varepsilon_0\left(\frac{\varepsilon_{сэф}}{\varepsilon_0}-1\right)\hat{P}_c\vec{E}^{0}_{c(p,s,t)}(\vec{r}')\right\}e^{i\left(wt-k_1r_{c(p,s,t)}\right)}\right],$$

где $\hat{L}_c$ и $\hat{P}_c$ – функциональные матрицы вида

$$\hat{L}_c=\begin{bmatrix}\Psi_{xxc}&\Psi_{xyc}&\Psi_{xzc}\\ \Psi_{yxc}&\Psi_{yyc}&\Psi_{yzc}\\ \Psi_{zxc}&\Psi_{zyc}&\Psi_{zzc}\end{bmatrix};\ \hat{P}_c=\begin{bmatrix}0&\Psi_{zc}&\Psi^{0}_{yc}\\ \Psi^{0}_{zc}&0&\Psi_{xc}\\ \Psi_{yc}&\Psi^{0}_{xc}&0\end{bmatrix}. \quad (14)$$

Величины, входящие в функциональные матрицы (14), имеют вид (1),(12)

$$\Psi_{xxc}=\frac{1}{r_{c(p,s,t)}}k^2\varepsilon_0\mu_0+\frac{3\left(x-x_{c,s}\right)^2-r^2_{c(p,s,t)}}{r^5_{c(p,s,t)}}-\frac{k_1^2\left(x-x_{c,s}\right)^2}{r^3_{c(p,s,t)}}+ik_1\frac{3\left(x-x_{c,s}\right)^2-r^2_{c(p,s,t)}}{r^4_{c(p,s,t)}},$$
$$\Psi_{yyc}=\frac{1}{r_{c(p,s,t)}}k^2\varepsilon_0\mu_0+\frac{3\left(y-y_{c,t}\right)^2-r^2_{c(p,s,t)}}{r^5_{c(p,s,t)}}-\frac{k_1^2\left(y-y_{c,t}\right)^2}{r^3_{c(p,s,t)}}+ik_1\frac{3\left(y-y_{c,t}\right)^2-r^2_{c(p,s,t)}}{r^4_{c(p,s,t)}},$$

$$\Psi_{zzc}=\frac{1}{r_{c(p,s,t)}}k^2\varepsilon_0\mu_0+\frac{3\left(z-z_{c,p}\right)^2-r^2_{c(p,s,t)}}{r^5_{c(p,s,t)}}-\frac{k_1^2\left(z-z_{c,p}\right)^2}{r^3_{c(p,s,t)}}+ik_1\frac{3\left(z-z_{c,p}\right)^2-r^2_{c(p,s,t)}}{r^4_{c(p,s,t)}},$$

$$\Psi_{xyc}=\Psi_{yxc}=\frac{3\left(x-x_{c,s}\right)\left(y-y_{c,t}\right)}{r^5_{c(p,s,t)}}-k_1^2\frac{\left(x-x_{c,s}\right)\left(y-y_{c,t}\right)}{r^3_{c(p,s,t)}}+ik_1\frac{3\left(x-x_{c,s}\right)\left(y-y_{c,t}\right)}{r^4_{c(p,s,t)}},$$

$$\Psi_{xzc}=\Psi_{zxc}=\frac{3\left(x-x_{c,s}\right)\left(z-z_{c,p}\right)}{r^5_{c(p,s,t)}}-k_1^2\frac{\left(x-x_{c,s}\right)\left(z-z_{c,p}\right)}{r^3_{c(p,s,t)}}+ik_1\frac{3\left(x-x_{c,s}\right)\left(z-z_{c,p}\right)}{r^4_{c(p,s,t)}},$$

$$\Psi_{xyc}=\Psi_{zyc}=\frac{3\left(y-y_{c,t}\right)\left(z-z_{c,p}\right)}{r^5_{c(p,s,t)}}-k_1^2\frac{\left(y-y_{c,t}\right)\left(z-z_{c,p}\right)}{r^3_{c(p,s,t)}}+ik_1\frac{3\left(y-y_{c,t}\right)\left(z-z_{c,p}\right)}{r^4_{c(p,s,t)}},$$

$$\Psi_{xc}=\frac{\left(x-x_{c,s}\right)}{r^3_{c(p,s,t)}}+ik_1\frac{\left(x-x_{c,s}\right)}{r^2_{c(p,s,t)}},\ \Psi^0_{xc}=-\Psi_{xc},$$

$$\Psi_{yc}=\frac{\left(y-y_{c,t}\right)}{r^3_{c(p,s,t)}}+ik_1\frac{\left(y-y_{c,t}\right)}{r^2_{c(p,s,t)}},\quad \Psi^0_{yc}=-\Psi_{yc},$$

$$\Psi_{zc}=\frac{\left(z-z_{c,p}\right)}{r^3_{c(p,s,t)}}+ik_1\frac{\left(z-z_{c,p}\right)}{r^2_{c(p,s,t)}},\quad \Psi^0_{zc}=-\Psi_{zc},$$

Поле в произвольной точке пространства, лежащей вне сфер, представим в виде (13):

$$\vec{E}\left(\vec{r},t\right)=\vec{E}_0\left(\vec{r},t\right)+\vec{E}_{pacc}\left(\vec{r},t\right),$$

где $\vec{E}_0\left(\vec{r},t\right)$ – невозмущенное поле падающей волны.

Заключение

Полученные соотношения могут найти применение при изучении рассеяния волн различного рода выпуклыми многогранниками, при создании на их основе новых видов ограниченных метакристаллов, в том числе и нанокристаллов с резонансными свойствами, и при изучении их поведения в различных внешних средах [4], а также при разработке методов моделирования электромагнитных явлений, которые могут происходить в реальных кристаллах в резонансных областях в оптическом и рентгеновском диапазонах длин волн [5].

Список литературы:

1. Khyzhnyak NA. The Green function of Maxwell's equations for inhomogeneous media // J. Technical Physics. 1958. Vol. 28, No. 7. P. 1952-1610 (in russian).

2. Kozar AI. Resonant metacrystals of small magnetodielectric spheres: monograph. Kharkiv : KNURE, 2014. 352 p. (in russian).

3. Kozar AI. Electromagnetic Wave Scattering with Special Spatial Lattices of Magnetodielectric Spheres // J. Telecommunication and Radio Engineering. New York, N.Y. (USA) : Begell House Inc. 2004. Vol. 61, No. 9. P. 734-749.

4. Kozar AI. Resonant Degenerate Crystal Made of Spheres Located Magnetodielectric Medium, International Journal of Electromagnetics and Applications, Vol. 3, No. 2, 2013, pp. 15-19. doi: 10.5923/j.idea.20130302.02.

5. Kozar AI. Electromagnetic lattice "invisibility" of the resonance cubic crystal made jfmagnetodielectric spheres // J. Telecommunication and Radio Engineering. New York, N.Y. (USA) : Begell House Inc. 2018. Vol. 77, issue 2. P. 155-159.

Поступила в редколлегию 02.11.2020

Сведения об авторах:

Козарь Анатолий Иванович – д-р физ.-мат. наук, профессор, профессор кафедры физики, Харьковский национальный университет радиоэлектроники, Украина; e-mail: d_ph@nure.ua, ORCID: https://orcid.org/0000-0001-9968-8674

ЗАСТОСУВАННЯ МЕТОДІВ РАДІОТЕХНІКИ

УДК 615.472.03 **DOI:10.30837/rt.2020.4.203.20**

В.В. СЕМЕНЕЦ, д-р техн. наук, В.И. ЛЕОНИДОВ, канд. техн. наук

ИССЛЕДОВАНИЕ АМПЛИТУДНО-ЧАСТОТНЫХ ХАРАКТЕРИСТИК БИОЛОГИЧЕСКИХ ТКАНЕЙ

Введение

Физические методы диагностики [1 – 8] функционального состояния биологических тканей (электротермометрия, цветовая и инфракрасная термография, капиллярная фотометрия, а также ультразвуковые методы и лазерная доплеровская флуометрия) в случае термических, механических и огнестрельных повреждений или в результате продолжительного сдавливания малоэффективны из-за разной степени поражения ткани по ходу раны и не дают возможности определить состояние каждой мышцы отдельно.

Поэтому до настоящего времени ни один из перечисленных выше методов не нашел широкого применения в практике оперативной оценки жизнеспособности (способности биологической ткани к самовосстановлению) поврежденных областей мягких тканей. В то же время хорошо известно, что при лечении поражений или при трансплантации тканей одним из важнейших условий успешного проведения операции является как можно более раннее определение границ некротических поражений. Однако надежных, широкодоступных и именно оперативных инструментальных методов оценки степени жизнеспособности тканей в настоящее время все еще не разработано.

Использование в качестве критерия оценки состояния биоткани такой физической величины как импеданса биоткани [9 – 15] основано на известном положении [10, 14], согласно которому модуль $|Z_{БТ}|$ импеданса нежизнеспособной ткани много меньше этой же величины, полученной при измерении импеданса пораженного участка биоткани. При этом величина $|Z_{БТ}|$ пораженного участка практически не зависит от частоты $f_{изм}$ используемого измерительного тока $I_{изм}$.

Для полностью жизнеспособной (непораженной) биоткани модуль импеданса есть функция частоты $|Z_{БТ}| = F(f_{изм})$. Наибольшие изменения функции $Z_{БТ}(f_{изм})$ наблюдаются в низкочастотной области при $f_{изм} < 10 кГц$.

В работе [10] вводится понятие коэффициента жизнеспособности, его еще называют коэффициентом поляризации [14], в следующем виде:

$$K_f = \frac{|Z_{f2}|}{|Z_{f1}|}, \quad \text{при} \qquad f_2 >> f_1 \tag{1}$$

Если выполняется неравенство $K_f > 1$ то принимается решение о том, что биоткань способна к самовосстановлению, в противном случае при $K_f \le 1$ принимается решение о том, что биоткань нежизнеспособна.

В выражении (1) значения частот f_1 и f_2 строго не определены, и, следовательно, критерий (1) не может гарантировать строгую определенность решения.

Также очевидно, что критерий (1) дает неопределенность решения о состоянии биоткани в области $K_f = 1 \pm \xi$, где ξ – малая величина, значение которой также является неопределенным. В общем случае область $K_f > 1$ может быть обширной и, следовательно, возникает

необходимость описания различий в состоянии биоткани при различных значениях K_f в этой области, где предположительно возможно формирование нескольких подобластей, отвечающих известному или выявленному в процессе экспериментальных исследований, набору детерминированных состояний биоткани.

Область решений $K_f = [\xi, 1]$ также может включать существенные различия в состоянии биоткани.

Кроме того, неопределенность в интерпретацию величины K_f вносят значительные флуктуации величины импеданса при повторении опытов даже для похожих или однотипных тканей и случаев поражения.

Нежизнеспособные ткани в зависимости от условий поражения и времени, прошедшего с момента поражения, могут содержать различный объем жидкой фракции (электролита), что существенно влияет на абсолютное значение импеданса исследуемой области биоткани. Эти обстоятельства приводят к трудностям однозначного определения граничных значений абсолютной величины импеданса для пораженных и непораженных участков биоткани как для биотканей различного типа, так и для различного типа и степени поражений.

Следовательно, использование только одного параметра, а именно величины абсолютного значения импеданса не является оптимальным подходом для обеспечения надежной диагностики состояния пораженной биоткани. Для развития диагностических возможностей методов импедансометрии необходимо расширить область измеряемых параметров, для чего необходимо провести исследования распределений импеданса в частотной и временной областях, с целью выявления оптимального подхода к повышению диагностических возможностей метода импедансометрии.

Цель работы – получение и анализ достаточной выборки статистического материала по частотному распределению характеристики модуля импеданса биоткани для разработки состоятельного заключения относительно их информативного содержания. Исследования проводились на биотканях растительного происхождения.

Основные положения

Для измерения амплитудно-частотных характеристик (АЧХ) биологических тканей использовалась измерительная схема, приведенная на рис. 1. Методика измерений предусматривала использование испытательных синусоидальных сигналов, которые составляют частотный ряд в диапазоне частот $D_{F=}[20\ Гц \ldots 2{,}0\ мГц]$.

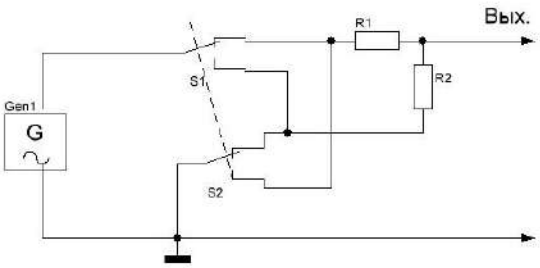


Рис. 1. Схема измерений

Эффективное значение напряжения, которое подавалось на образец ткани (резистор $R2$) через токоограничивающий резистор $R1$, составляло $U_{эф} = 1{,}5B \pm 5\%$. Величина тока через образец поддерживалась постоянной во время проведения экспериментов и при величине сопротивления резистора $R1 = 20кОм$ не превышала значения $I_{\max} \le 0{,}7 \cdot 10^{-6} A$, ошибка установки тока через образец не превышала $\delta I = \pm 5\%$. В исследовании было удобно использовать анализ зависимостей модуля напряжения на объекте. Такой метод значительно упрощал процедуру измерений и аппаратную часть экспериментов.

Размеры исследуемой области ограничены электродами игольчатого типа, расстояние между иглами $\Delta l = 10мм$, глубина погружения $\delta h = 2мм$.

В качестве исследуемых объектов использовались несколько видов растительной биологической ткани: яблоко, морковь, свекла, картофель, побеги алоэ.

Задачей исследования было определение граничных значений области изменения распределений напряжения на биологической ткани в зависимости от частоты при известных

исходных параметрах испытательных сигналов. При этом выдвигалась следующая рабочая гипотеза.

Модуль импеданса биологической ткани определяется соотношением объема живых клеток, обладающих свойством поляризации и объемом межклеточной жидкости, которая представляет собой раствор электролита. Если считать, что это соотношение для неповрежденной биологической ткани априори известно, то в результате повреждения в межклеточное пространство дополнительно поступает внутриклеточная жидкость (тоже электролит), при этом в процессе поляризации будет участвовать уже меньшее число клеток и, следовательно, модуль полного электрического сопротивления должен уменьшаться.

Нетрудно предположить, что нижним граничным значением модуля импеданса пораженной биологической ткани будет сопротивление тканевого электролита в предположении о том, что клеточная структура полностью разрушена.

Также нетрудно предположить, что проводимость тканевого электролита различна для различных типов тканей. Поэтому в качестве критерия для относительной оценки степени поражения клеточной структуры биологической ткани следует принять АЧХ некоторого «стандартного» электролита. В качестве такого эталона как показателя предельного поражения ткани целесообразно принять дисперсионную зависимость импеданса изотонического раствора соли $NaCl$ (физиологического раствора), при этом будем считать, что по мере увеличения тяжести поражения АЧХ биологической ткани стремится к АЧХ изотонического раствора. Этот критерий, возможно, будет не вполне справедлив в случае растительных биологических тканей, но мы его применяем в связи с тем, что конечной целью исследований в этой области знаний является создание системы информативных признаков для классификации состояния жизнеспособности биологических тканей животного происхождения.

Результаты экспериментальных наблюдений и их анализ

На рис. 2 приведены зависимости частотного распределения напряжения на исследуемом участке живой биологической ткани растительного происхождения. На рис. 2 приняты следующие обозначения: 1 – яблоко, 2 – изотонический раствор, 3 – картофель, 4 – картофель молодой, 5 – свекла, 6 – морковь, 7 – алоэ.

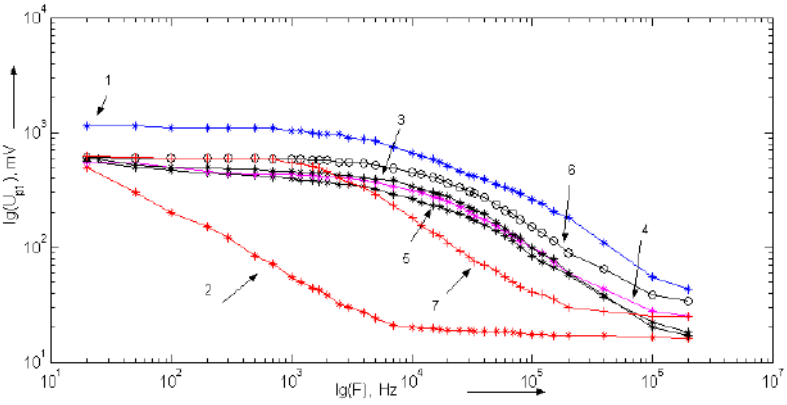


Рис. 2. АЧХ неповрежденной клеточной ткани

Анализ зависимостей на рис. 2. показывает, что в случае исследования живой клеточной структуры форма АЧХ образца биологической ткани имеет принципиальное отличие от формы АЧХ изотонического раствора.

На АЧХ биологической ткани можно выделить четыре характерных участка.

Первый участок – это относительно медленно спадающий сигнал при положительной кривизне в области частот $\Delta F_1 = [20; \ldots 1000]\ Гц$.

Второй участок в принятом логарифмическом масштабе приближается к линейному виду в диапазоне частот $\Delta F_2 = [1{,}0;\ 100]\ кГц$. На третьем участке наблюдается спад сигнала с отрицательной кривизной. Этот участок для всех образцов имеет малый диапазон частот: $\Delta F_3 = [100;\ 200]\ кГц$ для алоэ и $\Delta F_3 \cong 1000\ кГц$ для остальных типов исследуемых тканей. На четвертом участке сигнал почти не зависит от частоты в области частот $\Delta F_4 > 1\ мГц$.

В принятых координатах частотная зависимость для изотонического раствора явно отличается от АЧХ живой биологической ткани. На этой зависимости (кривая 2 на рис. 2) наблюдаются два явно различающихся участка. На первом участке в диапазоне частот

$\Delta F_{1fz} \cong [20; \ldots 7000]\ Гц$ наблюдается близкое к линейному уменьшение сигнала. На частотах $\Delta F_{2fz} > 7000\ кГц$ величина сигнала почти не зависит от частоты.

Из проведенного анализа следует предположение о том, что при некоторой промежуточной степени поражения биологической ткани АЧХ сигнала также будет приобретать некоторую промежуточную форму между кривой 2 и, например, кривой 1. Для проверки этой гипотезы были измерены АЧХ биологических тканей, которые подверглись замораживанию различной степени с последующим медленным нагревом до комнатной температуры. Графическое изображение полученных АЧХ приведены на рис. 3.

Анализ зависимостей рис. 3. подтверждает выдвинутую гипотезу о приближении формы АЧХ к АЧХ изотонического раствора по мере увеличения тяжести поражения. В этом эксперименте образцы растительной биологической ткани подвергались замораживанию путем выдержки в морозильной камере холодильника. Кривая 1 представляет собой АЧХ биологической ткани яблока, которая находилась в морозильной камере в течение 15 мин с последующим нагревом в комнатных условиях. Зависимость 2 получена на яблочной ткани после выдержки в морозильной камере в течение 30 мин. Кривая 3 и 5 представляют АЧХ полученные на картофеле и яблоке после их выдержки в морозильной камере в течение 2 час. Зависимость 4 представляет АЧХ изотонического раствора.

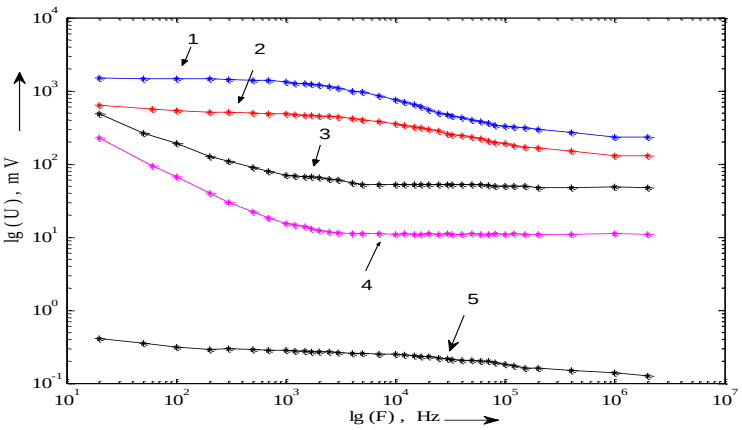


Рис. 3. АЧХ поврежденной клеточной ткани

Полученные результаты наглядно демонстрируют явно выраженное приближение формы зависимости к зависимости, полученной для изотонического раствора.

Также видно отличие после сильного замораживания яблочной ткани, в результате чего произошло полное разрушение клеточной структуры и измерения проводились по существу на жидкой фракции, представляющей смесь межклеточного и внутриклеточного электролитов. Видно, что модуль импеданса яблочного электролита значительно меньше, чем для изотонического раствора. Это явление можно объяснить значительным различием химического состава и, по-видимому, различием в плотности растворов. Для биологических тканей животного происхождения это явление наблюдаться не будет.

Полученный результат показывает, что форма АЧХ может служить информативным признаком объемного содержания здоровых клеток в исследуемом объеме биологической ткани и, следовательно, может служить признаком ее жизнеспособности.

Выводы

Основным результатом работы является обоснование информативности метода частотного анализа импеданса биологических тканей для диагностики их способности к самовосстановлению после полученных повреждений.

Также показано, что метод оценки жизнеспособности биологических тканей, построенный на принципе анализа АЧХ, имеет существенный недостаток, состоящий в том, что для получения этой характеристики требуется относительно большой интервал времени и достаточно сложная и, следовательно, дорогостоящая аппаратная реализация. Так, для синтеза частоты $f = 250\ кГц$ потребуется работа цифро-аналогового преобразователя на частоте $f \geq 5{,}0 \cdot 10^6\ Гц$.

Последующие работы, проводимые нами в области развития научного направления импедансометрии биотканей, будут направлены на проведение исследований по разработке и

созданию экспериментального образца, построенного на принципе измерения и анализа сигналов переходного процесса, возникающего в биологической ткани при подаче на нее импульса микротока, при котором реализуется анализ сигналов во временной области взамен анализу в частотной области. Такой подход в литературных источниках не описан, однако он представляется наиболее перспективным, так как время, затрачиваемое на анализ, ориентировочно составляет величину $t_{изм} \cong 0{,}2\,c$. Также при этом значительно упрощается аппаратная часть устройства.

Список литературы

1. Гэстищев В. К и др. Тепловидение в ранней диагностике гнойных воспалительных заболеваний мягких тканей и при контроле за течением раневого процесса // Сб. науч. тр. 1985. С. 482 – 484.
2. 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.
3. Isogai N. Application of medical thermography to the diagnosis of Freys syndrome // Head Neck. 1997. №19: 2. P.143 – 147.
4. Иванов В. В., Бачаури Н. М. Роль тепловидения в диагностике облитерирующих заболеваний сосудов нижних конечностей // Хирургия. 1992. № 5. С. 38 – 40.
5. Труфанов Г. Е., Дмитращенко А.А., Борисенко Л. В. и др. Спиральная компьютерная томография в диагностике множественной и сочетанной травмы // Медицина катастроф. 2006. № 4. С. 51.
6. 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.
7. 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.
8. Лежнев К.К. Сравнительная оценка методов определения жизнеспособности мягких тканей при огнестрельных повреждениях : автореф. дис. ... канд. мед. наук. 1990. 19 с.
9. Thomasset A. Bio-electrical properties of tissue impedance measurements // Lyon Med. 1962. № 207. P. 107–118.
10. Тарусов Б.Н. Электропроводность как метод определения жизнеспособности тканей // Архив биологических наук. 1938. Т. 52. Вып. 2. С. 178-1811.
11. Тарусов Б.Н. Сравнительные данные по измерению электропроводности различных тканей // Бюлл. эксп. биол. мед. 1943. № 15 (4–5). С. 44 – 50.
12. Тихомиров А.М. Импеданс биологических тканей и его применение в медицине. Москва : РГМУ, 2006. 12с.
13. Торнуев Ю.В., Колдышева Е.В., Лапий Г.А., Балахнин С.М., Бушманова Г.М., Преображенская В.К. Электроимпедансометрия в гистологической технологии // Биологические науки. Фундаментальные исследования. 2013. №6. С. 1164 – 1167.
14. 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 78(1), pages 71-78 DOI: 10.1615/ TelecomRadEng, v78.i1.80, 2019.
15. 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.

Поступила в редколлегию 04.11.2020

Сведения об авторах:

Леонидов Владимир Иванович – канд. техн. наук, с. н. с. кафедры биомедицинской инженерии, Харьковский национальный университет радиоэлектроники, Украина; e-mail:volodymyr.leonidov@nure.ua, ORCID: https://orcid.org/0000-0001-5218-3177

Семенец Валерий Васильевич – д-р техн. наук, проф., ректор, Харьковский национальный университет радиоэлектроники, Украина; e-mail: valery.semenets@nure.ua, ORCID: https://orcid.org/0000-0001-8969-2143

ОБРОБКА СИГНАЛІВ

УДК 004.932 **DOI:10.30837/rt.2020.4.203.21**

V.A. DUSHEPA, Y.A. TIAHNYRIADNO, I.V. BARYSHEV, D. Sci.

IMAGE REGISTRATION COMPARATIVE ANALYSIS: NORMALIZED CORRELATION VERSUS SIFT-BASED REGISTRATION

Introduction

Until now, a large variety of different image registration algorithms have been developed. They can usually be divided into two groups: area- (or intensity-) based and feature-based [1, 2]. It should also be noted that a new direction is actively developing now when trained neural networks are used as a measure of similarity [3].

Intensity-based algorithms are commonly used to determine the shift between images when there is little or no rotation and scale changes. If the considered model of geometric transformation between images is more complex (where, for example, the presence of rotation and change in scale cannot be neglected), then either the reliability of such algorithms drops sharply, or an excessive amount of computation is required for their normal operation (because it is necessary to iterate over all possible sets of transformation parameters, each time calculating the correlation measure of similarity). The most common among this group of methods are correlation methods.

At the same time, feature-based methods work quite stably with a variety of models of geometric transformations. However, their accuracy is inferior to correlation methods. Also, they are often inferior in speed [4]. Among the methods using the calculation of features, the most important place is occupied by the methods based on keypoints. In this case, the search (detection) of keypoints is first carried out on two images that are registered. Let's call one of them (usually larger) the reference image (RI), and the second image – the current image (CI). Then a descriptor is calculated for each keypoint. A descriptor is some array of values that describes this keypoint. As a result, we will have a set of descriptors for RI and a set of descriptors for CI. If we find correspondences between them, then we can estimate the geometric transformation between the images (using the found correspondences between the keypoints).

For comparison, from the group of intensity-based methods, the classic variation of the normalized cross-correlation method (further NCC to denote an algorithm) was chosen [5, 6], one of the most popular correlation methods. As a representative of the second group of methods, an algorithm that uses a SIFT detector (and a keypoint descriptor) was chosen [7]. SIFT was created at the turn of the 21st century. And, although since then there have been many different improvements to the original algorithm (for example, in [8]), this work uses the classic implementation available in the OpenCV package [9]. This should be enough to investigate the basic patterns and obtain approximate quantitative characteristics.

Aim and tasks of the research. The purpose of this work is to compare qualitatively and quantitatively (including computational performance) algorithms from two main classes. There are many works making comparisons within each class (for example for intensity-based – [10], feature-based – [11]) but almost no between different classes. A comparison of the two algorithms considered in the article will allow, in addition to confirming the obvious general patterns, to obtain specific indicators of quality and reliability, which are useful to understand when choosing a tool for registering images.

Also in the second part of the work, it is shown (and quantified) that the use of a combined algorithm (using the SIFT at the first stage, and the NCC at the second stage) allows to join the advantages of both approaches and achieve high estimation accuracy for complex geometric transformation models.

The novelty of this work is not the ideas of the approaches themselves, which are generally known, but specific numerical performance indicators calculated by a simulation experiment (including real terrain maps as images that are registered).

1. Simulation setup

The comparison was performed using a simulation model created in the Python programming language (with using OpenCV, SciPy [12], and NumPy [13] libraries). The structure of the computational experiment is shown in Fig. 1.

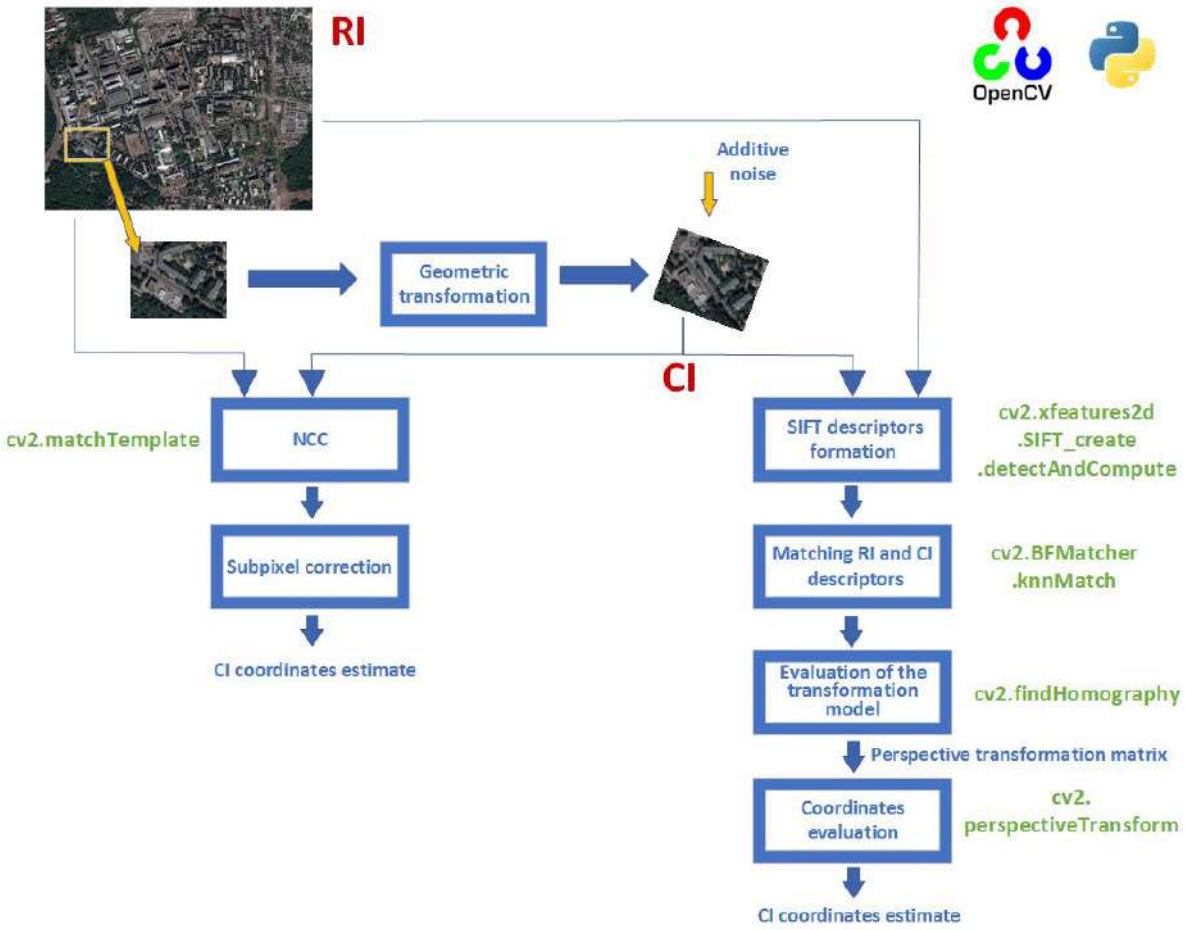


Fig. 1. The structure of the simulation experiment
(the elements of the OpenCV library that implement each of the stages are indicated)

First, a reference image is selected, for example, a satellite image (or its region). Then the model randomly selects a fragment of a given size (in section 2.1 the fragment of 200 by 200 pixels was used, and 50x50 – in the 2.2 section) of this image, adds distortion (rotate, scale, add random subpixel shift and noise). So we got CI. We passed RI and CI to both registration algorithms (NCC and SIFT-based). The coordinates of the CI relative to RI were estimated. We considered the position of the CI center to be the coordinates of the CI.

In the CI formation model, we calculated new pixel positions after geometric transformation and then used bicubic interpolation to find their intensities. In all experiments, the values of the subpixel shifts along X and Y were modeled with a uniform distribution in the intervals from -0.5 to 0.5.

The matchTemplate function (from OpenCV) performed an NCC evaluation. Also for the NCC, the gradient method of subpixel shift correction was used [5].

Implementations of SIFT feature selection algorithms and feature matching of two images are taken also from the OpenCV library. The descriptors are first calculated using the detectAndCompute method of the SIFT_create class. The resulting descriptors of the two images (RI and CI) are then matched. OpenCV implements two matching methods, BFMatcher and Flann, and all experiments in the work were performed using the BFMatcher class, which showed higher performance than Flann in our case. After that, the findHomography and getPerspectiveTransform functions are used to calculate the coordinates of the CI relative to RI.

The process of forming a CI and searching for it in the original image (RI) was repeated 100 times for each of the parameter sets. Based on these tests, the probability of correct registration (P) and the root-mean-square error (RMSE) were then calculated. The registration was considered erroneous when the obtained estimate of the CI position differed from the true value by more than 2 pixels. All of the following results were obtained with a signal-to-noise ratio of 20 (the standard deviation of the image was 20 times greater than the noise).

2. Experiment results

2.1. NCC and SIFT for real images registration

We used two main images (as RI) in our experiments: a real terrain snapshot of the National aerospace university “Kharkov aviation institute” (downloaded using [14], see Fig. 2, *a*) and a raccoon picture (Fig. 2, *b*).

a *b*

Fig. 2. Test images (RI): *a* – satellite image of the territory of NAU "KhAI", 1000x1000; *b* – raccoon image, 1280x1080

The SIFT descriptor is a vector with 128 values. For the RI from Fig. 2, *a*, the algorithm finds 17453 keypoints. While for a fragment (CI), the number will vary (depending on the fragment) from 500 to 800 keypoints.

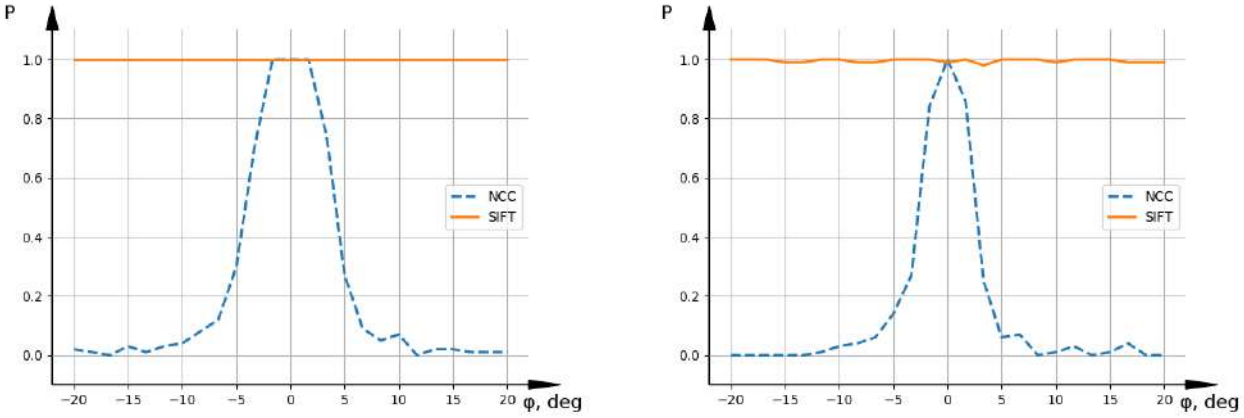
The average runtime for NCC is 0.0264 seconds. For the SIFT-based algorithm, this value is 0.44 seconds. If we consider that the keypoints for the RI are calculated in advance, then the execution time decreases to 0.1 seconds, which is still almost four times longer than for NCC.

At first, the rotation (φ) and the scaling change (s) were not simulated. In this case, the probability of correct matching for both algorithms was equal to 1 for signal-to-noise ratios greater than 10 (modern video cameras provide very low noise levels). The RMSE was less than 0.05 pixels (slightly lower for NCC compared to SIFT). Thus, in the absence of changes in scale and rotation, we can emphasize a slight advantage of the NCC in the accuracy.

Now let's analyze what will happen if there are a rotation and a change in scale (not taken into account in the NCC algorithm).

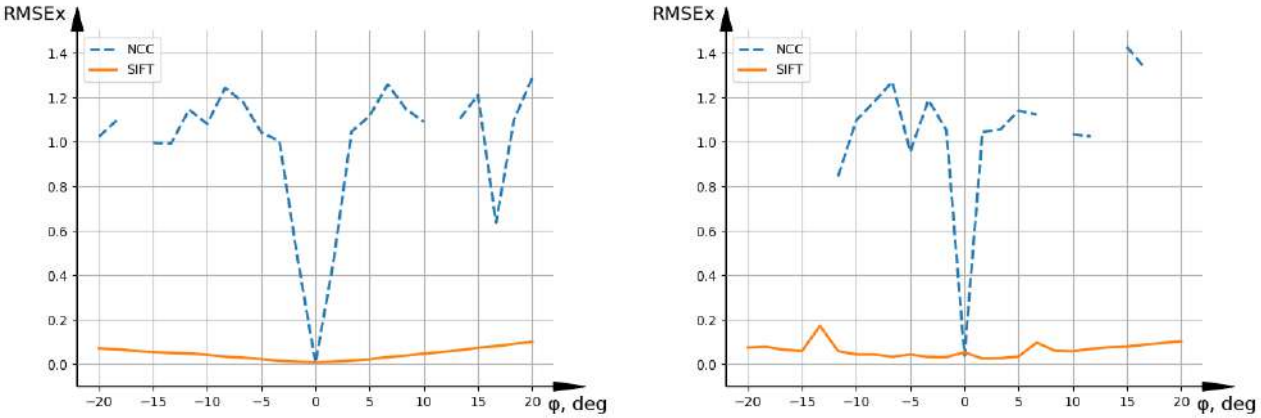
In Fig. 3 you can see that for NCC the probability of successful registration P begins to decline sharply when the absolute value of rotation angle is more than about 2 degrees for the image in Fig. 2, a and 1 degree – in Fig. 2, *b*. In Fig. 4, we see that the accuracy of the NCC registration also worsens when the absolute value of the angle increases. At the same time, the probability of the SIFT-based algorithm is almost always equal to one and the accuracy only slightly deteriorates with increasing angle modulus. If P is equal to zero, then the RMSE cannot be calculated, therefore the RMSE graphs have gaps.

We see a similar situation in the presence of scale distortion (in this work, only figures for the probability of correct registration are provided). With increasing scaling, the results of the NCC drop sharply. This appears earlier for the image in Fig. 2, *a*, which is obviously less "smooth" and accordingly has a higher frequency content.



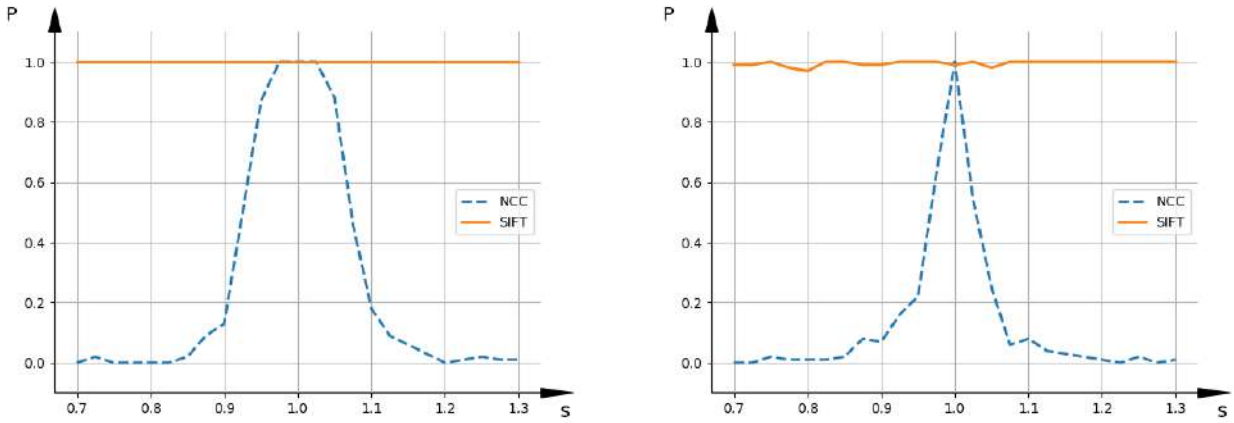
a *b*

Fig. 3. Effect of rotation φ on the probability of correct registration P: *a* – for the image in Fig. 2, *a*; *b* – for the image in Fig. 2, *b*



a *b*

Fig. 4. Effect of rotation φ on the RMSE (on X-axis): *a* – for the image in Fig. 2, *a*; *b* – for the image in Fig. 2, *b*



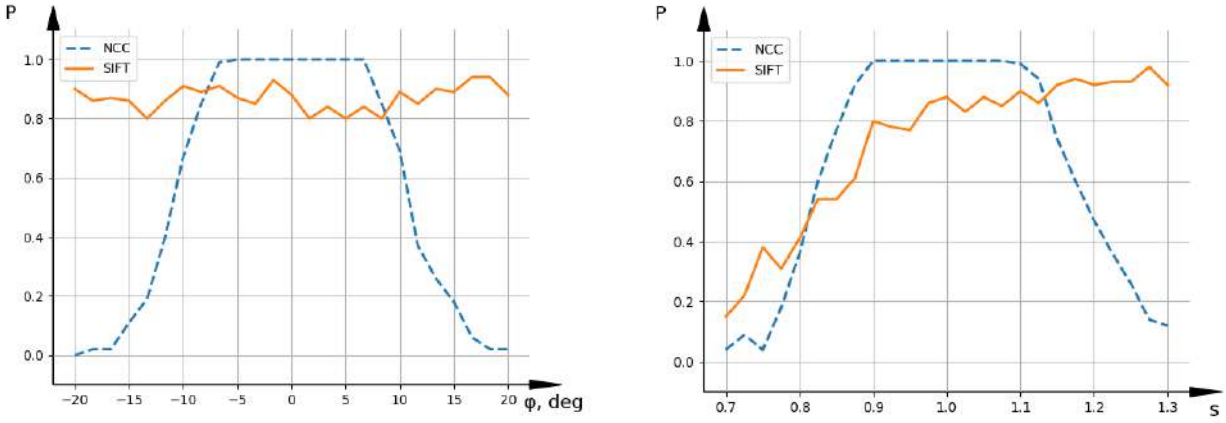
a *b*

Fig. 5. Effect of scale s on the probability of correct registration P: *a* – for the image in Fig. 2, *a*; *b* – for the image in Fig. 2, *b*

2.2. Small CI case (50x50)

If in previous experiments a CI with a size of 200x200 was used, then this checks what will happen with smaller fragments. Fig. 6 shows plots of P versus rotation and scale change (for the image in Fig. 2, *a*). It can be seen that the SIFT-based algorithm starts to work much worse. This is

because it is not always possible to select a sufficient number of keypoints for such a small CI. Although in such case it is possible to improve the situation somewhat by using keypoint selection settings (for example, changing the threshold for Lowe's ratio test [7], and, accordingly, choosing unreliable keypoints), the SIFT-based algorithm will have problems when working with small fragments.



a *b*

Fig. 6. Probability of correct registration P for small CI (50x50) and RI from Fig. 2, *a* with respect to: *a* – rotation φ; *b* – scale s

2.3. Combining SIFT-based registration and NCC

In this subsection, a two-stage algorithm was investigated, when the SIFT-based algorithm is used at the first stage, and then the obtained estimates are set as initial values for the modified NCC at the second stage. The modified NCC consists in solving an optimization problem with the NCC objective function in four parameters: shifts along X and Y axes, rotation, and scale. Such an algorithm was used, for example, in the work [15]. As can be seen from Fig. 7, this two-step algorithm is rotationally resistant (it behaves similarly for the scaling) and provides high accuracy. But at the same time, it requires almost 10 times more computational costs compared to the SIFT-based algorithm (with RI descriptors precomputation).

It should also be noted that such a high accuracy (thousandths of a pixel) as in Fig. 7 became possible due to the complete coincidence of the interpolation algorithms, which were used in the CI formation model and the registration algorithm. In reality, this is not the case, which leads to noticeably higher RMSE (at least hundredths of a pixel).

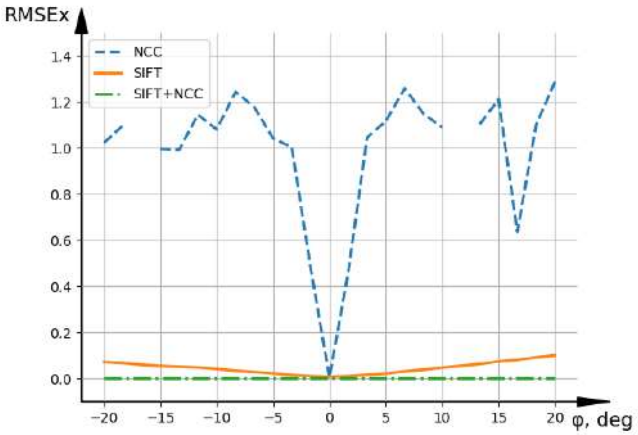


Fig. 7. Effect of rotation φ on the RMSE (on X-axis) for the image in Fig. 2, *a* (similar to Fig. 4, *a*, with a SIFT+NCC graph)

Conclusions

A comparative analysis of known registration algorithms belonging to different classes (based on pixel intensities or features) was carried out. Based on the above results, we see that SIFT-based registration is, although less accurate, but much more resistant to rotation and scale changes than the classical NCC. For the NCC, already starting from the rotation of 2 degrees (approximately, depends on the image) and a change in scale by 2 percent, the correct registration probability drops dramatically.

For a SIFT-based algorithm, it can be a problem to use small images in registration. For 50x50 fragments, the deterioration in the registration quality was already noticeable.

The two-stage algorithm considered in subsection 2.3 (SIFT+NCC) allows one to obtain an accurate algorithm that is resistant to rotation and scaling, but this will be accompanied by high computational costs (almost 10 times more than for the SIFT-based algorithm).

References:

1. Zitová B., Flusser J. Image registration methods: A survey // Image Vis. Comput. 2003. Vol. 21 (11). P. 977 – 1000.
2. Brown L. G. A survey of image registration techniques // ACM Comput. Surv. 1992. Vol. 24, No. 4. P. 325–376.
3. Uss M. L., Vozel B., Lukin V. V., Chehdi K. Efficient discrimination and localization of multimodal remote sensing images using CNN-based prediction of localization uncertainty // Remote Sensing. 2020. Vol. 12, No. 4., 703.
4. Conte G., Doherty P. Vision-based unmanned aerial vehicle navigation using georeferenced information // EURASIP J. Adv. Signal Process. 2009. Vol. 2009, Article 387308.
5. Душепа В., Усс М. Сравнительный анализ субпиксельных алгоритмов при совмещении изображений // Радіоелектронні і комп'ютерні системи. 2011. № 4. С. 41–51.
6. Gonzalez R. C., Woods R. E. Digital Image Processing, 4th ed. Pearson/Prentice Hall, 2018.
7. Lowe D. G. Distinctive image features from scale-invariant keypoints // International Journal of Computer Vision. 2004. Vol. 60, No. 2. P. 91–110.
8. Arandjelović R., Zisserman A. Three things everyone should know to improve object retrieval // 2012 IEEE Conference on Computer Vision and Pattern Recognition, Providence, RI. 2012. P. 2911-2918.
9. Bradski G. The OpenCV Library // Dr. Dobb's J. Softw. Tools. 2000.
10. Антюфеев В. И., Быков В. Н. Сравнительный анализ алгоритмов совмещения изображений в корреляционно-экстремальных системах навигации летательных аппаратов // Авиационно-космическая техника и технология. 2008. № 1 (48). С. 70 – 74.
11. Karami E., Prasad S., Shehata M. Image matching using SIFT, SURF, BRIEF, and ORB: performance comparison for distorted images // Proceedings of the 2015 Newfoundland Electrical and Computer Engineering Conference, St. John's, Canada. 2015.
12. Virtanen P. et al. SciPy 1.0: Fundamental algorithms for scientific computing in Python // Nature Methods. 2020. Vol. 17(3). P. 261-272.
13. Harris C. R. et al. Array programming with NumPy // Nature. Vol. 585. P. 357–362.
14. SASGIS. Веб-картография и навигация [Электронный ресурс]. Режим доступа: http://www.sasgis.org/sasplaneta
15. Dushepa V. A machine learning approach for image registration accuracy estimation // 2020 IEEE Ukrainian Microwave Week (UkrMW), Kharkiv, Ukraine. 2020. P. 368–372.

Received 05.10.2020

Відомості про авторів:

Душепа Віталій Анатолійович – ст. викладач кафедри аерокосмічних радіоелектронних систем (№ 501), Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», Україна; email: v.dushepa@khai.edu, ORCID: http://orcid.org/0000-0001-6105-3761

Тягнирядно Єгор Андрійович – бакалавр, Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», Україна; email: monkeber@gmail.com

Баришев Ігор Володимирович – д-р технічних наук, професор, професор кафедри аерокосмічних радіоелектронних систем (№ 501), Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут»,Україна; email: biv1937@ukr.net

УДК 004.89:621.396 **DOI:10.30837/rt.2020.4.203.22**

В.В. ЖИРНОВ, канд. техн. наук, С.В. СОЛОНСКАЯ, канд. техн. наук

СЕМАНТИЧЕСКИЙ АНАЛИЗ ФЛУКТУАЦИЙ РАДИОЛОКАЦИОННОЙ ПАЧКИ ДЛЯ ИДЕНТИФИКАЦИИ ВОЗДУШНЫХ ОБЪЕКТОВ

Введение

Недостаток классических радиолокационных систем состоит в низкой автоматизации процессов обработки данных, в том числе семантического анализа амплитудных флуктуаций пачки во временной области в интересах идентификации воздушных объектов. В статье приводится пример реализации разработанного авторами метода семантического анализа амплитудных флуктуаций пачки во временной области на основе математического аппарата алгебры конечных предикатов (АКП). Метод основан на определении семантических составляющих на этапе формирования и анализа символьной модели пачки импульсных сигналов от подвижных летательных аппаратов. Символьная модель пачки описывается предикатной функцией на множестве импульсных сигналов, превысивших некоторое пороговое значение. Для идентификации типов флуктуаций пачки вводятся предикаты-признаки, по их сочетанию любой вид флуктуации однозначно соотносится с одним из типов согласно разработанным уравнениям предикатных операций.

Известно описание детерминированных, дискретных и конечных интеллектуальных процессов [1 – 4], которые могут быть ориентированы на совершенствование информационной технологии обработки радиолокационных сигналов и ее практическое использование. Для описания семантической составляющей процессов обработки спектральных изображений необходим язык отношений и действий над ними. Понятие отношения эквивалентно понятию предиката. Алгебраический аппарат предикатов и предикатных операций эффективен и удобен для описания различной формализуемой информации, в том числе радиолокационной, а также моделирования деятельности оператора (эксперта) обзорной РЛС [5 – 8]. Использование АКП позволило приступить к формальному описанию абстрактных понятий, которыми пользуется оператор обзорной РЛС.

Цель и задачи исследования

Семантический анализ флуктуаций радиолокационной пачки для идентификации воздушных объектов – это получение семантических составляющих в процессе анализа амплитудных флуктуаций радиолокационной пачки. Объектами исследования являются логические отношения, учитывающие зависимые связи между компонентами амплитудных составляющих флуктуаций радиолокационной пачки либо отличительные особенности различных изображений, каковыми могут являться количество максимумов, расстояния между ними.

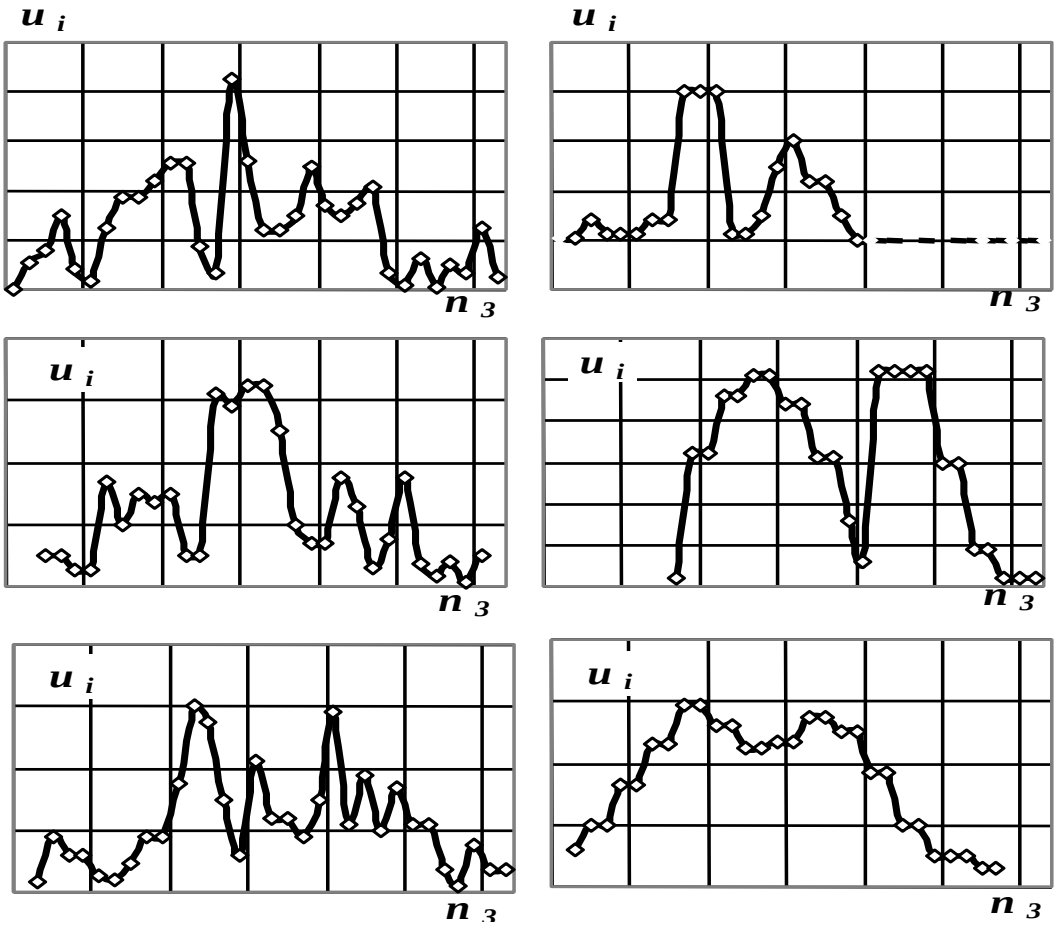
В работе рассматривается метод семантического анализа амплитудных флуктуаций радиолокационной пачки на основе предикатной модели процессных знаний формирования и анализа символьной модели совокупности импульсных сигналов от подвижных летательных аппаратов типа самолет, вертолет, БПЛА, и от мелких (точечных) атмосферных неоднородностей типа «ангел-эхо». Модель имеет пачечную структуру, и в результате семантического анализа амплитудных флуктуаций пачки во временной области необходимо получить классификационные отличительные признаки флуктуаций пачки от мешающих отражений и воздушных объектов. Необходимо исследовать семантические составляющие принятия решений, которые подобны алгоритмам принятия решений человеком-оператором. Разработать алгоритм и программно реализовать метод семантического анализа флуктуаций радиолокационной пачки для идентификации воздушных объектов в обзорных РЛС.

Семантическая модель радиолокационной пачки от точечных летательных аппаратов и мешающих отражений типа «ангел-эхо»

Семантическая модель процессных знаний формирования и анализа амплитудой картины пачки импульсных сигналов – это математическое описание процедур и отношений

при восприятии и анализе сигналов человеком-оператором в виде различительных признаков (или свойств) для определения типов объектов. Такое математическое описание процессов деятельности эксперта называется идентификацией. Процессы действий эксперта можно идентифицировать прямо и косвенно. При прямой или логической идентификации действий оператора рассматриваем, что для определенного действия оператора поступают сигналы (виды амплитудных флуктуаций пачки), выбираемые из некоторого множества амплитудных составляющих пачки, и регистрируются ответные сигналы. Всевозможные ответные сигналы деятельности оператора образуют множество.

В ходе исследований типов флуктуаций пачки использовались реальные экспериментальные данные (рис. 1), полученные на обзорной РЛС сантиметрового диапазона (длительность импульса 1 мкс, частота зондирования 365 Гц, период обзора 10 с).



а *б*

Рис. 1. Пачки импульсов отражений от ангел-эхо (*а*) и от воздушных объектов (б)

В результате анализа виды типов картин флуктуаций радиолокационной пачки в амплитудной области для мешающих отражений типа «ангел-эхо» и воздушных объектов классифицированы на некоторое количество типов S_j, $j = \overline{1,n}$ (рис. 2).

В разработанную модель входят процедуры формализации и анализа геометрического сигнального образа пачки от наблюдаемых объектов на основе алгебры предикатов [9 – 11] и операций создания предикатной модели процессных знаний для получения решений о наблюдаемых объектах локации на основе методов интеллектуального анализа реальных процессов.

Пусть $M = \{q_{11}, q_{12}, ..., q_{ij}, ..., q_{mn}\}$ – фиксированное множество, представляющее собой прямоугольную матрицу $\|A\|$ размерностью $M \times N$, состоящее из элементов $k = m \times n$ – значений амплитуд сигналов в элементах обработки зоны обзора РЛС, а B – некоторое из его подмножеств $B \subseteq M$, амплитуды сигналов которого q_{ij} превышают пороговые значения V_{ij}. Составляем набор логических элементов t_{ij} по следующему принципу: если $q_{ij} \in B$, то $t_{ij} = 1$; если $q_{ij} \notin B$, то $t_{ij} = 0$, $i = \overline{1,m}$, $j = \overline{1,n}$.

Предикат $A(x)$ на множестве M, соответствующий множеству B элементов обработки, превысивших порог, с характеристикой $(t_{11}, t_{12}, \cdots, t_{ij}, \cdots, t_{mn})$, запишется формулой

$$A(x) = t_{11}x^{q_{11}} \vee ... \vee t_{mn}x^{q_{mn}} = \bigvee_{i=1,\, j=1}^{mn} t_{ij}x^{q_{ij}} \tag{1}$$

Здесь выражение $x^{q_{ij}}$ – форма узнавания события. Когда $x = q_{ij}$, то $x^{q_{ij}} = 1$.

Предикатная модель процессных знаний о символьной модели радиолокационных отметок в общем виде – это система n унарных и бинарных предикатов Z_j:

$$M = \{Z_j, \ \ j = 1...n\}. \tag{2}$$

Такая система предикатов позволяет описать ситуацию вокруг анализируемой в данный момент информационной ячейки и позволяет формализовать процесс формирования символьного изображения флуктуаций отметки $A(x)$ в течение нескольких циклов зондирований РЛС. Их еще называют атрибутами или предикатными признаками процесса. Например, для радиолокационных систем обзора пространства это могут быть:

– унарный предикат Z_{pij} присутствия или наличия сигнала в a_{ij} информационной ячейке (i, j – номера элементов зоны обзора РЛС);

– бинарный предикат Z_{dij} ухода сигнала a_{ij} в соседнюю по дальности информационную ячейку;

– бинарный предикат Z_{aij} перехода сигнала в смежную по азимуту или соседнюю информационную ячейку, прилегающую к рассматриваемой ячейке.

При таких исходных условиях предикатные признаки формируются по следующему правилу:

$$Z_{pij} = 1, \text{ при } A_{ij} > 0 \tag{3}$$

$$Z_{dij} = 1, \text{ при } A_{i-1j} > 0 \wedge Z_{pij} = 1 \tag{4}$$

$$Z_{aij} = 1, \text{ при } Z_{pij} = 1 \wedge A_{ij-1} > 0, \tag{5}$$

где $A(x)$ – предикат события наличия-отсутствия сигнала в соответствующем элементе анализа.

Для радиолокационных станций (РЛС) обзора пространства амплитудная картина флуктуаций огибающей пачки описывается двумя составляющими [7, 8]:

1. Предикатным признаком символьной модели пачки сигналов (отметок) воздушных объектов, определяемым как решение уравнения

$$I_{m1} = Z_{mij} = \bigwedge_{l_1}^{l_n} Z_{ai,\, j+l_n} = Z_{ai,\, j+l_1} \wedge Z_{ai,\, j+l_2} \wedge \cdots \wedge Z_{ai,\, j+l_{n-1}} \wedge Z_{ai,\, j+l_n} = 1; \tag{6}$$

2. Предикатной моделью амплитудных флуктуаций радиолокационной пачки, определяемой как совокупность произведений каждого элемента символьной пачки на их амплитудные значения:

$$I_{m2} = q_{i,\,j+l_1} Z_{ai,\,j+l_1} \vee \ldots \vee q_{i,\,j+l_n} Z_{ai,\,j+l_n} = \bigvee_{l_1}^{l_n} q_{i,\,j+l_n} Z_{ai,\,j+l_n}, \qquad (7)$$

где l_1, l_n – номера элементов начала и конца пачки.

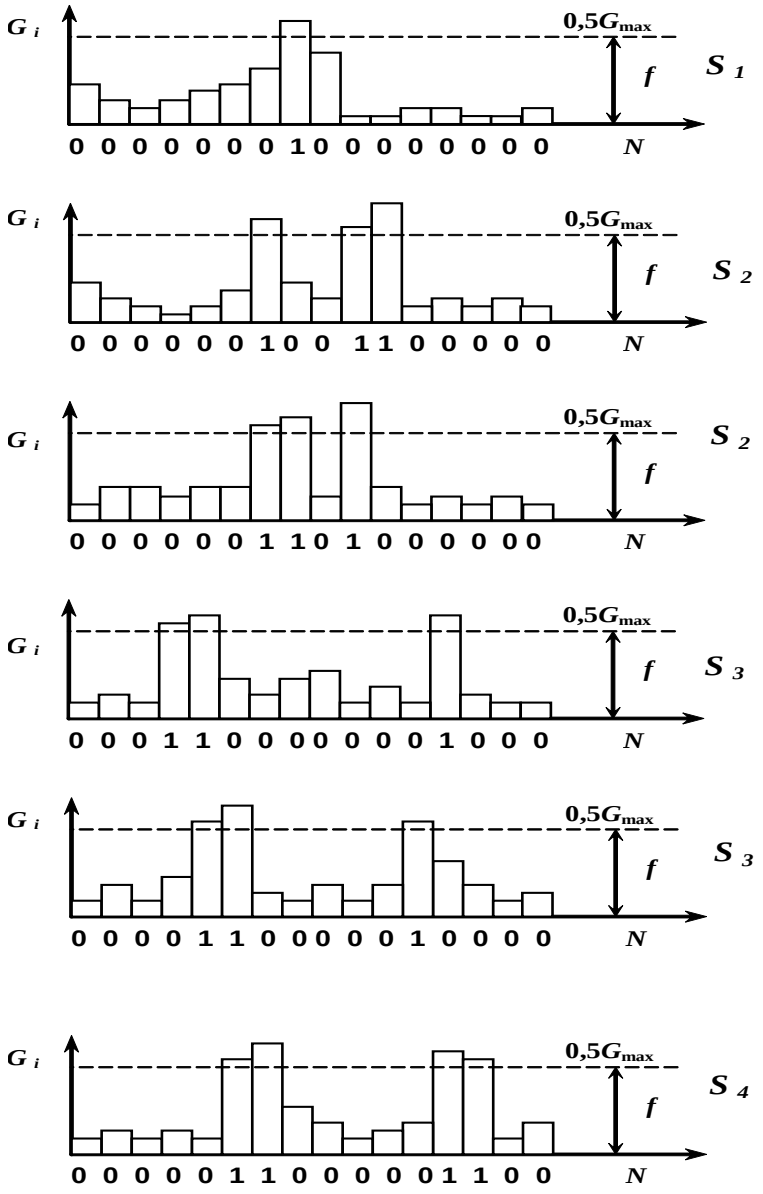


Рис. 2. Типы амплитудных картин флуктуаций пачек импульсов S_j, $j = \overline{1,4}$ и их предикатные функции $A(x)$ в виде кода, как результат превышения порога $0,5\,G_{\max}$

Метод семантического анализа амплитудных флуктуаций радиолокационной пачки на основе предикатной модели процессных знаний о символьной модели

Семантический или смысловой анализ амплитудных флуктуаций радиолокационной пачки проведен на логическом уровне обработки с помощью алгебры конечных предикатов

[9, 10]. Для анализа используем разработанную предикатную модель I_{m2} (7) амплитудных флуктуаций радиолокационной пачки, определяемой как совокупность произведений каждого элемента символьной пачки $Z_{ai,\,j+l_n}$ на их амплитудные значения $q_{i,\,j+l_n}$:

$$I_{m2} = q_{i,\,j+l_1} Z_{ai,\,j+l_1} \vee \ldots \vee q_{i,\,j+l_n} Z_{ai,\,j+l_n} = \bigvee_{l_1}^{l_n} q_{i,\,j+l_n} Z_{ai,\,j+l_n} .$$

Пусть $M = \{ q_1, q_2, ..., q_n \}$ – множество, состоящее из n элементов – значений амплитудных составляющих пачки, A – некоторое из его подмножеств $A \subseteq M$, амплитудные составляющие q_i которого превышают некое пороговое значение $|G_n| = |G_{max}|/2$. Для множества M составляем набор логических элементов $(t_1, t_2, ..., t_n)$ по следующему правилу: если $q_i \in A$, то $t_i = 1$; если $q_i \notin A$, то $t_i = 0$, $i = \overline{1,n}$. Набор $(t_1, t_2, ..., t_n)$ является характеристикой множества A как амплитудной картины радиолокационных сигналов от воздушных объектов.

Каждый тип амплитудной картины S_j, приведенный на рис. 2, имеет соответствующие нули и единицы согласно предикатной функции $A(x)$. Тип S_1 имеет одиночные группы единиц среди всех остальных нулей. Тип S_2 имеет две группы единиц, а количество нулей между ними меньше или равно двум.

Для идентификации с амплитудными типами была сформирована система предикатов-признаков L_i, чувствительных к количеству и разрывности нулей, единиц и групп сомкнутых единиц (амплитудных пиков) в предикате $A(x)$.

Был введен еще один вид предиката – F(y), построенный на множестве F, элементы $f_1, f_2, ..., f_{k-1}$ которого определены путем суммирования по модулю два каждого элемента t_i со смежным элементом. Для определения количества амплитудных пиков использована арифметическая сумма Φ предиката $F(t)$ $\Phi = \sum_{i}^{k-1} f_i = \sum_{i=1}^{k-1} [t_i + t_{i+1}] | M_2$, где индекс $|M_2$ означает суммирование по модулю два. Анализ возможных значений Φ для различных типов амплитудных картин показывает, что для одиночной группы сомкнутых единиц в множестве F результат суммирования всегда равен двум, независимо от ширины пика, т.е. от количества сомкнутых единиц. Для двух групп сомкнутых единиц результат такой операции равен четырем, для трех пиков – шести и т.д. В признаке $L_1^{j_i}$, верхний индекс j_i указывает на наличие в предикате f(x) на количество амплитудных пиков и определяется по следующему правилу: если $\Phi \geq 2$, то $j_i = \Phi/2$, иначе $j_i = 0$. В модели $j_i = P_i$.

Введен признак $L_2^{l_i}$, верхний индекс которого или номер предиката l_i указывает на количество нулей между группами единиц в предикате $A(x)$. В модели $l_i = L_i$. Для учета отличий амплитудных картин по энергетике принятого сигнала введен признак $L_3^{s_i}$, верхний индекс которого указывает на количество единиц в предикате $A(x)$. В модели $s_i = E_i$.

Алгоритм идентификации типов S_j для амплитудных картин описывается следующими уравнениями:

$$
\begin{aligned}
S_1 &= L_1^1 \wedge L_2^0 \wedge (L_3^1 \vee L_3^2);\\
S_2 &= L_1^2 \wedge (L_2^0 \vee L_2^1 \vee L_2^2 \vee L_2^3) \wedge (L_3^2 \vee L_3^3 \vee L_3^4);\\
S_3 &= L_1^2 \wedge (L_2^5 \vee L_2^6 \vee L_2^7 \vee L_2^8) \wedge L_3^3;\\
S_4 &= L_1^2 \wedge (L_2^4 \vee L_2^5 \vee L_2^6) \wedge (L_3^4 \vee L_3^5 \vee L_3^6)\\
&\dots\\
S_j &= (L_1^0 \vee L_1^1 \vee \dots \vee L_1^j) \wedge (L_2^0 \vee L_2^1 \vee \dots \vee L_2^{l_i}) \wedge (L_3^1 \vee L_3^2 \vee \dots \vee L_3^{s_i}).
\end{aligned}
\tag{8}
$$

В общем виде (8) можно представить как

$$
S_j = (\bigvee_{j_1}^{j} L_1^j) \wedge (\bigvee_{l_1}^{l_2} L_2^l) \wedge (\bigvee_{s_1}^{s_2} L_3^s). \tag{9}
$$

На основе полученных уравнений разработана функциональная схема определения типов флуктуаций пачки (рис. 3).

Таким образом, все операции по классификации и радиолокационному распознаванию воздушных объектов на основе предложенного алгоритма идентификации типов амплитудных флуктуаций пачки выполняются автоматически и в реальном масштабе времени. Следует также отметить, что в отличие от обычных статистик, порог формирования элементов q_i не является фиксированным, а адаптируется в каждой конкретной ситуации по уровню максимума амплитудного пика. Такая адаптация позволяет отображать информацию о форме и типе амплитудных флуктуаций независимо от энергетики пачки и, в конечном счете, стабилизирует вероятность ошибки при определении типа флуктуаций пачки.

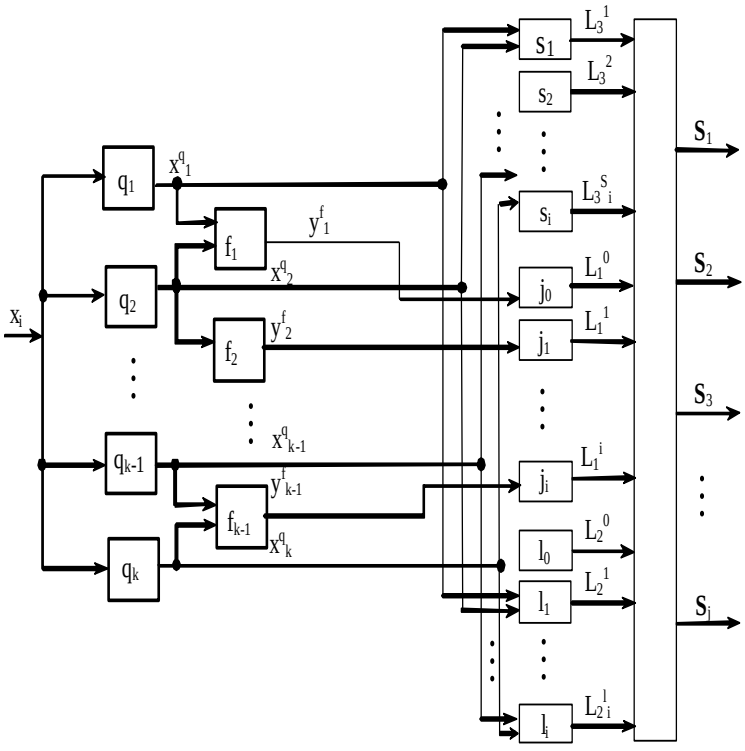


Рис. 3. Схема алгоритма определения типов флуктуаций пачки

Верификация и оценка эффективности разработанного метода [11, 12] проведены на основе реальных данных, полученных на обзорной РЛС сантиметрового диапазона (длительность импульса 1 мкс, частота зондирования 365 Гц, период обзора 10 с). На основе этих данных смоделированы типы характерных пачек радиолокационных сигналов. По результатам экспериментов все они были правильно идентифицированы.

Заключение

Разработан метод семантического анализа амплитудных флуктуаций радиолокационной пачки на основе предикатной модели процессных знаний формирования и анализа символьной модели совокупности импульсных сигналов от подвижных летательных аппаратов типа самолет, вертолет, БПЛА, и от атмосферных неоднородностей типа «ангел-эхо».

Модель имеет пачечную структуру. В результате семантического анализа амплитудных флуктуаций пачки во временной области можно получить классификационные отличительные признаки флуктуаций пачки от мешающих отражений и воздушных объектов. Исследованы семантические составляющие алгоритма принятия решений, которые подобны алгоритмам принятия решений человеком-оператором. Разработан алгоритм и программно реализован метод семантического анализа флуктуаций радиолокационной пачки для идентификации воздушных объектов в обзорных РЛС. Сигнальная информация описывается предикатной функцией на множестве амплитуд импульсов пачки, превысивших некоторое пороговое значение. Идентификация типов флуктуаций проводится путем решения разработанных уравнений предикатных операций. На основании полученных уравнений синтезирована функциональная схема автоматического определения типов флуктуаций. Верификация разработанного метода проведена на основе реальных данных, полученных на обзорной РЛС сантиметрового диапазона (длительность импульса 1 мкс, частота зондирования 365 Гц, период обзора 10 с). На основе этих данных смоделированы типы характерных пачек радиолокационных сигналов. По результатам экспериментов все они были правильно идентифицированы.

Список литературы

1. Li Jian Radar Signal Processing and Its Applications / Jian Li, R. Hummel, P. Stoica, E. G. Zelnio. Springer, 2013. 279 p.

2. Иванилов А.А. Реляционные алгебры и алгебры предикатов / А.А. Иванилов, Ю.П. Шабанов-Кушнаренко // Восточно–Европейский журнал передовых технологий. 2007. № 4/2. С. 43–48.

3. Russel S. Artificial intelligence. A modern approach Second Edition / S. Russel, P. Norvig. Williams, 2006. 1410 p.

4. Бондаренко М. Ф. Теория интеллекта : учебник / М. Ф. Бондаренко, Ю. П. Шабанов-Кушнаренко. Харьков : изд-во СМИТ, 2007. 576 с.

5. Горелик А. Л. Методы распознавания / А. Л. Горелик, В. А. Скрипкин. Москва : Высш. шк, 2004. 261 с.

6. Журавлев, Ю. И. Об алгебраическом подходе к решению задач распознавания или классификации // Проблемы кибернетики. 2005. Вып. 33. С. 5–68.

7. Жирнов В.В., Солонская С.В. Предикатная модель процессных знаний о наблюдаемых объектах в многоканальных интеллектуальных системах мониторинга // Радиотехника. 2019. Вып. 199. С. 67 – 74.

8. Solonskaya S.V., Zhirnov V.V. Intelligent analysis of radar data based on fuzzy transforms // Telecommunications and Radio Engineering (English translation of Elektrosvyaz and Radiotekhnika). 2018. 77 (15). P. 1321-1329.

9. Shubin Igor, Snisar Stanislav, Zhyrnov Volodymyr, Slavhorodskyi Vlad. Practical Application of Formal Representation of Information for Intelligent Radar Systems // 5th International Scientific-Practical Conference “Problems of Infocommunications. Science and Technology (PIC S&T)”, 2018, 9-12 October. P. 433-436.

10. Solonskaya S.V., Zhirnov V.V. Signal processing in the intelligence systems of detecting low-observable and low-doppler aerial targets // Telecommunications and Radio Engineering (English translation of Elektrosvyaz and Radio-tekhnika). 2018. Vol. 77, Issue 20. P. 1827-1835.

11. Igor Shubin, Svitlana Solonska, Stanislav Snisar, Volodymyr Zhyrnov, Vlad Slavhorodskyi, Victoria Skovorodnikova. Efficiency Evaluation for Radar Signal Processing on the Basis of Spectral-Semantic Model // 2020 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering, 2020 , 25 – 29 February. P. 171-174.

12. Solonska S., Zhyrnov V. Adaptive semantic analysis of radar data using fuzzy transform (Book Chapter). Springer, 2020, Lecture Notes on Data Engineering and Communications Technologies. Vol 48. P. 157-179.

Поступила в редколлегию 17.09.2020

Сведения об авторах:

Жирнов Владимир Витальевич – к.т.н., Харьковский национальный университет радиоэлектроники, в.н.с. НИЦ интегрированных радиоэлектронных систем и технологий, Украина; e-mail: nauka123@ukr.net

Солонская Светлана Владимировна – к.т.н., доцент кафедры естественных и гуманитарных наук, Харьковский национальный автомобильно-дорожный университет, Украина; e-mail: solonskaya@ukr.net, ORCID: https://orcid.org/0000-0002-8841-7825

РЕФЕРАТИ РЕФЕРАТЫ ABSTRACTS

МЕТОДИ ТА МЕХАНІЗМИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ
МЕТОДЫ И МЕХАНИЗМЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ
METHODS AND MECHANISMS OF CRYPTOGRAPHIC PROTECTION OF INFORMATION

УДК 004.056.5

Порівняльний аналіз одноразових підписів на базі геш-функцій / *В.В. Семенець, О.С. Марухненко, І.Д. Горбенко, Г.З. Халімов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 203. С. 5 – 18.

Підписи на основі геш-функцій є широким класом постквантових криптографічних алгоритмів, їх стійкість базується на складності задач пошуку колізій та прообразів для криптографічних геш-функцій. Основними перевагами цього класу є постквантовість, легка модифікація та добре досліджена математична база. До недоліків відносяться великі розміри підписів та обмежена кількість використань однієї пари ключів. До найбільш перспективних алгоритмів цього класу належать криптосистеми типу SPHINCS, які мають складну структуру, що включає, серед інших, одноразовий підпис Вінтерніца. В роботі проведено аналіз існуючих алгоритмів одноразового підпису, як широко відомих схем Лампорта та Вінтерніца з урахуванням модифікацій останнього, так і альтернативних методів. Проведено аналіз стійкості модифікованих алгоритмів, який показав, що їх стійкість базується на тій самій математичній базі, що і стійкість оригінальних алгоритмів. Вимога одноразового використання залишається критично важливою для безпеки кожного з досліджених алгоритмів. Порівняно розміри ключів та підписів та обчислювальну складність різних алгоритмів, що і складає їх основні відмінності. Модифіковані алгоритму не вносять принципово нових складових в криптосистеми але дозволяють досягти певної оптимізації, зміщуючи умови просторово-часового компромісу. Окремий інтерес представляє розширений підпис Лампорта, що має ту ж обчислювальну складність та розміри ключів, що і оригінальний алгоритм, і при цьому дозволяє вдвічі зменшити розмір підпису. В контексті криптосистеми SPHINCS підпис Вінтерніца залишається кращим варіантом, оскільки дозволяє повністю обчислювати публічний ключ безпосередньо з підпису.

Ключові слова: підписи на базі геш-функцій; одноразові підписи; підпис Лампорта; підпис Вінтерніца; постквантова криптографія.

Табл. 9. Бібліогр.: 13 назв.

УДК 004.056.5

Сравнительный анализ одноразовых подписей на основе хеш-функций / *В.В. Семенец, А.С. Марухненко, И.Д. Горбенко, Г.З. Халимов* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 203. С. 5 – 18.

Подписи на основе хеш-функций являются широким классом постквантовых криптографических алгоритмов, их стойкость базируется на сложности задач поиска коллизий и прообразов для криптографических хеш-функций. Основными преимуществами данного класса являются постквантовость, легкая модификация и хорошо исследованная математическая база. Недостатки – большие размеры подписей и ограниченное количество использований одной пары ключей. К наиболее перспективным алгоритмам этого класса относятся криптосистемы типа SPHINCS, которые имеют сложную структуру, включающую, среди прочих, одноразовую подпись Винтерница. В работе проведен анализ существующих алгоритмов одноразовой подписи, как широко известных схем Лампорта и Винтерница с учетом модификаций последнего, так и альтернативных методов. Проведен анализ стойкости модифицированных алгоритмов, который показал, что их безопасность базируется на той же математической базе, что и стойкость оригинальных алгоритмов. Требование одноразового использования остается критично важным для безопасности каждого из исследованных алгоритмов. Выполнено сравнение размеров ключей и подписей и вычислительной сложности различных алгоритмов, в чем и заключается их основные отличия. Модифицированные алгоритма не вносят принципиально новых составляющих в криптосистемы, но позволяют достичь определенной оптимизации, смещая условия пространственно-временного компромисса. Отдельный интерес представляет расширенная подпись Лампорта, имеющая ту же вычислительную сложность и размеры ключей, как и оригинальный алгоритм, и при этом позволяющая вдвое уменьшить размер подписи. В контексте криптосистемы SPHINCS подпись Винтерница остается лучшим вариантом, поскольку позволяет полностью вычислять публичный ключ непосредственно из подписи.

Ключевые слова: подписи на основе хеш-функций; одноразовые подписи; подпись Лампорта; подпись Винтерница; постквантовая криптография.

Табл. 9. Библиогр.: 13 назв.

UDC 004.056.5

Comparative analysis of one-time hash-based signatures / *V.V. Semenetz, O.S. Marukhnenko, I.D. Gorbenko, G.Z. Khalimov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №203. P. 5 – 18.

Hash-based signatures are a wide class of post-quantum cryptographic algorithms, their security is based on the complexity of collision and preimage search problems for cryptographic hash functions. The main advantages of this class are post-quantization, easy modification and a well-researched mathematical base. The disadvantages are large sizes of signatures and limited number of uses of one key pair. The most promising algorithms of this class include algorithms of the SPHINCS type, which have a complex structure, including, among others, a one-time Winternitz signature. The paper analyzes the existing one-time signature algorithms, both well-known Lamport and Winternitz schemes, taking into account modifications of the latter one, and alternative methods. An analysis of the security of modified algorithms has been shown, which showed that their security is based on the same mathematical basis as the security of the original algorithms. The one-time use requirement remains critical to the safety of each of the algorithms studied. The sizes of keys and signatures and computational complexity of various algorithms are compared, in what their basic differences consist. The modified algorithms do not add fundamentally new components in cryptosystems but they make it possible to achieve a certain optimization, shifting the conditions of space-time compromise. The extended Lamport signature is of a particular interest, having the same computational complexity and key sizes as the original algorithm, and at the same time allowing one to halve the signature size. In the context of the SPHINCS cryptosystem, the Winternitz signature remains the best option, since it allows the complete computation of the public key directly from the signature.

Key words: hash-based signatures; one-time signatures; Lamport signature; Winternitz signature; post-quantum cryptography.

9 tab. Ref: 13 items.

УДК 004.056.55

Аналіз та дослідження алгоритму цифрового підпису Picnic / *М.В. Єсіна, Б.С. Шахов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 203. С. 19 – 24.

Важливою особливістю постквантового періоду у криптографії є суттєва невизначеність щодо вихідних даних для криптоаналізу та протидії в частині можливостей квантових комп'ютерів, їх математичного та програмного забезпечень, а також застосування квантового криптоаналізу до існуючих криптоперетворень та криптопротоколів. В якості основних методів NIST США обрано математичні методи цифрового підпису (ЦП), що пройшли суттєвий аналіз та обґрунтування в процесі широких досліджень криптографами та математиками на найвищому рівні. Вони детально описані та пройшли дослідження на першому етапі міжнародного конкурсу NIST США. В процесі другого етапу прийнято ряд рішень стосовно об'єднання деяких кандидатів на постквантовий стандарт ЦП. Для подальших досліджень на 2-му етапі залишили 9 кандидатів: Crystals-Dilithium, Falcon, GeMSS, LUOV, MQDSS, Picnic, qTESLA, Rainbow та SPHINCS+. Три з них (Dilithium, Falcon, qTeSLA) засновані на стійкості алгебраїчних решіток (Lattice-based), чотири (GeMSS, LUOV, MQDSS, Rainbow) – на основі багатовимірних перетворень (MQ-перетворення), один (SPHINCS+) – на стійкості геш-функції, один (Picnic) – на стійкості геш-функції та блокових потокових шифрів. За результатами досліджень перспективних постквантових криптографічних алгоритмів типу цифровий підпис протягом 2-го раунду конкурсу NIST США було отримано наступні результати – були обрані алгоритми-фіналісти та альтернативні алгоритми. У якості алгоритмів-фіналістів були обрані такі алгоритми ЦП: Crystals-Dilithium, Falcon та Rainbow. У якості альтернативних алгоритмів – GeMSS, Picnic та SPHINCS+. У даній роботі розглядаються особливості побудови алгоритму цифрового підпису, який розглядається як кандидат на перспективний постквантовий стандарт конкурсу NIST PQC – Picnic, а також проводиться аналіз захищеності алгоритму від відомих атак. Приводяться дані з порівняння постквантових алгоритмів типу цифровий підпис. Наводиться опис алгоритму Picnic та його параметрів.

Ключові слова: аналіз відомих атак; блокові потокові шифри; відкритий ключ; геш-функції; ключові пари; постквантовий алгоритм Picnic; постквантова захищеність; стандарти шифрування; таємний ключ; цифровий підпис; LowMC.

Табл. 3. Бібліогр.: 7 назв.

УДК 004.056.55

Анализ и исследование алгоритма цифровой подписи Picnic / *М.В. Есина, Б.С. Шахов* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 203. С. 19 – 24.

Важной особенностью постквантового периода в криптографии является существенная неопределенность относительно исходных данных для криптоанализа и противодействия в части возможностей квантовых компьютеров, их математического и программного обеспечения, а также применение квантового криптоанализа к существующим криптопреобразованиям и криптопротоколам. В качестве основных методов NIST США избрал математические методы цифровой подписи (ЦП), прошедшие существенный анализ и обоснование в процессе широких исследований криптографами и математиками на высшем уровне. Они подробно описаны и прошли исследования на первом этапе международного конкурса NIST США. В процессе второго этапа принят ряд решений относительно объединения некоторых кандидатов на постквантовый стандарт ЦП. Для дальнейших исследований на 2-м этапе оставили 9 кандидатов: Crystals-Dilithium, Falcon, GeMSS, LUOV, MQDSS, Picnic, qTESLA, Rainbow и SPHINCS+. Три из них (Dilithium, Falcon, qTeSLA) основаны на стойкости алгебраических решеток (Lattice-based), четыре (GeMSS, LUOV, MQDSS, Rainbow) – на основе многомерных преобразований (MQ-преобразование), один (SPHINCS+) – на стойкости хеш-функции, один (Picnic) – на стойкости хеш-функции и блочных потоковых шифров. По результатам исследований перспективных постквантовых крипто-

графических алгоритмов типа цифровая подпись в течение 2-го раунда конкурса NIST США были получены следующие результаты – выбраны алгоритмы-финалисты и альтернативные алгоритмы. В качестве алгоритмов-финалистов выбраны алгоритмы ЦП: Crystals-Dilithium, Falcon и Rainbow. В качестве альтернативных алгоритмов – GeMSS, Picnic и SPHINCS+. В данной работе рассматриваются особенности построения алгоритма цифровой подписи, который рассматривается как кандидат на перспективный постквантовый стандарт конкурса NIST PQC – Picnic, а также проводится анализ защищенности алгоритма от известных атак. Приводятся данные из сравнения постквантовых алгоритмов типа цифровая подпись. Приводится описание алгоритма Picnic и его параметров.

Ключевые слова: анализ известных атак; блочные поточные шифры; открытый ключ; хеш-функции; ключевые пары; постквантовый алгоритм Picnic; постквантовая защищенность; стандарты шифрования; секретный ключ; цифровая подпись; LowMC.

Табл. 3. Библиогр.: 7 назв.

UDC 004.056.55

Analysis and research of digital signature algorithm Picnic / *M.V. Yesina, B.S. Shahov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №203. P. 19 – 24.

An important feature of the post-quantum period in cryptography is the significant uncertainty regarding the source data for cryptanalysis and counteraction in terms of the capabilities of quantum computers, their mathematical and software, as well as the application of quantum cryptanalysis to existing cryptotransformations and cryptoprotocols. Mathematical methods of digital signature (DS) have been chosen as the main methods of NIST USA, which have undergone significant analysis and substantiation in the process of extensive research by cryptographers and mathematicians at the highest level. They are described in detail and studied at the first stage of the US NIST International Competition. In the second round, a number of decisions were made to merge some candidates for the post-quantum DS standard. 9 candidates were left for further research at the 2nd round: Crystals-Dilithium, Falcon, GeMSS, LUOV, MQDSS, Picnic, qTESLA, Rainbow and SPHINCS+. Three of them (Dilithium, Falcon, qTeSLA) are based on the stability of algebraic lattices (Lattice-based), four (GeMSS, LUOV, MQDSS, Rainbow) are based on multivariate transformations (MQ-transformations), one (SPHINCS+) is based on the stability of hash-function, one (Picnic) is based on the stability of the hash-function and block stream ciphers. During the 2nd round of the US NIST Competition the following finalist algorithms and alternative algorithms were selected as digital signatures according to the results of research on promising post-quantum cryptographic algorithms. As finalists algorithms such DS algorithms as Crystals-Dilithium, Falcon and Rainbow. Alternative algorithms are GeMSS, Picnic and SPHINCS+ were selected. This paper studies the peculiarities of construction of the digital signature algorithm considered as a candidate for the promising post-quantum standard of the NIST PQC competition – Picnic, also it analyzes the protection of the algorithm from known attacks. Data from the comparison of post-quantum algorithms such as digital signature are given. The description of the Picnic algorithm and its parameters are given.

Key words: analysis of known attacks; block stream ciphers; public key; hash functions; key pairs; post-quantum algorithm Picnic; post-quantum security; encryption standards; secret key; digital signature; LowMC.

3 tab. Ref: 7 items.

УДК 004.056.5

Уточнення оцінок ймовірності успіху атаки подвійної витрати на блокчейн системи з урахуванням моделі незалежних гравців / *М.А. Полуяненко, Ю.І. Горбенко, В.Е. Сафоненко, О.О. Кузнецов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 203. С. 25 – 37.

Технологія блокчейн досліджується в багатьох інноваційних програмах, таких як: криптовалюта; розумні контракти; системи зв'язку; охорона здоров'я; Інтернет речі; фінансові системи; розробка програмного забезпечення; електронне голосування та багато інших. Використовуючи прозору і повністю розподілену однорангову архітектуру блокчейн, додатки виграють від моделі, в якій можливо тільки додавання даних, в якій «транзакції» приймаються в блокчейн реєстр і при правильному функціонуванні системи не можуть бути модифіковані або видалені. Прозорість блокчейн систем дозволяє зберігати загальнодоступні і незаперечні записи. Тимчасова блокчейн система забезпечує перевірене ведення реєстру без централізованого управління, що дозволяє вирішувати проблеми єдиної точки відмови і єдиної точки довіри. У статті розглядається питання безпеки застосування облікових систем, побудованих за децентралізованими принципами з використанням блокчейн технології. Особливу увагу приділяється проблемі можливості проведення подвійних витрат в таких облікових системах. Наводяться приклади реорганізації записів у блокчейн реєстрах, які були виконані за допомогою вдалого проведення атак 51 % на алгоритми консенсусу на основі Доказу виконаної роботи. Приводиться уточнення аналітичних виразів ймовірності проведення атак 51 %, отриманих в роботах С. Накамото та М. Розенфельда, коли використовували більш загальну модель – модель незалежних гравців, де ймовірність формування блоків зловмисниками та чесною мережею є незалежними подіями. Наводяться результати порівняння ймовірності успіху атаки подвійних витрат на блокчейн системи, розрахованих за різними моделями.

Ключові слова: атака подвійний витрати; технологія блокчейн; протоколи консенсусу; децентралізовані системи.

Іл. 3. Бібліогр.: 83 назв.

УДК 004.056.5

Уточнение оценок вероятности успеха атаки двойной траты на блокчейн системы на основе модели независимых игроков / *Н.А. Полуяненко, Ю.І. Горбенко, В.Э. Сафоненко, А.А. Кузнецов* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 203. С. 25 – 37.

Технология блокчейн исследуется во многих инновационных приложениях, таких как: криптовалюты; умные контракты; системы связи; здравоохранение; Интернет вещи; финансовые системы; разработка программного обеспечения; электронное голосование и многие другие. Используя прозрачную и полностью распределенную одноранговую архитектуру блокчейн, приложения выигрывают от модели, в которой возможно только добавление данных, в которой «транзакции» принимаются в блокчейн реестр и при правильном функционировании системы не могут быть модифицированы или удалены. Прозрачность блокчейн систем позволяет хранить общедоступные и неопровержимые записи. Одноранговая блокчейн система обеспечивает проверяемое ведение реестра без централизованного управления, что позволяет решать проблемы единой точки отказа и единой точки доверия. В статье рассматривается вопрос безопасности применения учетных систем, построенных децентрализованными принципами с использованием блокчейн технологии. Особое внимание уделяется проблеме проведения двойных расходов в таких учетных системах. Приводятся примеры реорганизации записей в блокчейн реестрах, которые были выполнены с помощью удачного проведения атак 51 % на алгоритмы консенсуса на основе Доказательства выполненной работы. Приводится уточнение аналитических выражений вероятности проведения атак 51 %, полученных в работах С. Накамото и М. Розенфельда, когда использовали более общую модель – модель независимых игроков, где вероятность формирования блоков злоумышленниками и честной сетью являются независимыми событиями. Приводятся результаты сравнения вероятности успеха атаки двойных расходов на блокчейн системы, рассчитанных по разным моделям.

Ключевые слова: атака двойной траты; технология блокчейн; протоколы консенсуса; децентрализованные системы.

Ил. 3. Библиогр.: 83 назв.

UDC 004.056.5

Refinement of estimates of the success probability of a double-spend attack on the Blockchain System, Based on the Independent Players Model / *N.A. Poluyanenko, Yu.I. Gorbenko, V.E. Safonenko, A.A. Kuznetsov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. № 203. P. 25 – 37.

Blockchain technology is being studied in many innovative applications, such as: cryptocurrencies, smart contracts, communication systems, healthcare, Internet of Things, financial systems, software development, electronic voting and many others. Using a transparent and fully distributed peer-to-peer blockchain architecture, applications benefit from a data-only model, in which “transactions” are accepted into the blockchain ledger and, if the system is functioning properly, cannot be modified or deleted. The transparency of blockchain systems makes it possible to store publicly available and irrefutable records. A peer-to-peer blockchain system provides verifiable ledger maintenance without centralized management, which solves the problems of a single point of failure and a single point of trust. The article deals with the issue of the security of application of accounting systems built on decentralized principles using blockchain technology. Particular attention is paid to the problem of the possibility of double spending in such accounting systems. The article exemplifies the reorganization of records in blockchain ledgers, performed by successfully carrying out a 51% attack on consensus algorithms based on proof of work. Given refinement of analytical expressions of 51% attack probability obtained in the works of S. Nakamoto and M. Rosenfeld using a more general model, namely, the model of independent players, where the probability of block formation by attackers and an honest network are independent events. The results of comparing of the success probability of a double-spending attack on the blockchain systems calculated according to different models are presented.

Key words: double spend attack; blockchain technology; consensus protocols; decentralized systems.

3 fig. Ref: 83 items.

УДК 004.056.5

Приховування даних на основі адресації шумоподібних сигналів / *О.О. Кузнецов, О.А. Смирнов, А.С. Киян, Т.Ю. Кузнецова* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 203. С. 38 – 49.

Для передачі секретних повідомлень використовуються різні обчислювальні методи. Наприклад, криптографічні методи приховують смисловий зміст повідомлень, що передаються, представляючи їх у вигляді шумоподібних безглуздих даних. Стеганографічні методи приховують факт існування інформаційних повідомлень. Для цього повідомлення приховуються всередині контейнерів (cover files) – надлишкових даних, які передаються відкритим способом і не викликають ні в кого підозр. Сторонній спостерігач може перехоплювати cover files, аналізувати і досліджувати їх, проте детектувати приховані дані і тим більше їх відновлювати для нього дуже складно або взагалі неможливо. У статті обговорюються методи приховування даних у контейнерах-переносчиках з використанням технологій прямого розширення спектра. Представляється новий метод, який полягає у прямій адресації псевдовипадкових послідовностей. З одного боку це значно зменшує викривлення контейнерів-переносчиків. З іншого боку – інтенсивність помилок у відновлених повідомленнях не збільшується. Результати експериментальних досліджень показують, що за порівнянням з іншими відомими методами дійсно вдається зменшити викривлення контейнерів-переносників (в експериментах використовувались контейнери-зображення). У статті приводяться наочні приклади, а також показані переваги запропонованого методу.

Приводяться результати експериментальних досліджень за оцінкою якості зображень. Ці результати підтверджують адекватність та достовірність теоретичних оцінок.

Ключові слова: стеганографія з розширеним спектром; приховування даних; контейнери-зображення; пряме розширення спектру; псевдовипадкова послідовність.

Іл. 8. Бібліогр.: 37 назв.

УДК 004.056.5

Сокрытие данных на основе адресации шумоподобных сигналов / *А.А. Кузнецов, А.А. Смирнов, А.С. Киян, Т.Ю. Кузнецова* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 203. С. 38 – 49.

Для передачи секретных сообщений используются различные вычислительные методы. Например, криптографические методы скрывают смысловое содержание передаваемых сообщений, представляя их в виде шумоподобных бессмысленных данных. Стеганографические методы скрывают факт существования информационных сообщений. Для этого сообщения скрываются внутри контейнеров (cover files) – избыточных данных, которые передаются открытым способом и не вызывают ни у кого подозрений. Сторонний наблюдатель может перехватывать cover files, анализировать и исследовать их, однако детектировать сокрытые данные и тем более их восстанавливать для него очень сложно или вообще невозможно. В статье обсуждаются методы сокрытия данных в контейнерах-переносчиках с использованием технологии прямого расширения спектра. Предлагается новый метод, который заключается в прямой адресации псевдослучайных последовательностей. С одной стороны, это значительно уменьшает искажение контейнеры-переносчики. С другой стороны, интенсивность ошибок в восстановленных сообщениях не увеличивается. Результаты экспериментальных исследований показывают, что по сравнению с другими известными методами действительно удается уменьшить искажения контейнеров-переносчиков (в экспериментах использовались контейнеры-изображения). В статье приводятся наглядные примеры, а также показаны преимущества предложенного метода. Приводятся результаты экспериментальных исследований по оценке качества изображений, подтверждающие адекватность и достоверность теоретических результатов.

Ключевые слова: стеганография с расширенным спектром; сокрытие данных; контейнеры-изображения; прямое расширение спектра; псевдослучайная последовательность.

Ил. 8. Библиогр.: 37 назв.

UDC 004.056.5

Data hiding based on noise-like signal addressing / *A.A. Kuznetsov, O.A. Smirnov, A.S. Kiian, T.Y. Kuznetsova* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №203. P. 38 – 49.

There are various computing techniques (methods) to transmit secret messages. For example, cryptographic techniques hide the semantic content of transmitted messages, presenting them in the form of noise-like minor data. Steganographic techniques hide the existence of information messages itself. In this case, messages are hidden inside cover files, i.e., redundant data that are transmitted in an open way and do not cause suspicion in anyone. An outside observer can intercept cover files, analyze and examine them. However, it is very difficult or even impossible to detect and recover hidden data. This article discusses the techniques for hiding data in cover images using direct spread spectrum. We propose a new technique that consists in direct addressing of pseudo-random sequences. On the one hand, it significantly reduces cover file distortion. On the other hand, the error rate in recovered messages does not increase. Our experiments have shown, that Spread Spectrum Steganography technique indeed reduce the distortion in cover images compared to other techniques. We give some illustrative examples and show the advantages of the proposed method. Even with a significant increase in encoding density, the quality of cover images does not degrade. We also conduct experiments and evaluate image quality based on Mean Squared Error (MSE) and Peak Signal-to-Noise Ratio (PSNR). The obtained results of experimental studies confirm the adequacy and reliability of the research results. The main disadvantage of the proposed data hiding technique is a high computational complexity. To recover messages, it is necessary to calculate sequentially the correlation coefficients with a large number of pseudo-random sequences.

Key words: Spread Spectrum Steganographic; Data Hiding; cover images; direct spread spectrum; pseudo-random sequence

8 fig. Ref: 37 items.

УДК 621.391.15:519.7

Оцінка ефективності диференціального додавання точок кривих в узагальненій формі Едвардса / *А.В. Бессалов, Л.В. Ковальчук, Н.В. Кучинська* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 203. С. 50 – 59.

Дано огляд основних властивостей трьох класів кривих в узагальненій формі Едвардса: повних, квадратичних і скручених кривих Едвардса. Проведено аналіз алгоритму Монтгомері диференціального додавання точок для кривої в формі Монтгомері. Наведено оцінку рекордно малої вартості обчислення скалярного добутку kP точки P, яка дорівнює $5M+4S+1U$ на одному кроці ітеративного циклу (M – вартість операції обчислення добутку в скінченному полі, S – вартість піднесення до квадрату, U – вартість множення на відому константу). Дано ретельний вивід формул додавання-віднімання і подвоєння точок для кривої в узагальненій формі Едвардса в проективних координатах Фарашахи – Хоссейни. Перехід від тривимірних проективних координат

$(X:Y:Z)$ до двовимірних координат $(W:Z)$ дозволяє для кривих Едвардса досягти тієї ж самої мінімальної вартості обчислень $5M+4S+1U$, що і для кривої в формі Монтгомері. Обговорюються аспекти вибору придатної для криптографії кривої в формі Едвардса і оптимізації її параметрів в задачі диференціального додавання точок. Рекомендуються скручені криві Едвардса порядку $N_E = 4n$ (n - просте) при $p \equiv 5 \bmod 8$, для яких мінімізація параметрів a та d дозволяє досягнути мінімальної оцінки вартості $5M+4S$ для одного кроку обчислення скалярного добутку точки. Показано, що перехід від кривих в формі Вейерштраса, які використовуються в сучасних криптографічних стандартах, до кривих в формі Едвардса, дозволяє отримати потенціальний виграш в швидкості обчислення скалярного добутку точки в 3,09 рази.

Ключові слова: крива в узагальненій формі Едвардса; повна крива Едвардса; скручена крива Едвардса; квадратична крива Едвардса; порядок кривої; порядок точки; ізоморфізм; диференціальне додавання; вартість обчислень; квадратичний лишок; квадратичний нелишок.

Бібліогр.: 10 назв.

УДК 621.391.15:519.7

Оценка эффективности дифференциального сложения точек кривых в обобщенной форме Эдвардса / *А.В. Бессалов, Л.В. Ковальчук, Н.В. Кучинская* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 203. С. 50 – 59.

Дан обзор основных свойств трех классов кривых в обобщенной форме Эдвардса: полных, квадратичных и скрученных кривых Эдвардса. Проведен анализ алгоритма Монтгомери дифференциального сложения точек для кривой в форме Монтгомери. Приведена оценка рекордно малой стоимости вычисления скалярного произведения kP точки P, равная $5M+4S+1U$ на одном шаге итеративного цикла (M – стоимость вычисления умножения в конечном поле, S - стоимость возведения в квадрат, U – стоимость умножения на известную константу). Приведен подробный вывод формул сложения-вычитания и удвоения точек для кривой в обобщенной форме Эдвардса в проективных координатах Фарашахи – Хоссейни. Переход от трехмерных проективных координат $(X:Y:Z)$ к двухмерным координатам $(W:Z)$ позволяет для кривых Эдвардса достичь той же минимальной стоимости вычислений $5M+4S+1U$, что и для кривой в форме Монтгомери. Обсуждаются аспекты выбора приемлемой для криптографии кривой в форме Эдвардса и оптимизации ее параметров в задаче дифференциального сложения точек. Рекомендуются скрученные кривые Эдвардса с порядком $N_E = 4n$ (n - простое) при $p \equiv 5 \bmod 8$, минимизация параметров a и d которых позволяет достичь минимальной оценки стоимости $5M+4S$ одного шага вычисления скалярного произведения точки. Показано, что переход от используемых в современных стандартах кривых в форме Вейерштрасса к кривым в форме Эдвардса позволяет получить потенциальный выигрыш в скорости вычисления скалярного произведения точки в 3,09 раза.

Ключевые слова: кривая в обобщенной форме Эдвардса; полная кривая Эдвардса; скрученная кривая Эдвардса; квадратичная кривая Эдвардса; порядок кривой; порядок точки; изоморфизм; дифференциальное сложение; стоимость вычислений; квадратичный вычет; квадратичный невычет.

Библиогр.: 10 назв.

UDC 621.391.15:519.7

Evaluation of the efficiency of differential addition of points of curves in the generalized Edwards form / *A.V. Bessalov, L.V. Kovalchuk, N.V. Kuchynska* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №203. P. 50 – 59.

A survey of the main properties of three classes of curves in the generalized Edwards form is given: complete, quadratic and twisted Edwards curves. The analysis of the Montgomery algorithm for differential addition of points for the Montgomery curve is carried out. An estimation of the record low cost of computing the scalar product kP of a point P is given, which is equal to $5M+4S+1U$ on one step of the iterative cycle (M is the cost of finite field multiplication, S is the cost of squaring, U is the cost of field multiplication by a known constant). A detailed derivation of the formulas for addition-subtraction and doubling point s for the curve in the generalized Edwards form in projective coordinates of Farashahi-Hosseini is carried out. Moving from three-dimensional projective coordinates *(X: Y: Z)* to two-dimensional coordinates *(W: Z)* allows achieving the same minimum computational cost for the Edwards curves as for the Montgomery curve. Aspects of the choice of an Edwards-form curve acceptable for cryptography and its parameters optimization in the problem of differential addition of points are discussed. Twisted Edwards curves with the order of $N_E = 4n$ (n is prime) are recommended, minimizing the parameters a and d allows achieving the minimum cost estimation $5M+4S$ for one step of computing the point product. It is shown that the transition from the Weierstrass curves (the form used in modern cryptographic standards) to the Edwards curves makes it possible to obtain a potential gain in the speed of computing the scalar product of the point by a factor of 3.09.

Key words: Edwards curve in generalized form; complete Edwards curve; twisted Edwards curve; quadratic Edwards curve; curves order; points order; isomorphism; differential addition; computing cost; square; non square.

Ref: 10 items.

УДК 004.056.55

Постквантовий алгоритм інкапсуляції ключів Classic McEliece / *М.С. Луценко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 203. С. 60 – 81.

Проводиться комплексний аналіз кандидата-фіналіста міжнародного конкурсу постквантової криптографії NIST PQC, а саме – алгоритму інкапсуляції ключів на основі кодових криптосистем Classic McEliece. Метою роботи є первинне дослідження базових характеристик алгоритму Classic McEliece, таких як математична модель, очікувана криптографічна стійкість і кількісна оцінка витрачених ресурсів.

Проводиться аналіз математичної моделі алгоритму Classic McEliece, наводиться опис основних функцій і перетворень, порівняння первинної моделі алгоритму, запропонованого Робертом Мак-Елісом в 1978 р., і алгоритму, що розглядається, аналіз внесених авторами Classic McEliece модифікацій. Також наводяться рекомендації щодо подальших напрямків досліджень і доробок алгоритму.

В якості первинної оцінки криптографічної стійкості проведений аналіз відповідності сучасним вимогам до постквантових криптосистем, а саме – властивості нерозрізненості для атак на основі підібраного відкритого тексту, нерозрізненості для неадаптивних і адаптивних атак на основі підібраного шифротесту.

Проводиться аналіз витрат пам'яті на зберігання системних параметрів, оцінка впливу їх розміру на швидкодію системи. Також проводиться порівняння характеристик алгоритму Classic McEliece з подібними алгоритмами на основі алгебраїчних кодів, які були представлені в якості альтернативних варіантів на конкурсі NIST PQC, а саме алгоритмами BIKE і HQC. Оцінка швидкодії проводиться для трьох базових функцій алгоритму: генерації ключів, інкапсуляції і деінкапсуляції.

Ключові слова: криптосистеми з відкритим ключем; криптосистеми на основі алгебраїчних кодів; пост квантова криптографія; інкапсуляція ключів; швидкодія.

Табл. 4. Іл. 9. Бібліогр.: 15 назв.

УДК 004.056.55

Постквантовый алгоритм инкапсуляции ключей Classic McEliece / *М.С. Луценко* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 203. С. 60 – 81.

Проводится комплексный анализ кандидата-финалиста международного конкурса постквантовой криптографии NIST PQC, а именно – алгоритма инкапсуляции ключей на основе кодовых криптосистем Classic McEliece. Целью работы – первичное исследование базовых характеристик алгоритма Classic McEliece, таких как математическая модель, ожидаемая криптографическая стойкость и количественная оценка затрачиваемых ресурсов.

Проводится анализ математической модели алгоритма Classic McEliece, приводится описание основных функций и преобразований, сравнение первичной модели алгоритма, предложенного Робертом Мак-Элисом в 1978 г., и рассматриваемого алгоритма, анализ внесенных авторами Classic McEliece модификаций. Также приводятся рекомендации по дальнейшим направлениям исследований и доработок алгоритма.

В качестве первичной оценки криптографической стойкости проведен анализ соответствия современным требования к постквантовым криптосистемам, а именно – обеспечение свойства неразличимости для атак на основе подобранного открытого текста, неразличимость для неадаптивных и адаптивных атак на основе подобранного шифротекста.

В работе проводится анализ затрат памяти на хранение системных параметров, оценка влияния их размера на быстродействие системы. Также проводится сравнение характеристик алгоритма Classic McEliece с подобными алгоритмами на основе алгебраических кодов, которые были представлены в качестве альтернативных вариантов на конкурсе NIST PQC, а именно – алгоритмами BIKE и HQC. Оценка быстродействия проводится для трех базовых функций алгоритма: генерации ключей, инкапсуляции и деинкапсуляции.

Ключевые слова: криптосистемы с открытым ключом; криптосистемы на основе алгебраических кодов; пост квантовая криптография; инкапсуляция ключей; быстродействие.

Табл. 4. Ил. 9. Библиогр.: 15 назв.

UDC 004.056.55

Post-quantum algorithm of Classic McEliece key encapsulation / *M.S. Lutsenko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №203. P. 60 – 81.

A comprehensive analysis of a candidate-finalist of the International Post-quantum Cryptography Competition NIST PQC, namely, the Classic McEliece algorithm, the key encapsulation algorithm based on code cryptosystems, is carried out. The aim of this work is a primary study of the basic characteristics of the Classic McEliece algorithm, such as the mathematical model, the expected cryptographic strength and quantitative assessment of the resources.

The paper gives the analysis of the mathematical model of the Classic McEliece algorithm, description of the main functions and transformations, comparison of the primary model of the algorithm proposed by Robert McEliece in 1978 with the considered algorithm, analysis of the modifications made by the authors of Classic McEliece. It also provides recommendations for further areas of research and refinement of the algorithm. As a primary assessment of cryptographic security, an analysis of compliance with modern requirements for post-quantum cryptosystems is carried out, namely, ensuring the property of indistinguishability for attacks based on selected plaintext, indistinguishability for non-adaptive and adaptive attacks based on selected cipher text.

The paper analyzes the memory costs for storing system parameters, evaluating the impact of their size on the system performance. The characteristics of the Classic McEliece algorithm are compared with similar algorithms based on

the algebraic codes presented as alternatives at the NIST PQC Competition, namely, the BIKE and HQC algorithms. The performance evaluation is carried out for three basic functions of the algorithm: keys generation, encapsulation and de-encapsulation.

Key words: public key cryptosystems; cryptosystems based on algebraic codes; post-quantum cryptography; key encapsulation; performance.

4 tab. 9 fig. Ref: 15 items.

УДК 003.026:004.056

Проект стандарту електронного підпису Rainbow та його основні властивості і можливості щодо застосування / *Д.В. Гармаш, Г.А. Малєєва, С.О. Кандій* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 203. С. 82 – 90.

За результатами другого етапу міжнародного конкурсу щодо проведення досліджень та розробки стандартів асиметричних криптографічних перетворень постквантового періоду позитивну оцінку та визнання фіналістом отримав механізм електронного підпису (ЕП) Rainbow. Його важливими перевагами, у порівнянні з іншими постквантовими ЕП є менша складність прямого та зворотного перетворень – вироблення та перевірки підпису, а також суттєво зменшена довжина підпису. Разом з тим довжина відкритого ключа у нього достатньо велика. Тому є думка, що Rainbow не підходить як алгоритм ЕП загального призначення для заміни алгоритмів, які наразі визначені у FIPS 186-4. Зокрема, великі відкриті ключі роблять ланцюги сертифікатів надзвичайно великими. Однак є додатки, яким не потрібно надто часто надсилати ключі, тому цей недолік у цих випадках може бути несуттєвим. За цих умов механізм ЕП Rainbow може знайти застосування, в тому числі збільшуючи різноманітність постквантових ЕП. Також, суттєво проблемним є обмеження рівнів безпеки ЕП Rainbow 256 біт проти класичного та 128 біт проти квантового криптоаналізу.

Предметом статті є аналіз та узагальнення конструкцій механізму Oil-Vinegar систем автентифікації з відкритим ключем на основі застосування ЕП Rainbow. Це важливий напрямок щодо створення безпечних та ефективних систем автентифікації для практичних застосувань з використанням відкритих ключів, наприклад недорогих смарт-карт, коли потрібна швидкодія при виробленні та перевірці ЕП. Особливістю такого механізму автентифікації є реалізація ідеї багаторівневої системи Oil-Vinegar. Вважається, що система автентифікації на основі ЕП повинна бути більш безпечною у змісті криптографічної стійкості та більш ефективною у змісті широкого застосування у малопотужних тощо додатках. Важливість вирішення цієї проблемної задачі полягає у потенційному застосуванні механізму Rainbow, як надійно безпечної та дуже ефективної системи автентифікації з відкритим ключем на основі ЕП.

Ключові слова: класичний та квантовий криптоаналіз; модель загроз при застосуванні ЕП; перелік загроз ЕП; постквантовий період.

Табл. 1. Бібліогр.: 8 назв.

УДК 003.026:004.056

Проект стандарта электронной подписи Rainbow и его основные свойства и возможности применения / *Д.В. Гармаш, Г.А. Малеева, С.О. Кандий* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 203. С. 82 – 90.

По результатам второго этапа международного конкурса по проведению исследований и разработки стандартов асимметричных криптографических преобразований постквантового периода положительную оценку и признание финалистом получил механизм электронной подписи (ЭП) Rainbow. Его важными преимуществами по сравнению с другими постквантовыми ЭП, это меньше сложность прямого и обратного преобразований – выработка и проверки подписи, а также существенно уменьшена длина подписи. Вместе с тем длина открытого ключа у него достаточно велика. Поэтому есть мнение, что Rainbow не подходит как алгоритм ЭП общего назначения для замены алгоритмов, которые сейчас определены в FIPS 186-4. В частности, большие открытые ключи делают цепи сертификатов чрезвычайно большими. Однако есть приложения, которым не нужно слишком часто посылать ключи, поэтому этот недостаток в этих случаях может быть несущественным. В этих условиях механизм ЭП Rainbow может найти применение, в том числе увеличивая разнообразие постквантовых ЭП. Также, существенно проблемным является ограничение уровней безопасности ЭП Rainbow 256 бит против классического и 128 бит против квантового криптоанализа.

Предметом статьи является анализ и обобщение конструкций механизма Oil-Vinegar систем аутентификации с открытым ключом на основе применения ЭП Rainbow. Это важное направление по созданию безопасных и эффективных систем аутентификации для практических приложений с использованием открытых ключей, например недорогих смарт-карт, когда требуется быстродействие при выработке и проверке ЭП. Особенностью такого механизма аутентификации является реализация идеи многоуровневой системы Oil-Vinegar. Считается, что система аутентификации на основе ЭП должна быть более безопасной в смысле криптографической стойкости и более эффективной в смысле широкого применения в маломощных т.д. приложениях. Важность решения этой проблемной задачи заключается в потенциальном применении механизма Rainbow, как надежно безопасной и очень эффективной системы аутентификации с открытым ключом на основе ЭП.

Ключевые слова: классический и квантовый криптоанализ; модель угроз при применении ЭП; перечень угроз ЭП; постквантовый период.

Табл. 1. Библиогр.: 8 назв.

UDC 003.026:004.056

Draft of Rainbow electronic signature standard and its main properties and application possibilities / *D.V. Garmash, G.A. Maleeva, S.O. Kandiy* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №203. P. 82 – 90.

According to the results of the second stage of the international competition for research and development of standards for asymmetric cryptographic transformations of the post-quantum period, the Rainbow electronic signature (ES) mechanism received a positive assessment and recognition as a finalist. Its important advantages over other post-quantum ESs consist in less complexity of direct and inverse transformations, i.e., signature generation and verification, as well as significantly reduced signature length. At the same time, the length of its public key is quite large. Therefore, it is thought that Rainbow is not suitable as a general-purpose ES algorithm to replace the algorithms currently defined in FIPS 186-4. In particular, large public keys make certificate chains extremely large. However, there are applications that do not need to send keys too often, so this disadvantage in these cases may be insignificant. Under these conditions, the Rainbow ES mechanism can find application, including that one increasing the diversity of postquantum ESs. Also, it is significantly problematic to limit the security levels of Rainbow ES 256 bits against classical and 128 bits against quantum cryptanalysis.

The subject of this article is the analysis and generalization of designs of the Oil-Vinegar public key authentication systems mechanism based on the Rainbow ES use. This is an important direction in creating secure and efficient authentication systems for practical applications using public keys, such as inexpensive smart cards, when speed is required in the production and verification of ES. A feature of such authentication mechanism is the implementation of the idea of a multilevel Oil-Vinegar system. It is believed that the ES-based authentication system should be more secure in terms of cryptographic stability and more efficient in terms of widespread use in low-power, etc. applications. The importance of solving this problem lies in the potential use of the Rainbow mechanism as a secure and highly efficient public-key authentication system based on ES.

Key words: classical and quantum cryptanalysis; threat model when using ES; list of ES threats; postquantum period.

1 tab. Ref: 8 items.

МЕТОДИ ТА МЕХАНІЗМИ ЗАХИСТУ ІНФОРМАЦІЇ
МЕТОДЫ И МЕХАНИЗМЫ ЗАЩИТЫ ИНФОРМАЦИИ
INFORMATION PROTECTION METHODS AND MECHANISMS

УДК 004.056.52

Метод і методика формального проектування комплексної системи захисту інформації в інформаційно-телекомунікаційних системах / *Р.Ю. Гвоздьов, Р.В. Олійников* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 203. С. 91 – 96.

Метою статті є розробка методики формального проектування комплексної системи захисту інформації в інформаційно-телекомунікаційних системах. На даний момент не існує методик для формального проектування комплексної системи захисту інформації в інформаційно-телекомунікаційних системах, тому розробка такої методики є актуальною задачею. В статті розглядаються методи формалізованого моделювання політики безпеки інформації та методи формалізованого опису інформаційно-телекомунікаційної системи та процесів обробки інформації. Обґрунтовується необхідність формального проектування комплексної системи захисту інформації та описуються вимоги при розробці формальних описів комплексної системи захисту інформації згідно з нормативними документами в сфері технічного захисту інформації. Наводиться порівняльна характеристика методів формалізованого моделювання політики безпеки інформації та методів формалізованого опису інформаційно-телекомунікаційної системи та процесів обробки інформації. В результаті порівняння пропонується використовувати метод UML для формального опису інформаційно-телекомунікаційної системи, а метод UMLsec – для моделювання політики безпеки. Пропонується алгоритм формування комплексу засобів захисту в інформаційно-телекомунікаційній системі з формальної моделі політики безпеки та з формалізованого опису інформаційно-телекомунікаційної системи та процесів обробки інформації.

Ключові слова: комплексна система захисту інформації; інформаційно-телекомунікаційна система; формальне проектування; Ponder; UML; UMLsec.

Табл. 3. Бібліогр.: 3 назв.

УДК 004.056.52

Метод и методика формального проектирования комплексной системы защиты информации в информационно-телекоммуникационных системах / *Р.Ю. Гвоздев, Р.В. Олейников* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 203. С. 91 – 96.

Целью статьи является разработка методики формального проектирования комплексной системы защиты информации в информационно-телекоммуникационных системах. На данный момент не существует методик для формального проектирования комплексной системы защиты информации в информационно-телекоммуникационных системах, поэтому разработка такой методики является актуальной задачей. В статье рассматриваются методы формализованного моделирования политики безопасности информации и методы

формализованного описания информационно-телекоммуникационной системы и процессов обработки информации. Обосновывается необходимость формального проектирования комплексной системы защиты информации и описываются требования при разработке формальных описаний комплексной системы защиты информации в соответствии с нормативными документами в сфере технической защиты информации. Приводится сравнительная характеристика методов формализованного моделирования политики безопасности информации и методов формализованного описания информационно-телекоммуникационной системы и процессов обработки информации. В результате сравнения предлагается использовать метод UML для формального описания информационно-телекоммуникационной системы, а метод UMLsec – для моделирования политики безопасности. Предлагается алгоритм формирования комплекса средств защиты в информационно-телекоммуникационной системе с формальной модели политики безопасности и с формализованного описания информационно-телекоммуникационной системы и процессов обработки информации.

Ключевые слова: комплексная система защиты информации; информационно-телекоммуникационная система; Ponder; UML; UMLsec.

Табл. 3. Библиогр.: 3 назв.

UDC 004.056.52

Method and technique of formal design of complex information security system in information and telecommunication systems / *R.Y. Gvozdov, R.V. Oliynykov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №203. P. 91 – 96.

The aim of the article is to develop a methodology for the formal design of the complex information security system in information and telecommunication systems. At the moment, there are no methods for the formal design of complex information security system in information and telecommunication systems, so the development of such a methodology is an urgent task. The article discusses the methods of formalized modeling of information security policy and methods of formalized description of the information and telecommunications system and information processing processes. The necessity of formal design of complex information security system is substantiated and the requirements for the development of formal descriptions of an integrated information security system in accordance with regulatory documents in the field of technical protection of information are described. The comparative characteristics of the methods of formalized modeling of information security policy and methods of formalized description of the information and telecommunication system and information processing processes are given. As a result of the comparison, it is proposed to use the UML method for the formal description of the information-telecommunication system, and the UMLsec method for the security policy modeling. An algorithm for the formation of a complex of protection facilities in an information and telecommunications system is proposed from a formal model of security policy and from a formalized description of an information and telecommunications system and information processing processes.

Key words: complex information security system; information and telecommunication system, Ponder; UML; UMLsec.

3 tab. Ref: 3 items.

УДК 681.3.06:519.248.681

Використання BLOCKCHAIN в автомобільній безпеці / *І.Д. Горбенко, Д.О. Фесенко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 203. С. 97 – 108.

Проведено аналіз проблематики використання систем автентифікації для автомобільних систем. Показано, що сучасними системами захисту автомобілів все більше цікавляться зловмисники. Автомобілі стають більш технологічними, це в свою чергу відкриває нові можливості компрометації роботи вузлів та систем автомобіля, тому до систем безпеки пред'являються все більш жорсткі вимоги щодо забезпечення ефективності та безпечності їх функціонування. Розглянуті сучасні системи захисту від незаконного заволодіння автотранспортом, більш відомі всім як «сигналізація», намагаються стримувати атаки зловмисників, але в свою чергу можуть привносити додаткові бекдори для зловмисників зовсім ненавмисно, наприклад додаючи цікаву функцію в систему автомобіля, а згодом ця функція може мати двояке значення через проблеми з системою автентифікації. Тож, виходячи з цього, системи безпеки автомобіля повинні мати найвищий рівень безпеки автентифікації, для реалізації якого пропонується використання децентралізованої мережі блокчейн з вузлами для кожного автомобіля, що автентифікують користувача групово, це дозволить відійти від стандартної клієнт-серверної архітектури, що є недостатньо захищеною. Основними шляхами вирішення зазначеної проблеми є побудування комплексної системи безпеки, що в свою чергу включає покращений та надійний захід автентифікації на основі децентралізованої мережі блокчейн та двох комплексних схем оновлення системи передачі критичних даних автомобіля – мережі CAN. Використання даних систем дозволить поліпшити показники захищеності системи автентифікації та інформації, що курсує між блоками критичної важливості, що покращить безпечність автомобіля як від угонів, так і від можливостей створення зловмисниками аварійних ситуацій дистанційно.

Ключові слова: blockchain; атака; вразливість; децентралізація; підміна; automotive security.

Іл. 3. Бібліогр.: 4 назв.

УДК 681.3.06:519.248.681

Использование BLOCKCHAIN в автомобильной безопасности / *И.Д. Горбенко, Д.А. Фесенко* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 203. С. 97 – 108.

Проведен анализ проблематики использования систем аутентификации для автомобильных систем. Показано, что злоумышленники все больше интересуются современными системами защиты автомобилей. Автомобили становятся более технологичными, это в свою очередь открывает новые возможности компрометации работы узлов и систем автомобиля, поэтому к системам безопасности предъявляются все более жесткие требования по обеспечению эффективности и безопасности их функционирования. Рассмотрены современные системы защиты от незаконного завладения автотранспортом, более известные всем как «сигнализация» пытаются сдерживать атаки злоумышленников, но в свою очередь могут привносить дополнительные бэкдоры для злоумышленников совершенно непреднамеренно, например, добавляя интересную функцию в систему автомобиля, а затем эта функция может иметь двоякое значение из-за проблем с системой аутентификации. Поэтому, исходя из этого, системы безопасности автомобиля должны иметь высокий уровень безопасности аутентификации, для реализации которого предлагается использовать децентрализованную сеть блокчейн с узлами для каждого автомобиля. Это позволит отойти от стандартной клиент-серверной архитектуры, которая является недостаточно защищенной. Использование данных систем позволит улучшить показатели защищенности системы аутентификации и информации, курсирующий между блоками критической важности, улучшит безопасность автомобиля как от угонов, так и от возможностей создания злоумышленниками аварийных ситуаций дистанционно.

Ключевые слова: blockchain; атака; уязвимость; децентрализация; подмена; automotive security.

Ил. 3. Библиогр.: 4 назв.

UDC 681.3.06:519.248.681

Using BLOCKCHAIN in automotive security / *I.D. Gorbenko, D. Fesenko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №203. P. 97 – 108.

The analysis of problems of using authentication systems for automobile systems is carried out. It is shown that criminals are increasingly interested in modern car protection systems, cars are becoming more technological, which in turn opens up new opportunities for compromising the operation of vehicle components and systems, so security systems are increasingly required to ensure efficiency and safety. Modern systems of protection against illegal seizure of vehicles, better known as "alarms" try to deter attacks by intruders, but in turn can bring additional backdoors for intruders completely unintentionally, for example by adding an interesting feature to the car system, and then this feature can be dual due to problems with the authentication system. Therefore, based on this, car security systems must have the highest level of authentication security, which requires the use of a decentralized blockchain network with nodes for each car, authenticating the user in groups, this will move away from the standard client-server architecture, which is not sufficiently secure. . The main ways to solve this problem are to build a comprehensive security system, which in turn includes an improved and reliable authentication measure based on a decentralized blockchain network and two comprehensive schemes to update the critical data transmission system of the car – CAN network. The use of these systems will improve the security of the identification system and information flowing between critical units, which will improve the safety of the car from theft, as well as from the ability of attackers to create emergencies remotely.

Key words: blockchain; attack; vurlerability; decentralization; substitute; automotive security

3 fig. Ref: 4 items.

УДК 004.056.5

Дослідження властивостей носіїв інформації для стеганографічного приховування даних в кластерних файлових системах / *К.Ю. Шеханін, Ю.І. Горбенко, Л.О. Горбачова, О.О. Кузнецов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 203. С. 109 – 120.

Останніми роками набули розвитку методи технічної стеганографії. В таких системах приховування інформації досягається шляхом використання властивостей, які штучно зроблено людиною при побудові різних технічних засобів. Прикладом технічної стеганографії є застосування особливостей побудови кластерних файлових систем. Вони дозволяють ефективно приховувати інформацію шляхом зміни чергування окремих кластерів т.з. покрівельних файлів. Імена (назви) таких файлів є ключовою інформацією, і відновити приховуване повідомлення без назв покрівельних файлів вкрай важко. У роботі описано та проаналізовано різні сучасні технології збереження інформації, а саме HDD, Flash-USB, SSD. Проаналізовано кількість реалізованої продукції, ціна, швидкість зчитування та запису. Також проаналізовано важливі показники ефективності носіїв інформації з точки зору стеганографічних методів приховування інформації у кластерних файлових системах. Наприклад, досліджено швидкість послідовного зчитування/запису та швидкість доступу до випадкового кластеру, що відповідає швидкості доступу до фрагментованного файлу. Для цього використовувалися результати тестувань з ресурсу UserBenchmark. Тестування виконувалися методами Sequential та Random4k. Як висновок надана оцінка носіїв інформації та надано рекомендації щодо використання носія інформації та методу приховування даних шляхом перемішування кластерів у структурі файлової системи.

Ключові слова: файлові носії інформації; фрагментація; швидкість доступу; приховування даних; стеганографія

Табл. 5. Іл. 4. Бібліогр.: 39 назв.

УДК 004.056.5

Исследование свойств носителей информации для стеганографического сокрытия данных в кластерных файловых системах / *К.Ю. Шеханин, Ю.І. Горбенко, Л.О. Горбачова, А.А. Кузнецов* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 203. С. 109 – 120.

В последние годы получили развитие методы технической стеганографии. В таких системах сокрытие информации достигается путем использования свойств, искусственно созданных человеком при построении различных технических средств. Примером технической стеганографии является применение особенностей построения кластерных файловых систем. Это позволяет эффективно скрывать информацию путем изменения чередования отдельных кластеров т.н. кровельных файлов. Имена (названия) таких файлов являются ключевой информацией, и восстановить скрываемое сообщение без названий кровельных файлов крайне трудно. В работе описаны и проанализированы различные современные технологии хранения информации, а именно HDD, Flash-USB, SSD. Проанализированы количество реализованной продукции, цена, скорость считывания и записи. Также проанализированы важные показатели эффективности носителей информации с точки зрения стеганографических методов сокрытия информации в кластерных файловых системах. Например, исследованы скорость последовательного чтения/записи и скорость доступа к случайному кластера, соответствующая скорость доступа к фрагментованному файлу. Для этого использовались результаты тестирования с ресурса UserBenchmark. Тестирование выполнялись методами Sequential и Random4k. Как вывод дана оценка носителей информации и даны рекомендации по использованию метода сокрытия данных путем перемешивания кластеров в структуре файловой системы.

Ключевые слова: файловые носители информации; фрагментация; скорость доступа; сокрытие данных; стеганография

Табл. 5. Ил. 4. Библиогр.: 39 назв.

UDC 004.056.5

Study of storage devices properties for steganographic data hiding in cluster file systems / *K.Yu. Shekhanin, Yu.I. Gorbenko, L.O. Gorbachova, A.A. Kuznetsov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №203. P. 109 – 120.

Methods for technical steganography have been developed in recent years. Hiding of information in such systems is achieved by using properties artificially created by human while constructing various technical means. An example of technical steganography is the application of the features of constructing clustered file systems. This makes it possible to hide information effectively by changing the alternation of individual clusters, the so-called cover files. The names of such files are the key information and it is extremely difficult to recover a hidden message without links (i.e. without names) of cover files. This work describes and analyzes various modern information storage technologies, namely HDD, Flash-USB, SSD. We have analyzed different indicators such as the number of implemented products, price, speed of reading and writing. The important indicators of storage media efficiency with regard to steganographic methods of hiding information in cluster file systems were also analyzed. For example, we have investigated the speed of sequential reading / writing and the speed of access to a random cluster that is similar to the speed of access to a fragmented file. For this, we used the test results from the UserBenchmark resource. Tests were performed using Sequential and Random4k methods. In conclusion, an assessment of information carriers is given and recommendations are given on using the method of hiding data by mixing clusters in the structure of the file system.

Key words: File storage media; fragmentation; speed of access; data hiding; steganographic

5 tab. 4 fig. Ref: 39 items.

УДК 004.056.52

Менеджмент вразливостей з використанням формалізованого опису / *В.О. Поддубний, О.В. Сєверінов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 203. С. 121 – 125.

Розглядаються основні етапи менеджменту вразливостей та проблеми, які виникають при оцінці ризиків й прийнятті рішень під час менеджменту вразливостей в інформаційно-телекомунікаційній системі. Здійснюється припущення, що сучасні методики не є достатніми для ефективного менеджменту вразливостей. Висувається необхідність створення системи оцінювання ризиків для покращення процедур прийняття рішень. Здійснюється порівняння формалізованого та неформалізованого опису інформаційно-телекомунікаційної системи. Як результатом такого порівняння є висновок, що формалізований опис має низку переваг, тому створювана система повинна бути саме формалізованою, а для цього необхідно щоб вона була побудована на базі формалізованого опису інформаційно-телекомунікаційної системи. При додаванні якісного оцінювання вразливостей (наприклад оцінок вразливостей згідно з Common Vulnerability Scoring System) ця система матиме однозначність трактування, буде чіткою, гнучкою та простою в використанні. Додатковою перевагою такої системи є можливість автоматизації процесів оцінки та прийняття рішень, що дозволить виключити людський вплив та мінімізувати суб'єктивний фактор під час менеджменту вразливостей в інформаційно-телекомунікаційній системі. Така система не виключить вплив адміністратора безпеки та аудиту, проте допоможе йому в прийнятті рішень, оцінці ризиків, зменшить вірогідність помилок, допоможе новому персоналу під час вибору рішень.

Ключові слова: вразливості; система менеджменту вразливостями; СУІБ; формалізований опис ІТС; якісне оцінювання вразливостей; NVD; CVSS.

Іл. 2. Бібліогр.: 10 назв.

УДК 004.056.52

Менеджмент уязвимостей с использованием формализованного описания / *В.А. Поддубный, О.В. Северинов* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 203. С. 121 – 125.

Рассматриваются основные этапы менеджмента уязвимостей и проблемы, которые возникают при оценке рисков и принятии решений во время управления уязвимостей в информационно-телекоммуникационной системе. Осуществляется предположение, что современные методики не являются достаточными для эффективного менеджмента уязвимостей. Выдвигается необходимость создания системы оценки рисков для улучшения процедур принятия решений. Осуществляется сравнение формализованного и неформализованного описания информационно-телекоммуникационной системы. Как результат такого сравнения сделан вывод, что формализованное описание имеет ряд преимуществ, поэтому создаваемая система должна быть именно формализованной, а для этого необходимо, чтобы она была построена на базе формализованного описания информационно-телекоммуникационной системы. При добавлении качественной оценки уязвимостей (например, оценок уязвимостей согласно Common Vulnerability Scoring System) эта система будет иметь однозначность трактовки, будет четкой, гибкой и простой в использовании. Дополнительным преимуществом такой системы является возможность автоматизации процессов оценки и принятия решений, что позволит исключить человеческое влияние и минимизировать субъективный фактор при менеджменте уязвимостей в информационно-телекоммуникационной системе. Такая система не исключит влияние администратора безопасности и аудита, однако поможет ему в принятии решений, оценке рисков, уменьшит вероятность ошибок, поможет новому персоналу во время выбора решений.

Ключевые слова: уязвимости; система менеджмента уязвимостями; СУИБ; формализованное описание ИТС; качественное оценивание уязвимостей; NVD; CVSS.

Ил. 2. Библиогр.: 10 назв.

UDC 004.056.52

Vulnerability management using a formalized description / *V.O. Poddubnyi, O.B. Severinov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №203. P. 121 – 125.

The article considers the main stages of vulnerability management and the problems arising in risk assessment and decision making during vulnerability management in the information and telecommunications system. It is assumed that modern techniques are not sufficient for effective vulnerability management. There is a need for creating a risk assessment system to improve decision-making procedures. The comparison of the formalized and informal description of the information and telecommunication system is described. The conclusion from the comparison results is that the formalized description has a number of advantages, so it is necessary that it should be built based on a formalized description of the information and telecommunication system. When adding qualitative vulnerability assessments (such as Common Vulnerability Scoring System vulnerabilities), this system will be unambiguous, clear, flexible, and easy to use. An additional advantage of such a system is the ability to automate assessment and decision-making processes, which will eliminate human influence and minimize the subjective factor in the management of vulnerabilities in the information and telecommunications system. Such a system will not exclude the influence of the security administrator, but will help him in decision-making, risk assessment, reduce the likelihood of errors, will help new staff in choosing decisions.

Key words: vulnerabilities; vulnerability management system; ISMS; formalized description of ITS; qualitative assessment of vulnerabilities; NVD; CVSS.

2 fig. Ref: 10 items.

МЕТОДИ СИНТЕЗУ ТА АНАЛІЗУ СИГНАЛІВ
МЕТОДЫ СИНТЕЗА И АНАЛИЗА СИГНАЛОВ
METHODS OF SYNTHESIS AND ANALYSIS OF SIGNALS

УДК 621.391

Методи синтезу і формування систем нелінійних дискретних сигналів для сучасних інформаційно-комунікаційних систем / *І.Д. Горбенко, О.А. Замула, Хо Чі Лик* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 203. С. 126 – 132.

Наведено результати вирішення актуальної проблеми поліпшення показників ефективності функціонування інформаційно-комунікаційних систем (ІКС), зокрема інформаційної безпеки, завадостійкості, скритності, швидкості формування і обробки інформації. Використовувані методи формування та обробки даних, а також класи широкосмугових сигналів, які застосовуються як фізичний переносник даних, не дозволяють забезпечити необхідні (особливо для об’єктів критичної інфраструктури) показники інформаційної безпеки і завадозахищеності. При цьому як дискретні послідовності (ДП), які розширюють спектр (маніпулюють несучою частотою), повинні бути використані ДП, які засновані на нелінійних правилах побудови і мають покращені кореляційні, ансамблеві і структурні властивості. Запропоновано методи синтезу і формування нелінійних дискретних складних сигналів, а саме – так званих криптографічних сигналів. Перший метод, що представлено, використовує випадкові (псевдовипадкові) процеси. Інший метод засновано на реалізації операції децимації вихідної дискретної послідовності символів, яка отримана за результатами реалізації першого методу, і забезпечує синтез сис-

теми сигналів для визначеної тривалості сигналу. Отримані аналітичні вирази для визначення часу синтезу системи сигналів із застосуванням запропонованих методів. Показано, що швидкодія методу формування сигналів на основі операції децимації для визначеної тривалості сигналу більш ніж на три порядки перевищує швидкодію методу, що заснований на використанні випадкових (псевдовипадкових) процесів. На основі проведеного комп'ютерного моделювання показано, що сигнали, які отримані із застосуванням запропонованих методів, мають ідентичні властивості (кореляційні, ансамблеві, структурні).

Ключові слова: функція кореляції; дискретні послідовності; синтез систем сигналів; шумоподібний сигнал, стійкість перед перешкодами прийому сигналів; криптографічний сигнал; статистичні характеристики кореляційної функції, децимація.

Табл. 4. Бібліогр.: 10 назв.

УДК 621.391

Методы синтеза и формирование системы нелинейных дискретных сигналов для современных информационно-коммуникационных систем / *И.Д. Горбенко, А.А. Замула, Хо Чи Лык* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 203. С. 126 – 132.

Приводятся результаты решения актуальной проблемы улучшения показателей эффективности функционирования информационно-коммуникационных систем (ИКС), в частности информационной безопасности, помехоустойчивости, скрытности, скорости формирования и обработки информации. Используемые методы формирования и обработки данных, а также классы широкополосных сигналов, применяемых в качестве физических переносчиков данных, не позволяют обеспечить необходимые (особенно для объектов критической инфраструктуры) показатели информационной безопасности и помехозащищенности. При этом в качестве дискретных последовательностей (ДП), которые расширяют спектр (манипулируют несущей частотой), должны быть использованы ДП, основанные на нелинейных правилах построения и имеющие улучшенные корреляционные, ансамблевые и структурные свойства.

Предложены методы синтеза и формирования нелинейных дискретных сложных сигналов, а именно так называемых криптографических сигналов. Первый метод, который представлен в статье, использует случайные (псевдослучайные) процессы. Другой метод основан на реализации операции децимации исходной дискретной последовательности символов, полученной по результатам реализации первого метода, и обеспечивает синтез ансамбля сигналов для определенной длительности сигнала.

Получены аналитические выражения для определения времени синтеза ансамбля сигналов с применением предложенных методов. Показано, что быстродействие метода формирования сигналов на основе операции децимации, для определенной длительности сигнала, более чем на три порядка превышает быстродействие метода, основанного на использовании случайных (псевдослучайных) процессов. На основе проведенного компьютерного моделирования показано, что сигналы, полученные с применением предложенных методов, обладают идентичными корреляционными, ансамблевыми, структурными свойствами.

Ключевые слова: функция корреляции; дискретные последовательности; синтез систем сигналов; шумоподобный сигнал, помехоустойчивость приема сигналов; криптографический сигнал; статистические характеристики корреляционной функции, децимация.

Табл. 4. Библиогр.: 10 назв.

UDC 621.391

Methods of synthesis and formation of a system of nonlinear discrete signals for modern information and communication systems / *I.D. Gorbenko, A.A. Zamula, Ho Tri Luc* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №203. P. 126 – 132.

The paper presents the results of solving the urgent problem of improving the performance indicators of information and communication systems (ICS), in particular, information security, noise immunity, secrecy, the speed of formation and processing of information. The use of the distributed spectrum technology (broadband noise-like signals) is a promising direction for ensuring the security of information resources. The methods used for data formation and processing, as well as the classes of broadband signals used as physical data carriers, do not allow providing the necessary (especially for critical infrastructure facilities) indicators of information security and noise immunity. In this case, as discrete sequences (DS) that expand the spectrum (manipulate the carrier frequency), should be used DS based on nonlinear construction rules and having improved correlation, ensemble and structural properties. Methods for the synthesis and formation of nonlinear discrete complex signals, namely, the so-called cryptographic signals, are proposed. The first method, presented in the article, uses random (pseudo-random) processes. Another method is based on the implementation of the operation of decimation of the original discrete sequence of symbols obtained from the results of the implementation of the first method; it provides the synthesis of an ensemble of signals for a certain signal duration. Analytical expressions are obtained for determining the synthesis time of an ensemble of signals using the proposed methods. It is shown that the speed of the signal generation method based on the decimation operation for a certain signal duration is more than three orders of magnitude higher than the speed of the method based on the random (pseudo-random) processes used. At the same time, based on the carried out computer simulation, it is shown that the signals obtained using the proposed methods have identical correlation, ensemble, and structural properties.

Key words: correlation function; discrete sequences; synthesis of signal systems; noise-like signal, noise immunity of signal reception; cryptographic signal; statistical characteristics of the correlation function, decimation.

4 tab. Ref: 10 items.

УДК 621.391

Порівняльний аналіз завадостійкості прийому нелінійних складних дискретних сигналів зі стандартними сигналами АФМ-16 BPSK / *С.Г. Рассомахін, О.А. Замула, І.Д. Горбенко, Хо Чі Лик* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 203. С. 133 – 140.

Показано, що рішення проблеми підвищення завадозахищеності (завадостійкості і скритності функціонування) ІКС може бути досягнуто на основі застосування систем нелінійних сигналів з поліпшеними ансамблевими, структурними і кореляційними властивостями. Розглянуто два класи нелінійних складних дискретних сигналів: характеристичні дискретні сигнали (ХДС) і криптографічні сигнали (КС). Представлено методи синтезу зазначених сигналів. Наведено статистична імітаційна модель для дослідження завадостійкості різних класів сигналів в гауссовому каналі. Із застосуванням такої моделі отримано оцінки ймовірності помилки у залежності від відношення сигнал/шум для різних класів сигналів, а саме ХДС, КС та стандартних сигналів BPSK АФМ-16. Показано, що для відношення сигнал/шум – 10, ймовірність помилки для ХДС складає 4.6875e-06, для КС – 3.515625e-06, а для – АФМ-16 – 0.002025. Таким чином, використання нелінійних складних дискретних сигналів, зокрема ХДС та КС, дозволяє суттєво підвищити завадостійкість прийому сигналів у сучасних ІКС. Зважаючи на покращені ансамблеві і структурні властивості зазначених нелінійних сигналів, є можливість значно поліпшити показники крипто- і імітозахищеності функціонування систем.

Ключові слова: завадостійкість прийому; скритність; інформаційна безпека; дискретні послідовності; гаусів канал; ймовірність помилки; шумоподібний сигнал.

Табл. 1. Іл. 5. Бібліогр.: 10 назв.

УДК 621.391

Сравнительный анализ помехоустойчивости приема нелинейных сложных дискретных сигналов со стандартными сигналами АФМ-16 BPSK / *С.Г. Рассомахин, А.А. Замула, И.Д. Горбенко, Хо Чи Лык* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 203. С. 133 – 140.

Показано, что решение проблемы повышения помехозащищенности (помехоустойчивости и скрытности функционирования) ИКС может быть достигнуто на основе применения систем нелинейных сигналов с улучшенными ансамблевыми, структурными и корреляционными свойствами. Рассмотрены два класса нелинейных сложных дискретных сигналов: характеристические дискретные сигналы (ХДС) и криптографические сигналы (КС). Представлены методы синтеза указанных сигналов. Приведена статистическая имитационная модель для исследования помехоустойчивости различных классов сигналов в гауссовом канале. С применением такой модели получены оценки зависимости вероятности ошибки от отношения сигнал / шум для различных классов сигналов, а именно: ХДС, КС и стандартных сигналов BPSK АФМ-16. Показано, что для отношения сигнал / шум – 10 вероятность ошибки для ХДС составляет 4.6875e-06, для КС – 3.515625e-06, а для – АФМ-16 – 0.002025. Таким образом, использование нелинейных сложных дискретных сигналов, в частности ХДС и КС, позволяет существенно повысить помехоустойчивость приема сигналов в современных ИКС. Учитывая улучшенные ансамблевые и структурные свойства указанных нелинейных сигналов, есть возможность значительно улучшить показатели крипто- и имитозащищенности функционирования систем.

Ключевые слова: помехоустойчивость приема; скрытность; информационная безопасность; дискретные последовательности; гауссов канал; вероятность ошибки; шумоподобный сигнал.

Табл. 1. Ил. 5. Библиогр.: 10 назв.

UDC 621.391

Comparative analysis of noise immunity of reception of nonlinear complex discrete signals with standard signals AFM-16 BPSK / *S.G. Rassomakhin, A.A. Zamula, I.D. Gorbenko, Ho Tri Luc* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №203. P. 133 – 140.

The article shows that the solution to the problem of increasing the noise immunity (noise immunity and secrecy of functioning) of the ICS can be achieved using systems of nonlinear signals with improved ensemble, structural and correlation properties. Two classes of nonlinear complex discrete signals are considered: characteristic discrete signals (CDS) and cryptographic signals (CS). Methods for the synthesis of these signals are presented. The paper gives a statistical simulation model for studying the noise immunity of various classes of signals in the Gaussian channel. Using this model, estimates of the dependence of the error probability on the signal-to-noise ratio were obtained for various classes of signals, namely: CDS, KS and standard BPSK AFM-16 signals. It is shown that for the signal-to-noise ratio – 10 the error probability for the CDR is 4.6875e-06, for the CS is 3.515625e-06, and for the AFM-16 is 0.002025. Thus, the use of nonlinear complex discrete signals, in particular, CDS and KS, can significantly increase the noise immunity of signal reception in modern ICS. At the same time, taking into account the improved ensemble and structural properties of these nonlinear signals, it is possible to improve significantly the indicators of crypto- and imitation security of the systems functioning.

Key words: reception immunity; secrecy; information security; discrete sequences; Gaussian channel; error probability; noise-like signal.

1 tab. 5 fig. Ref: 10 items.

УДК 621.391

Статистичні властивості похідних систем сигналів / *О.А. Замула, І.Д. Горбенко, Хо Чі Лик* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 203. С. 141 – 147.

Актуальною проблемою залишається пошук ефективних методів синтезу дискретних сигналів (послідовностей), що відповідають потенційно можливим граничним характеристикам кореляційних функцій і володіють необхідними кореляційними, структурними, ансамблевими властивостями. Авторами запропоновано метод синтезу похідних систем сигналів, для яких у якості вихідних застосовуються ортогональні сигнали, а у якості таких, що продукують, – нелінійні дискретні складні криптографічні сигнали (КС). Синтез останніх засновано на використанні випадкових (псевдовипадкових) процесів, у тому числі, алгоритмів криптографічного перетворення інформації. Синтезовані таким чином похідні сигнали володіють покращеними (у порівнянні з лінійними класами сигналів) ансамблевими і кореляційними властивостями, тоді як статистичні властивості таких систем сигналів є не вивченими. Наведено результати тестування похідних систем сигналів із застосуванням тестів, що визначені у FIPS PUB 140 та NIST 800-22. Аналіз результатів дозволяє стверджувати, що статистичні властивості даного класу похідних сигналів задовольняють вимогам, що пред'являються до псевдовипадкових послідовностей: непередбачуваність, незворотність, випадковість, незалежність символів і ін. По суті такі сигнали не відрізняються від випадкових послідовностей. Застосування запропонованого класу похідних сигналів дозволить поліпшити показники завадостійкості прийому сигналів, інформаційної безпеки і скритності функціонування ІКС.

Ключові слова: тестування похідних сигналів; дискретні послідовності; завадостійкість прийому сигналів; криптографічний сигнал; похідний сигнал; ортогональний сигнал; статистичні властивості сигналів.

Табл. 8. Бібліогр.: 10 назв.

УДК 621.391

Статистические свойства производных систем сигналов / *А.А. Замула, И.Д. Горбенко, Хо Чи Лык* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 203. С. 141 – 147.

Актуальной проблемой остается поиск эффективных методов синтеза дискретных сигналов (последовательностей), соответствующих потенциально возможным предельным характеристикам корреляционных функций и обладающих необходимыми корреляционными, структурными, ансамблевыми свойствами. Авторами предложен метод синтеза производных систем сигналов, для которых в качестве исходных применяются ортогональные сигналы, а в качестве производящих – нелинейные дискретные сложные криптографические сигналы (КС). Синтез последних основан на использовании случайных (псевдослучайных) процессов, в том числе алгоритмов криптографического преобразования информации. Синтезированные таким образом производные сигналы обладают улучшенными (по сравнению с линейными классами сигналов) ансамблевыми и корреляционными свойствами, тогда как статистические свойства таких систем сигналов остаются не изученными. Приведены результаты тестирования производных систем сигналов с применением тестов, которые определены в FIPS PUB 140 и NIST 800-22. Анализ результатов позволяет утверждать, что статистические свойства данного класса производных сигналов удовлетворяют требованиям, предъявляемым к псевдослучайным последовательностям: непредсказуемость, необратимость, случайность, независимость символов и др. По сути, такие сигналы не отличаются от случайных последовательностей. Применение предложенного класса производных сигналов позволит улучшить показатели помехоустойчивости приема сигналов, информационной безопасности и скрытности функционирования ИКС.

Ключевые слова: тестирование производных сигналов; дискретные последовательности; помехоустойчивость приема сигналов; криптографический сигнал; производный сигнал; ортогональный сигнал; статистические свойства сигналов.

Табл. 8. Библиогр.: 10 назв.

UDC 621.391

Statistical properties of derived signal systems / *A.A. Zamula, I.D. Gorbenko, Ho Tri Luc* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №203. P. 141 – 147.

The search for effective methods of synthesis of discrete signals (sequences) that correspond to the potentially possible limiting characteristics of correlation functions and possess the necessary correlation, structural, ensemble properties remains an urgent problem. The authors have proposed a method for the synthesis of derivatives of signal systems, for which orthogonal signals are used as the initial ones, and nonlinear discrete complex cryptographic signals (CS) are used as generating signals. The synthesis of the latter ones is based on the use of random (pseudo-random) processes, including algorithms for cryptographic information transformation. Derivative signals synthesized in this way have improved (in comparison with linear signal classes) ensemble and correlation properties, while the statistical properties of such signal systems remain unexplored. The paper presents the results of testing derived signal systems using the tests defined in FIPS PUB 140 and NIST 800-22. Analysis of the results obtained allows us to assert that the statistical properties of this class of derived signals satisfy the requirements for pseudo-random sequences: unpredictability, irreversibility, randomness, independence of symbols, etc. In essence, such signals do not differ from random sequences. The use of the proposed class of derived signals will improve the performance of signal reception noise immunity, information security and secrecy of the ICS functioning.

Key words: testing of derived signals; discrete sequences; noise immunity of signal reception; cryptographic signal; derived signal; orthogonal signal; statistical properties of signals.

8 tab. Ref: 10 items.

РАДІОТЕХНІЧНІ СИСТЕМИ
РАДИОТЕХНИЧЕСКИЕ СИСТЕМЫ
RADIO ENGINEERING SYSTEMS

УДК 621.396.96, 621.397.48:004.932.2

Комплексна обробка сигналів інтегрованої системи спостереження безпілотних літальних апаратів з використанням цілевказівки / *В.М. Карташов, В.Н. Олейніков, В.І. Леонідов, В.В. Воронін, А.І. Капуста, І.С. Селєзнев, Є.В. Першин* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 203. С. 148 – 161.

Одна з актуальних науково-технічних проблем сучасності полягає в розробці методів і засобів захисту різноманітних об'єктів від впливу безпілотних літальних апаратів (БПЛА), які становлять значну потенційну загрозу для різних областей діяльності людини – військової, господарської та повсякденної. Значні технічні можливості, широка номенклатура і порівняно невисока вартість БПЛА в поєднанні з труднощами їх спостереження і контролю – основні особливості даної проблеми. У даний час для виявлення і спостереження безпілотних літальних апаратів широко використовуються радіолокаційний, акустичний, оптичний і інфрачервоний методи і відповідні засоби.

У статті розглянуто інформаційні можливості кожного з методів і засобів, що входять до складу комплексної системи виявлення, вимірювання координат і параметрів руху БПЛА. Показано, що найкращими пошуковими можливостями володіє радіолокаційний метод, йому поступаються оптичний, інфрачервоний і акустичний методи. Обговорюється алгоритм послідовного підключення наявних в комплексній системі інформаційних ресурсів з урахуванням наявності у відповідних засобів пошукових можливостей.

Синтезовані нові ефективні методи комплексної обробки багатомодальних сигналів і зображень в інтегрованій комплексній системі спостереження безпілотних літальних апаратів, побудовані з урахуванням природного просторового ешелонування різних інформаційних каналів і з використанням цілевказівки. Показано особливості об'єднання багатомодальної інформації з використанням нейромережевих технологій при використанні цілевказань у комплексній системі.

Ключові слова: безпілотний літальний апарат; виявлення; розпізнавання; радіолокаційна станція; содар; відеокамера; комплексна система; обробка сигналів; цілевказування.

Табл. 1. Іл. 5. Бібліогр.: 44 назв.

УДК 621.396.96, 621.397.48:004.932.2

Комплексная обработка сигналов интегрированной системы наблюдения беспилотных летательных аппаратов с использованием целеуказания / *В.М. Карташов, В.Н. Олейников, В.И. Леонидов, В.В. Воронин, А.И. Капуста, И.С. Селезнев, Е.В. Першин* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 203. С. 148 – 161.

Одна из актуальных научно-технических проблем современности заключается в разработке методов и средств защиты разнообразных объектов от воздействия беспилотных летательных аппаратов (БПЛА), несущих значительную потенциальную угрозу для различных областей деятельности человека – военной, хозяйственной и повседневной. Значительные технические возможности, широкая номенклатура и сравнительно невысокая стоимость БПЛА в сочетании с трудностями их наблюдения и контроля – основные особенности данной проблемы. В настоящее время для обнаружения и наблюдения беспилотных летательных аппаратов широко используются радиолокационный, акустический, оптический и инфракрасный методы и соответствующие средства.

Рассмотрены информационные возможности каждого из методов и средств, входящих в состав комплексной системы обнаружения, измерения координат и параметров движения БПЛА. Показано, что наилучшими поисковыми возможностями обладает радиолокационный метод, ему уступают оптический, инфракрасный и акустический методы. Обсуждается алгоритм последовательного подключения имеющихся в комплексной системе информационных ресурсов с учетом наличия у соответствующих средств поисковых возможностей.

Синтезированы новые эффективные методы комплексной обработки многомодальных сигналов и изображений в интегрированной комплексной системе наблюдения беспилотных летательных аппаратов, построенные с учетом естественного пространственного эшелонирования различных информационных каналов и с использованием целеуказания. Показаны особенности объединения многомодальной информации с использованием нейросетевых технологий при использовании целеуказаний в комплексной системе.

Ключевые слова: беспилотный летательный аппарат; обнаружение; распознавание; радиолокационная станция; содар; видеокамера; комплексная система; обработка сигналов; целеуказание.

Табл. 1. Ил. 5. Библиогр.: 44 назв.

UDC 621.396.96, 621.397.48:004.932.2

Complex processing of signals of integrated unmanned aerial vehicles surveillance system with the use of target designation / *V.M. Kartashov, V.M. Oleinikov, V.P. Ryabukha, V.I. Leonidov, V.V. Voronin, A.I. Kapusta, I.S. Selezniov, I.V. Pershyn* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №203. P. 148 – 161.

One of the urgent scientific and technical problems of our time is the development of methods and means of protecting various objects against the impact of unmanned aerial vehicles (UAVs) which carry a significant potential threat

to various areas of human activity – military, economic and everyday life. Significant technical capabilities, a wide range and relatively low cost of UAVs, combined with the difficulties of their observation and control, are the main features of this problem. Currently, radar, acoustic, optical and infrared methods with the appropriate facilities are widely used to detect and observe unmanned aerial vehicles.

The article discusses the information capabilities of each of the methods and tools that are a part of an integrated system for detecting, measuring coordinates and parameters of UAV motion. It is shown that the radar method has the best search capabilities, while optical, infrared and acoustic methods are inferior to it. An algorithm for sequential connection of information resources available in an integrated system is discussed, taking into account the availability of search capabilities of the relevant means.

New effective methods of complex processing of multimodal signals and images in a complex integrated surveillance system for unmanned aerial vehicles, built taking into account the natural spatial separation of various information channels and using target designation, have been synthesized. The features of combining multimodal information with the use of neural network technologies when using target designations in an integrated system are shown.

Key words: unmanned aerial vehicle; detection; recognition; radar station; sodar; video camera; integrated system; signal processing; target designation.

1 tab. 5 fig. Ref: 44 items.

УДК 621.396.96:004.045

Оптимізація обробки даних в літакових відповідачах системи ідентифікації «свій-чужий» / *І.В. Свид, І.І. Обод, Г.Е. Заволодько* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 203. С. 162 – 169.

Синтезована оптимальна структура обробки даних літакового відповідача системи ідентифікації «свій-чужий», на основі критерію Неймана – Пірсона. Показано, що при синтезі та аналізі оптимальної структури обробки сигнальних даних у літакових відповідачах систем ідентифікації «свій-чужий» необхідно враховувати багатоканальність прийому сигналів запиту та обмеження відносної пропускної здатності літакового відповідача, яка зумовлена наявним принципом побудови системи як одноканальної системи масового обслуговування з відмовами. Запропоновані моделі дозволяють реалізувати структури обробки даних сигналів запиту для ситуацій міжканального злиття попередніх канальних рішень про виявлення сигналів запиту або імпульсних складових сигналів запиту. В запропонованій структурі оптимізація обробки даних здійснюється не тільки за часовими, але й за просторовими параметрами сигналів запиту, а також враховується відносна пропускна здатність літакового відповідача. Показано, що міжканальне злиття результатів виявлення складових імпульсів сигналів запиту більш переважне в порівнянні з існуючим алгоритмом злиття результатів виявлення сигналів запиту, так як дозволяє підвищити якість виявлення сигналів запиту та знизити залежність ймовірності виявлення сигналів запиту від відносної пропускної здатності літакового відповідача.

Ключові слова: система ідентифікації «свій-чужий»; управління повітряним рухом; повітряний об’єкт; літаковий відповідач; обробка даних; сигнал запиту; сигнал відповіді; оптимізація; критерій Неймана – Пірсона; відносна пропускна здатність; алгоритм злиття.

Іл. 4. Бібліогр.: 28 назв.

УДК 621.396.96:004.045

Оптимизация обработки данных в самолетных ответчиках системы идентификации «свой-чужой» / *И.В. Свид, И.И. Обод, А.Э. Заволодько* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 203. С. 162 – 169.

Синтезирована оптимальная структура обработки данных самолетного ответчика системы идентификации «свой-чужой», на основе критерия Неймана-Пирсона. Также показано, что при синтезе и анализе оптимальной структуры обработки сигнальных данных в самолетных ответчиках систем идентификации «свой-чужой» необходимо учитывать многоканальность приема сигналов запроса и ограничения относительной пропускной способности самолетного ответчика, которая обусловлена имеющимся принципом построения системы как одноканальной системы массового обслуживания с отказами. Предложенные модели позволяют реализовать структуры обработки данных сигналов запроса для ситуаций межканального слияния предыдущих канальных решений об обнаружении сигналов запроса или импульсных составляющих сигналов запроса. В предложенной структуре оптимизация обработки данных осуществляется не только по времени, но и по пространственным параметрам сигналов запроса, а также учитывается относительная пропускная способность самолетного ответчика. Показано, что межканальные слияния результатов выявления составляющих импульсов запросных сигналов более предпочтительно по сравнению с существующим алгоритмом слияния результатов обнаружения запросных сигналов, так как позволяет повысить качество обнаружения запросных сигналов и снизить зависимость вероятности обнаружения запросных сигналов от относительной пропускной способности самолетного ответчика.

Ключевые слова: система идентификации «свой-чужой»; управления воздушным движением; воздушный объект; самолетный ответчик; обработка данных; сигнал запроса; сигнал ответа; оптимизация; критерий Неймана – Пирсона; относительная пропускная способность; алгоритм слияния.

Ил. 4. Библиогр.: 28 назв.

UDC 621.396.96:004.045

Optimization of data processing in aircraft transponder of the "friend or foe" identification system / *I.V. Svyd, I.I. Obod, G.E. Zavolodko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №203. P. 162 – 169.

The paper synthesizes the optimal structure of data processing of the aircraft transponder of the “friend or foe” identification system based on the Neumann-Pearson criterion. It is also shown, that when synthesizing and analyzing the optimal structure of signal data processing in aircraft transponders of "friend or foe" identification systems, it is necessary to take into account the multichannel reception of request signals and limitations of relative throughput of the aircraft transponder, which is caused by the existing principle of constructing the system as single-channel queuing system with failures. The proposed models make it possible to implement the structures of data processing of request signals for situations of inter-channel merging of previous channel decisions on the detection of request signals or pulse components of the request signals. In the proposed structure, the optimization of data processing is carried out not only in time but also in the spatial parameters of the request signals, and also takes into account the relative bandwidth of the aircraft responder. It is shown that the inter channel merging of the results of detecting the component pulses of the query signals is more preferable compared to the existing algorithm of merging the results of detecting the query signals, as it improves the quality of query signal detection and reduces the dependence of query signal detection of relative response.

Key words: identification system "friend or foe"; air traffic control; air object; aircraft respondent; Data Processing; request signal; response signal; optimization; Neumann-Pearson criterion; relative bandwidth; fusion algorithm.

4 fig. Ref: 28 items.

ЕЛЕКТРОДИНАМІКА, ОПТИКА, ТЕХНІКА, НВЧ
ЭЛЕКТРОДИНАМИКА, ОПТИКА, ТЕХНИКА СВЧ
ELECTRODYNAMICS, OPTICS, MICROWAVE TECHNOLOGY

УДК 537.862

Способи регулювання зворотного зв'язку в лазерах терагерцового діапазону / *М.І. Дзюбенко, В.А. Маслов, В.П. Радіонов, А.А. Фомін* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 203. С. 170 – 175.

Оптимальний коефіцієнт зворотного зв'язку в активному відкритому резонаторі є важливою умовою високої ефективності лазерної генерації. Для точного підбору оптимуму зв'язку і підтримки оптимуму на всіх режимах роботи лазера необхідна можливість плавного регулювання зв'язку. У лазерах терагерцового (ТГц) діапазону є ряд особливостей, які необхідно враховувати при виборі схем регулювання зворотного зв'язку. В роботі наведено огляд і порівняльний аналіз схем лазерних резонаторів (ТГц) діапазону з плавним регулюванням виведення випромінювання. Розглянуто, як давно відомі і широко використовувані, так і новітні схеми лазерних резонаторів. Плавне регулювання вдається реалізувати в резонаторах які утворені металевими дзеркалами повного внутрішнього відбиття і вивідними дзеркалами у вигляді металевих дзеркал з отворами або одновимірних металевих решіток. Проведено аналіз переваг і недоліків кожної з розглянутих оптичних схем лазерних резонаторів.

Показано, що наведені схеми резонаторів дають можливість регулювати і оптимізувати зворотний зв'язок в лазері в процесі його роботи. Всі вони не відрізняються високою складністю і можуть бути реалізовані шляхом переобладнання діючих лазерів. Вибирати конкретну схему слід відповідно до специфіки застосування лазера. Застосування резонаторів з плавним регулюванням зв'язку дозволяє досягати високої ефективності лазерів на всіх енергетичних режимах роботи.

Ключові слова: терагерцові лазери; відкриті резонатори; плавне регулювання зворотного зв'язку.

Іл. 4. Бібліогр.: 8 назв.

УДК 537.862

Способы регулировки обратной связи в лазерах терагерцевого диапазона / *М.И. Дзюбенко, .А. Маслов, В.П. Радионов, А.А. Фомин* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 203. С. 170 – 175.

Оптимальный коэффициент обратной связи в активном открытом резонаторе является важным условием высокой эффективности лазерной генерации. Для точного подбора оптимума связи и поддержания оптимума на всех режимах работы лазера требуется возможность плавной регулировки связи. В лазерах терагерцевого (ТГц) диапазона имеется ряд особенностей, которые необходимо учитывать при выборе схем регулировки обратной связи. В работе приведен обзор и сравнительный анализ схем лазерных резонаторов (ТГц) диапазона с плавной регулировкой вывода излучения. Рассмотрены как давно известные и широко используемые, так и новейшие схемы лазерных резонаторов. Плавную регулировку удается реализовать в резонаторах, образованных металлическими зеркалами полного внутреннего отражения и выводными зеркалами в виде металлических зеркал с отверстиями или одномерных металлических решеток. Проведен анализ преимуществ и недостатков каждой из рассмотренных оптических схем лазерных резонаторов.

Показано, что приведенные схемы резонаторов дают возможность регулировать и оптимизировать обратную связь в лазере в процессе его работы. Все они не отличаются высокой сложностью и могут быть реализованы путем переоборудования действующих лазеров. Выбирать конкретную схему следует в соответствии со спецификой применения лазера. Применение резонаторов с плавной регулировкой связи позволяет добиваться высокой эффективности лазеров на всех энергетических режимах работы.

Ключевые слова: терагерцевые лазеры; открытые резонаторы; плавная регулировка обратной связи.

Ил. 4. Библиогр.: 8 назв.

UDC 537.862

Methods for adjusting feedback in terahertz lasers / *M.I. Dzyubenko, V.A. Maslov, V.P. Radionov, A.A. Fomin* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №203. P. 170 – 175.

The optimal feedback coefficient in an active open resonator is an important condition for high lasing efficiency. For precise selection of the optimum communication and maintaining the optimum in all modes of laser operation, the ability to adjust smoothly the communication is required. Terahertz (THz) lasers have a number of features that one should take into account when choosing feedback control schemes. The paper presents a review and comparative analysis of the schemes of laser resonators (THz) in the range with a smoothly controlled radiation output. The authors consider both long known and widely used, as well as the latest schemes of laser resonators. Smooth adjustment can be realized in resonators formed by metal mirrors of total internal reflection and output mirrors in the form of metal mirrors with holes or one-dimensional metal gratings. The analysis of the advantages and disadvantages of each of the considered optical schemes of laser resonators is carried out.

It is shown that the given resonator schemes make it possible to control and optimize the feedback in the laser during its operation. All of them are not very complex and can be realized by re-equipping existing lasers. The choice of a specific scheme should be made in accordance with the specifics of the laser application. The use of resonators with smooth coupling control makes it possible to achieve high efficiency of lasers at all energy operating modes.

Key words: terahertz lasers; open resonators; smooth feedback control.

4 fig. Ref: 8 items.

УДК 537.226.3

Однорезонаторний НВЧ пристрій для контролю комплексної диелектричної проникності рідких паливно-мастильних матеріалів / *Б.В. Жуков, С.І. Борбульов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 203. С. 176 – 180.

Представлена спрощена структурна схема однорезонаторного НВЧ діелектрометра, призначеного для контролю комплексної діелектричної проникності рідких паливно-мастильних матеріалів. Розглянуто структурну схему НВЧ датчика діелектрометра, виконаного у вигляді паралелепіпеда, всередині якого розміщені хвилеведучі тракти, резонатор, керований і опорний генератори, змішувальний і детекторні діоди і атенюатори. Наведено загальний вигляд нижньої частини корпусу НВЧ датчика.

Розглянуто методику початкового налаштування НВЧ датчика, в процесі якої встановлюється початкові частоти керованого і опорного генераторів і визначається діапазон електронної перебудови частоти керованого генератора.

Наведено методику калібрування діелектрометра по порожній кюветі, яка дозволяє визначити придатність кювети для її використання при проведенні вимірювання комплексної діелектричної проникності зразків паливно-мастильних матеріалів, а також виключити вплив розкиду діелектричної проникності матеріалу кювети на результати вимірювання комплексної діелектричної проникності зразків ПММ.

Розглянуто методику дослідження параметрів зразків паливно-мастильних матеріалів, на підставі вимірів якої дані вимірювань представляються на комплексній площині для виконання аналізу отриманих результатів.

Наведено методику дослідження відмінності зразка паливно-мастильних матеріалу від його еталона, яка включає вимірювання параметрів порожній кювети, вимір дійсної та уявної складових комплексної діелектричної проникності зразка паливно-мастильних матеріалу і його еталона та аналіз відмінностей їх дійсних і уявних складових на комплексній площині.

Ключові слова: діелектрометр; резонатор; пально-мастильні матеріали; комплексна площина; кювета; еталон; діелектрична проникність; надвисокочастотний датчик.

Іл. 4. Бібліогр.: 3 назв.

УДК 537.226.3

Однорезонаторное СВЧ устройство для контроля комплексной диэлектрической проницаемости жидких горюче-смазочных материалов / *Б.В. Жуков, С.И. Борбулев* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 203. С. 176 – 180.

Представлена упрощенная структурная схема однорезонаторного СВЧ диэлектрометра, предназначенного для контроля комплексной диэлектрической проницаемости жидких горюче-смазочных материалов. Рассмотрена структурная схема СВЧ датчика диэлектрометра, выполненного в виде параллелепипеда, внутри которого размещены волноведущие тракты, резонатор, управляемый и опорный генераторы, смесительный и детекторный диоды и аттенюаторы. Приведен общий вид нижней части корпуса СВЧ датчика.

Рассмотрена методика первоначальной настройки СВЧ датчика, в процессе которой выполняется установка начальных частот управляемого и опорного генераторов и определение диапазона электронной перестройки частоты управляемого генератора.

Приведена методика калибровки диэлектрометра по пустой кювете, которая позволяет определить пригодность кюветы для ее использования при проведении измерения комплексной диэлектрической проницаемости образцов горюче-смазочных материалов, а также исключить влияние разброса диэлектрической проницаемости материала кюветы на результаты измерения комплексной диэлектрической проницаемости образцов ГСМ.

Рассмотрена методика исследования параметров образцов горюче-смазочных материалов, на основании измерений которой данные измерений представляются на комплексной плоскости для выполнения анализа полученных результатов.

Приведена методика исследования отличия образца горюче-смазочного материала от его эталона, которая включает измерение параметров пустой кюветы, измерение действительной и мнимой составляющих комплексной диэлектрической проницаемости образца горюче-смазочного материала и его эталона и анализ отличий их действительных и мнимых составляющих на комплексной плоскости.

Ключевые слова: диэлектрометр; резонатор; горючесмазочные материалы; комплексная плоскость; кювета, эталон; диэлектрическая проницаемость; сверхвысокочастотный датчик.

Ил. 4. Библиогр.: 3 назв.

UDC 537.226.3

Single resonator microwave device for monitoring the complex dielectric constant of liquid fuels and lubricants / *B.V. Zhukov, S.I. Borbulev* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №203. P. 176 – 180.

A simplified structural diagram of a single-cavity microwave dielectric meter designed to control the complex permittivity of liquid fuels and lubricants is presented. The structural diagram of the microwave sensor of the dielectrometer, made in the form of a parallelepiped, inside which waveguide paths, a resonator, controlled and reference generators, mixing and detector diodes and attenuators is considered. A general view of the lower part of the microwave sensor housing is given.

The technique of initial tuning of the microwave sensor is considered, during which the initial frequencies of the controlled and reference oscillators are set and the range of electronic frequency tuning of the frequency of the controlled generator is determined.

A method for calibrating a dielectrometer with an empty cuvette is presented. This method makes it possible to determine the suitability of the cuvette for its use in measuring the complex dielectric constant of samples of fuels and lubricants, and to exclude the influence of the dispersion of the dielectric constant of the material of the cuvette on the results of measuring the complex dielectric constant of fuels and lubricants.

The technique of studying the parameters of samples of fuels and lubricants is considered, based on which the measurement data are presented on a complex plane for analyzing the results obtained.

A technique for studying the difference between a fuel and lubricant sample and its standard is presented, which includes measuring the parameters of an empty cell, measuring the real and imaginary components of the complex dielectric constant of the fuel and lubricant sample and its standard, and analyzing the differences between their real and imaginary components on a complex plane.

Key words: dielectric meter; resonator; fuels and lubricants; complex plane; cuvette; standard; dielectric constant; microwave sensor.

4 fig. Ref: 3 items.

УДК 537.86

Розсіювання електромагнітних хвиль дискретним октаедром з резонансних сфер / *А.І. Козар* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 203. С. 181 – 185.

Наведено рішення задачі про розсіяння електромагнітних хвиль дискретним опуклим многогранником – октаедром з резонансних магнітодіелектричних сфер на основі складної ромбічної кристалічної решітки.

Тут розглядається випадок, еквівалентний рентгенівській оптики кристалів, коли $a/\lambda' << 1$ і може бути $a/\lambda_g \sim 1; d,h,l/\lambda' \sim 1$, де a – радіус сфер; λ', λ_g – довжини розсіяної хвилі поза і всередині сфер; d,h,l – постійні решітки. Рішення задачі отримано на основі інтегральних рівнянь електродинаміки Фредгольма 2-го роду, з нелокальними граничними умовами.

Знайдені у роботі вирази для метакрістала у формі октаедра можна використати для вивчення розсіяних кристалом полів в зонах Френеля і Фраунгофера, а також для вивчення його внутрішнього поля.

Отримані в роботі співвідношення можуть знайти застосування при вивченні розсіювання хвиль різного роду опуклими многогранниками, створення на їх основі нових видів обмежених метакристалів, в тому числі і нанокристалів з резонансними властивостями і при вивченні їх поведінки в різних зовнішніх середовищах.

А також при розробці методів моделювання електромагнітних явищ, які можуть відбуватися в реальних кристалах в резонансних областях в оптичному і рентгенівському діапазонах довжин хвиль.

Ключові слова: електромагнітні хвилі; сфера; кристал; рівняння; октаедр.

Іл. 1. Бібліогр.: 5 назв.

УДК 537.86

Рассеяние электромагнитных волн дискретным октаэдром из резонансных сфер / *А.И. Козарь* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 203. С. 181 – 185.

Приведено решение задачи о рассеянии электромагнитных волн дискретным выпуклым многогранником – октаэдром из резонансных магнитодиэлектрических сфер на основе сложной ромбической кристаллической решетки.

Здесь рассматривается случай, эквивалентный рентгеновской оптике кристаллов, когда $a/\lambda' << 1$ и может быть a/λ_g ~1; $d,h,l/\lambda'$ ~1, где a – радиус сфер; λ', λ_g – длины рассеиваемой волны вне и внутри сфер; d,h,l – постоянные решетки. Решение задачи получено на основе интегральных уравнений электродинамики Фредгольма 2-го рода с нелокальными граничными условиями.

Найденные в работе выражения для метакристалла в форме октаэдра можно использовать для изучения рассеянных кристаллом полей в зонах Френеля и Фраунгофера, а также для изучения его внутреннего поля.

Полученные в работе соотношения могут найти применение при изучении рассеяния волн различного рода выпуклыми многогранниками, создания на их основе новых видов ограниченных метакристаллов, в том числе и нанокристаллов с резонансными свойствами и при изучении их поведения в различных внешних средах. А также при разработке методов моделирования электромагнитных явлений, которые могут происходить в реальных кристаллах в резонансных областях в оптическом и рентгеновском диапазонах длин волн.

Ключевые слова: электромагнитные волны; сфера; кристалл; уравнение; октаэдр.

Ил. 1. Библиогр.: 5 назв.

UDC 537.86

Scattering of electromagnetic waves by a discrete octahedron from resonant spheres / *A.I. Kozar* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №203. P. 00 – 00.

A solution is given to the problem of scattering of electromagnetic waves by a discrete convex polyhedron – an octahedron of resonant magnetodielectric spheres based on a complex rhombic crystal lattice.

Here we consider a case equivalent to the X-ray optics of crystals, when $a/\lambda' << 1$ and can be a/λ_g ~1; $d,h,l/\lambda'$ ~1, where a is the radius of the spheres; λ', λ_g are the lengths of the scattered wave outside and inside the spheres; d,h,l are constant lattices. The solution of the problem is obtained based on the Fredholm integral equations of electrodynamics of the second kind with nonlocal boundary conditions.

The expressions found in this work for a metacrystal in the form of an octahedron can be used to study the fields scattered by the crystal in the Fresnel and Fraunhofer zones, as well as to study its internal field.

The relations obtained in this work can find application in the study of the scattering of waves of various kinds by convex polyhedrons, the creation on their basis of new types of limited metacrystals, including nanocrystals with resonance properties, and in the study of their behavior in various external media. As well as in the development of methods for modeling electromagnetic phenomena that can occur in real crystals in resonance regions in the optical and X-ray wavelength ranges.

Key words: electromagnetic waves; sphere; crystal; equation; octahedron.

1 fig. Ref: 5 items.

ЗАСТОСУВАННЯ МЕТОДІВ РАДІОТЕХНІКИ
ПРИМЕНЕНИЕ МЕТОДОВ РАДИОТЕХНИКИ
APPLICATION OF METHODS OF RADIO ENGINEERING

УДК 615.472.03

Дослідження частотних характеристик імпедансу біологічних тканин / *В.В. Семенець, В.І. Леонідов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 203. С. 186 – 190.

Формулюється 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.

Приводяться результати експериментальних вимірів характеристик імпедансу в діапазоні частот 20 Гц – 2,0 МГц. Аналізуються частотні залежності модуля напруги на біотканини рослинного походження при її неушкодженому стані, а також після витримки зразків біотканини в морозильній камері на інтервалах часу від 15 хв до двох годин.

Проводиться порівняльний аналіз отриманих частотних залежностей. Показано істотну відмінність частотних залежностей модуля напруги на біотканини від частотної залежності модуля напруги на ізотонічному розчині. Вводиться поняття про те, що критерієм оцінки ступеня поразки біотканини може служити ступінь відмінності частотного розподілу модуля імпедансу біотканини від модуля імпедансу ізотоничного розчину.

Формулюється висновок про доцільність розвитку методу імпедансометрії як методу діагностики життєздатності біотканини, показано, що найбільш перспективним підходом до розвитку методів імпедансометрії є аналіз перехідних процесів при збурюванні біотканини імпульсами електричного струму малої величини.

Ключові слова: імпедансометрія; життєздатність; частотна характеристика; інформативні ознаки.

Іл. 3. Бібліогр.: 15 назв.

УДК 615.472.03

Исследование частотных характеристик импеданса биологических тканей / *В.В. Семенец, В.И. Леонидов* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 203. С. 186 – 190.

Формулируется постановка задачи выявления информативных признаков жизнеспособности биологических тканей при использовании метода импедансометрии. Показано, что так как в настоящее время в медицинской диагностической практике отсутствует приборная база, позволяющая в оперативной обстановке осуществлять диагностику способности биологической ткани к самовосстановлению после получения травм и поражений в результате термического воздействия, огнестрельного ранения или длительного сдавливания, то разработка методов и средств инструментальной диагностики в этой области знаний является важной современной задачей.

Приводятся результаты экспериментальных измерений характеристик импеданса в диапазоне частот 20 Гц – 2,0 МГц. Анализируются частотные зависимости модуля напряжения на биоткани растительного происхождения при ее неповрежденном состоянии, а также после выдержки образцов биоткани в морозильной камере на интервалах времени от 15 мин до 2-х часов.

Проводится сопоставительный анализ полученных частотных зависимостей. Показано существенное отличие частотных зависимостей модуля напряжения на биоткани от частотной зависимости модуля напряжения на изотоническом растворе. Вводится понятие о том, что критерием оценки степени поражения биоткани может служить степень отличия частотного распределения модуля импеданса биоткани от модуля импеданса изотонического раствора.

Приводится вывод о целесообразности развития метода импедансометрии как метода диагностики жизнеспособности биоткани, показано, что наиболее перспективным подходом к развитию методов импедансометрии есть анализ переходных процессов при возмущении биоткани импульсами электрического тока малой величины.

Ключевые слова: импедансометрия; жизнеспособность; частотная характеристика; информативные признаки.

Ил. 3. Библиогр.: 15 назв.

UDC 615.472.03

Investigation of frequency characteristics of biological tissues impedance / *V.V. Semenetz, V.I. Leonidov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №203. P. 186 – 190.

The problem of identifying informative signs of biological tissues viability using the impedance measurement method is formulated. At present there is no instrumental base that makes it possible in an operational setting to diagnose the ability of biological tissue to heal itself after injury and damage as a result of thermal exposure, gunshot wound or prolonged compression. It is shown in this article that development of methods and tools for instrumental diagnostics in medical diagnostic practice is an important modern challenge.

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 modulus of voltage on biological tissues of plant origin are analyzed in its intact state, as well as after exposure of biological tissue samples in a freezer at time intervals from 15 minutes to 2 hours.

A comparative analysis of the obtained frequency dependences is carried out. A significant difference between the frequency dependences of the voltage modulus on biological tissues and the frequency dependence of the voltage modulus on an isotonic solution is shown. The concept is introduced that the degree of difference between the frequency distribution of the biological tissue impedance module from the impedance module of an isotonic solution can serve as a criterion for assessing the degree of damage to biological tissue.

A conclusion is made about the advisability of developing the impedance measurement method as a method for diagnosing the viability of biological tissue; it is shown that the most promising approach to the development of impedance measurement methods is the analysis of transient processes when biological tissue is disturbed by small electric current pulses.

Key words: impedance measurement; viability; frequency response; informative signs.

3 fig. Ref: 15 items.

ОБРОБКА СИГНАЛІВ
ОБРАБОТКА СИГНАЛОВ
SIGNAL PROCESSING

УДК 004.932

Порівняльний аналіз алгоритмів суміщення зображень: нормована кореляція проти суміщення на основі SIFT / *В.А. Душепа, Є.А. Тягнирядно, І.В. Баришев* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 203. С. 191 – 196.

Проведено порівняння алгоритмів суміщення зображень: класичної нормованої кореляції (як представника алгоритмів, заснованих на інтенсивностях пікселів) і алгоритму, заснованого на SIFT (суміщення на основі ознак). Для нормованої кореляції також використовувався градієнтний алгоритм субпіксельної корекції. Було проведено порівняння ефективності їх роботи на реальних зображеннях (в тому числі карті місцевості) при моделюванні штучних спотворень. Досліджувалася точність визначення положення (зміщення) одного зображення щодо іншого при наявності повороту і зміни масштабу. Експеримент був проведений за допомогою імітаційної моделі, створеної мовою програмування Python при використанні бібліотеки комп'ютерного зору OpenCV.

Результати експериментів показують, що при відсутності повороту і зміни масштабу між зображеннями, що суміщуються, нормована кореляція забезпечує дещо меншу середньоквадратичну помилку. При цьому за наявності навіть невеликих таких спотворень, наприклад, повороту більш ніж на два градуси і зміни масштабу більш ніж на два відсотки, вірогідність правильного суміщення для нормованої кореляції різко падає. Також було відзначено, що перевагами нормованої кореляції є майже в п’ять разів більша швидкодія і можливість її використання для невеликих фрагментів (50x50 і менше), де для алгоритму SIFT проблематично виділити достатню кількість ключових точок.

Також показано, що використання двоетапного алгоритму (суміщення на основі SIFT на першому етапі, і оптимізація з нормованою кореляцією у якості критерію на другому) дозволяє отримати одночасно і високу точність, і стійкість до повороту і зміни масштабу, ціною великих обчислювальних витрат.

Ключові слова: алгоритми суміщення зображень; нормована кореляція; SIFT; python; OpenCV.

Іл. 7. Бібліогр.: 15 назв.

УДК 004.932

Сравнительный анализ алгоритмов совмещения изображений: нормированная корреляция против совмещения на основе SIFT / *В.А. Душепа, Е.А. Тягнырядно, И.В. Барышев* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 203. С. 191 – 196.

Проведено сравнение алгоритмов совмещения изображений: классической нормированной корреляции (как представителя алгоритмов, основанных на интенсивностях пикселей) и алгоритма, основанного на SIFT (совмещение на основе признаков). Для нормированной корреляции также использовался градиентный алгоритм субпиксельной коррекции. Было проведено сравнение эффективности их работы на реальных изображениях (в том числе карте местности) при моделировании искусственных искажений. Исследовалась точность определения положения (смещения) одного изображения относительно другого при наличии поворота и изменения масштаба. Эксперимент был проведен с помощью имитационной модели, созданной на языке программирования Python при использовании библиотеки компьютерного зрения OpenCV.

Результаты экспериментов показывают, что при отсутствии поворота и изменения масштаба между совмещаемыми изображениями нормированная корреляция обеспечивает несколько меньшую среднеквадратическую ошибку. При этом при наличии даже небольших таких искажений, например поворота более чем на два градуса и изменения масштаба более чем на два процента, вероятность правильного совмещения для нормированной корреляции резко падает. Также было отмечено, что преимуществами нормированной корреляции является почти в пять раз большее быстродействие и возможность ее использования для небольших фрагментов (50x50 и менее), где для алгоритма SIFT проблематично выделить достаточное количество ключевых точек.

Также показано, что использование двухэтапного алгоритма (совмещение на основе SIFT на первом этапе, и оптимизация с нормированной корреляцией в качестве критерия на втором) позволяет получить одновременно и высокую точность, и устойчивость к повороту и изменению масштаба, ценой больших вычислительных затрат.

Ключевые слова: алгоритмы совмещения изображений; нормированная корреляция; SIFT; python; OpenCV.

Ил. 7. Библиогр.: 15 назв.

UDC 004.932

Comparative analysis of algorithms for images fusion: normalized correlation versus fusion based on SIFT / *V.A. Dushepa, Y.A. Tiahnyriadno, I.V. Baryshev* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №203. P. 191 – 196.

The paper compares the image registration algorithms: the classical normalized correlation (as a representative of intensity-based algorithms) and the SIFT-based algorithm (feature-based registration). A gradient subpixel correction algorithm was also used for normalized correlation. We compared the effectiveness of their work on real images (in-

cluding a terrain map) when modeling artificial distortions. The accuracy of determining the position (shift) of one image relative to another in the presence of rotation and scale changes was studied. The experiment was carried out using a simulation model created in the Python programming language using the OpenCV computer vision library.

The results of the experiments show that in the absence of rotation and scale changes between the registered images the normalized correlation provides a slightly smaller root-mean-square error. At the same time, if there are even small such distortions, for example, a rotation of more than 2 degrees and a scale change of more than 2 percent, the probability of correct registration for the normalized correlation drops sharply. It was also noted that the advantages of normalized correlation are almost 5 times higher speed and the possibility of using it for small fragments (50x50 or less), where it is problematic for the SIFT algorithm to allocate a sufficient number of keypoints.

It was also shown that the use of a two-stage algorithm (SIFT-based registration at the first stage, and optimization with normalized correlation as a criterion at the second) allows you to get both high accuracy and stability to rotation and scale change, but this will be accompanied by high computational costs.

Key words: image registration algorithms; normalized correlation; SIFT; python; OpenCV.

7 fig. Ref: 15 items.

УДК 004.89: 621.396

Семантичний аналіз флуктуацій радіолокаційної пачки для ідентифікації повітряних об'єктів / *В.В. Жирнов, С.В. Солонська* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 203. С. 197 – 203.

Розроблено та програмно реалізовано метод семантичного аналізу амплітудних флуктуацій радіолокаційної пачки для ідентифікації повітряних об'єктів в оглядових РЛС. Метод заснований на визначенні семантичних складових на етапі формування й аналізу символьної моделі пачки імпульсних сигналів від рухомих повітряних об'єктів. Сигнальна інформація описується предикатною функцією процесних знань формування та аналізу символьної моделі пачки імпульсних сигналів від рухомих повітряних об'єктів типу літак, вертоліт, БПЛА, та від атмосферних неоднорідностей типу «ангел-луна». В результаті семантичного аналізу амплітудних флуктуацій пачки в тимчасовій області отримані класифікаційні відмітні ознаки флуктуацій пачки від віддзеркалень, що заважають, і повітряних об'єктів. Досліджено семантичні складові алгоритму прийняття рішень, які подібні алгоритмам прийняття рішень оператором. У розробленому алгоритмі сигнальна інформація описується предикатною функцією на множині амплітуд імпульсів пачки, які перевищили певне порогове значення. Ідентифікація типів флуктуацій проводиться шляхом вирішення розроблених рівнянь предикатних операцій. На підставі отриманих рівнянь синтезована функціональна схема автоматичного визначення типів флуктуацій. Верифікація розробленого методу проведена на реальних даних, отриманих на оглядовій РЛС сантиметрового діапазону (тривалість імпульсу 1 мкс, частота зондування 365 Гц, період огляду 10 с). На основі цих даних змодельовані типи характерних пачок радіолокаційних сигналів. За результатами експериментів все вони були правильно ідентифіковані.

Ключові слова: семантичний аналіз; радіолокаційний сигнал; ідентифікація; заважаючи відбиття; повітряний об'єкт.

Іл. 3. Бібліогр.: 12 назв.

УДК 004.89: 621.396

Семантический анализ флуктуаций радиолокационной пачки для идентификации воздушных объектов / *В.В. Жирнов, С.В. Солонская* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 203. С. 197 – 203.

Разработан и программно реализован метод семантического анализа амплитудных флуктуаций радиолокационной пачки для идентификации воздушных объектов в обзорных РЛС. Метод основан на определении семантических составляющих на этапе формирования и анализа символьной модели пачки импульсных сигналов от подвижных воздушных объектов. Сигнальная информация описывается предикатной функцией процессных знаний формирования и анализа символьной модели пачки импульсных сигналов от подвижных летательных аппаратов типа самолет, вертолет, БПЛА, и от атмосферных неоднородностей типа «ангел-эхо. В результате семантического анализа амплитудных флуктуаций пачки во временной области получены классификационные отличительные признаки флуктуаций пачки от мешающих отражений и воздушных объектов. Исследованы семантические составляющие алгоритма принятия решений, которые подобны алгоритмам принятия решений оператором. В разработанном алгоритме сигнальная информация описывается предикатной функцией на множестве амплитуд импульсов пачки, превысивших некоторое пороговое значение. Идентификация типов флуктуаций проводится путем решения разработанных уравнений предикатных операций. На основании полученных уравнений синтезирована функциональная схема автоматического определения типов флуктуаций. Верификация разработанного метода проведена на реальных данных, полученных на обзорной РЛС сантиметрового диапазона (длительность импульса 1 мкс, частота зондирования 365 Гц, период обзора 10 с). На основе этих данных смоделированы типы характерных пачек радиолокационных сигналов. По результатам экспериментов все они были правильно идентифицированы.

Ключевые слова: семантический анализ; радиолокационный сигнал; идентификация; мешающие отражения; воздушный объект.

Ил. 3. Библиогр.: 12 назв.

UDC 004.89: 621.396

Semantic analysis of fluctuations of a radar pack for identification of air objects / *V. Zhyrnov, S. Solonskaya* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №203. P. 197 – 203.

A method for semantic analysis of amplitude fluctuations of the radar pack to identify air objects in surveillance radars has been developed and implemented in software. This method is based on the determination of semantic components at the stage of formation and analysis of the symbolic model of a burst of impulse signals from mobile aircraft. Signal information is described by the predicate function of the process knowledge of the formation and analysis of the symbolic model of a burst of impulse signals from mobile aircraft such as an airplane, helicopter, UAV, and from atmospheric inhomogeneities of the angel-echo type. As a result of semantic analysis of the amplitude fluctuations, classification distinguishing attributes of fluctuations from interfering reflections and air objects are obtained. The semantic components of the decision-making algorithm, which are similar to decision-making algorithms by the operator, are investigated. In the developed algorithm, the signal information is described by a predicate function on the set of amplitudes of burst pulses exceeding a certain threshold value. Identification of the types of fluctuations is carried out by solving the developed equations of predicate operations. Based on these equations, a functional diagram of automatic determination of the fluctuation types is synthesized. The verification of the developed method was carried out on real data obtained on a survey centimeter-band radar (pulse duration 1 μs, sounding frequency 365 Hz, survey period 10 s). Based on these data, types of characteristic packs of radar signals are simulated. According to the results of the experiments, they were all correctly identified.

Key words: semantic analysis; radar signal; identification; interfering reflections; air object.

3 fig. Ref: 12 items.

СПИСОК РЕЦЕНЗЕНТІВ У 2020 р.
СПИСОК РЕЦЕНЗЕНТОВ В 2020 г.
LIST OF REVIEWERS IN 2020

Dr. Sc. (Technology) Professor	Alexander Zamula	V. N. Karazin Kharkiv National University (Kharkiv, Ukraine)
Dr. Sc. (Physics and Mathematics) Professor	Anatoliy Luchaninov	Kharkiv National University of Radio Electronics (Kharkiv, Ukraine)
Cand. Sc. (Physics and Mathematics) Professor	Anton Drozdov	National Technical University “Kharkiv Polytechnic Institute” (Kharkiv, Ukraine)
Dr. Sc. (Technology) Professor	Dmytro Ageiev	Kharkiv National University of Radio Electronics (Kharkiv, Ukraine)
Dr. Sc. (Technology) Professor	Hennadii Khalimov	Kharkiv National University of Radio Electronics (Kharkiv, Ukraine)
Dr. Sc. (Physics and Mathematics) Professor	Igor Bondarenko	Kharkiv National University of Radio Electronics (Kharkiv, Ukraine)
Dr. Sc. (Physics and Mathematics)	Igor Mytsenko	O. Ya. Usikov Institute for Radiophysics and Electronics (Kharkiv, Ukraine)
Dr. Sc. (Technology) Professor	Igor Zakharov	Kharkiv National University of Radio Electronics (Kharkiv, Ukraine)
Dr. Sc. (Technology) Professor	Ivan Antipov	Kharkiv National University of Radio Electronics (Kharkiv, Ukraine)
Dr. Sc. (Technology) Professor	Ivan Gorbenko	V. N. Karazin Kharkiv National University (Kharkiv, Ukraine)
Cand. Sc. (Physics and Mathematics) Professor	Natalia Konovalova	Institute of Astrophysics of the Academy of Sciences of the Republic of Tajikistan
Dr. Sc. (Technology) Professor	Oleksandr Kuznetsov	V. N. Karazin Kharkiv National University (Kharkiv, Ukraina)
Dr. Sc. (Technology) Professor	Oleksandr Miroshnyk	Kharkiv National Technical University of Agriculture. Vasilenko (KhNTUSG) (Kharkiv, Ukraine)
Dr. Sc. (Technology) Professor	Oleksandr Potii	JSC "Institute of Information Technologies"
Dr. Sc. (Technology) Professor	Oleksandr Tsopa	Kharkiv National University of Radio Electronics (Kharkiv, Ukraine)
Dr. Sc. (Physics and Mathematics) Professor	Olexander Gritsunov	Kharkiv National University of Radio Electronics (Kharkiv, Ukraine)
Dr. Sc. (Physics and Mathematics) Professor	Petro Nikolyuk	Vasyl’ Stus Donetsk National University (Vinnytsia, Ukraine)
Dr. Sc. (Technology) Professor	Sergey Gerasimov	Ivan Kozhedub Kharkiv National University of the Air Force (Kharkiv, Ukraine)
Cand. Sc. (Technology) Professor	Sergey Gubin	National Aerospace University H.E. Zhukovsky "Kharkiv Aviation Institute" (Kharkiv, Ukraina)
Dr. Sc. (Technology) Professor	Sergey Lapta	H.S. Skovoroda Kharkiv National Pedagogical University
Corresponding Member of the National Academy of Sciences of Ukraine Dr. Sc. (Physics and Mathematics) Professor	Sergey Tarapov	O. Ya. Usikov Institute for Radiophysics and Electronics (Kharkiv, Ukraine)
Cand. Sc. (Technology) Professor	Serguyi Kulish	National Aerospace University H.E. Zhukovsky "Kharkiv Aviation Institute" (Kharkiv, Ukraine)
Cand. Sc. (Physics and Mathematics) Professor	Svetlana Kolomiets	Kharkiv National University of Radio Electronics (Kharkiv, Ukraine)
Dr. Sc. (Physics and Mathematics) Professor	Valeriy Bezruk	Kharkiv National University of Radio Electronics (Kharkiv, Ukraine)

Dr. Sc. (Technology) Professor	Valeryi Volosyuk	National Aerospace University H.E. Zhukovsky "Kharkiv Aviation Institute" (Kharkiv, Ukraine)
Dr. Sc. (Physics and Mathematics) Professor	Vladislav Lutsenko	O. Ya. Usikov Institute for Radiophysics and Electronics (Kharkiv, Ukraine)
Dr. Sc. (Technology) Professor	Volodymyr Doroshenko	Kharkiv National University of Radio Electronics (Kharkiv, Ukraine)
Dr. Sc. (Technology) Professor	Volodymyr Kartashov	Kharkiv National University of Radio Electronics (Kharkiv, Ukraine)
Dr. Sc. (Technology) Professor	Volodymyr Lukin	National Aerospace University H.E. Zhukovsky "Kharkiv Aviation Institute" (Kharkiv, Ukraine)
Dr. Sc. (Physics and Mathematics) Professor	Vyacheslav Tykhonov	Kharkiv National University of Radio Electronics (Kharkiv, Ukraine)
Cand. Sc. (Technology) Professor	Yuryi Gavryliyk	Kremenchuk Flight College of National Aviation University (KFC NAU)
Dr. Sc. (Physics and Mathematics) Professor	Yuryi Logvinov	O. Ya. Usikov Institute for Radiophysics and Electronics (Kharkiv, Ukraine)

ЗБІРНИК НАУКОВИХ ПРАЦЬ
РАДІОТЕХНІКА
Випуск 203
Українською, російською, та англійською мовами

СБОРНИК НАУЧНЫХ ТРУДОВ
РАДИОТЕХНИКА
Выпуск 203
На украинском, русском и английском языках

COLLECTION OF SCIENTIFIC PAPERS
RADIOTEKHNIKA
Issue 203
In Ukrainian, Russian and English

Коректор Л.І. Сащенко

Підп. до друку 30.12.2020. Формат 60x90/8. Папір офсет. Гарнітура Таймс. Друк. ризограф.
Ум. друк. арк. 11,3. Обл.-вид. арк. 10,8. Тираж 300 прим. Зам. № 353. 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.