MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE

KHARKIV NATIONAL
UNIVERSITY OF RADIO ELECTRONICS

RADIOTEKHNIKA

All-Ukrainian
interdepartmental scientific and technical collection

ISSN 0485-8972
eISSN 2786-5525

Founded in 1965

I S S U E 2 0 8

Kharkiv
Kharkiv National
University of Radio Electronics
2022

UDC 621.3

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

Website: rt.nure.ua

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

The authors are responsible for the content of the article.

Editorial Team

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

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

Recommended by the Scientific and Technical Council of Kharkiv National University of Radio Electronics, protocol № 2/2 dated 30.03.2022

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

Journal "Radiotekhnika" is included in the Catalog of subscription editions of Ukraine, subscription index **08391**.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ
УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ

РАДІОТЕХНІКА

Всеукраїнський
міжвідомчий науково-технічний збірник

ISSN 0485-8972
eISSN 2786-5525

Засновано в 1965 р.

В И П У С К 2 0 8

Харків
Харківський національний
університет радіоелектроніки
2022

УДК 621.3

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

Сайт: rt.nure.ua

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

Рекомендовано Науково-технічною радою Харківського національного університету радіоелектроніки, протокол № 2/2 від 30.03.2022 р.

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**.

CONTENT

SYSTEMS AND METHODS OF INFORMATION PROTECTION

RADIOLOCATION AND RADIONAVIGATION

TELECOMMUNICATIONS MEAS

PHYSICS OF DEVICES, ELEMENTS AND SYSTEMS

ЗМІСТ

СИСТЕМИ І МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ

РАДІОЛОКАЦІЯ І РАДІОНАВІГАЦІЯ

ЗАСОБИ ТЕЛЕКОМУНІКАЦІЙ

ФІЗИКА ПРИЛАДІВ, ЕЛЕМЕНТІВ І СИСТЕМ

УДК 004.056 **DOI:10.30837/rt.2022.1.208.01**

І.Д. ГОРБЕНКО, д-р техн. наук, О.А. ЗАМУЛА, д-р техн. наук

НАУКОВИЙ ПІДХІД ДО ЙМОВІРНІСНОЇ ОЦІНКИ ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ ВІД НАВ'ЯЗУВАННЯ ХИБНИХ ПОВІДОМЛЕНЬ У ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

Вступ

Функціонування цілої низки сучасних телекомунікаційних систем (ТКС), здійснюється в умовах зовнішніх і внутрішніх впливів, обумовлених, з одного боку, дією природних перешкод, перешкод від інших радіотехнічних систем, що функціонують на близьких частотах або в спільній ділянці діапазону частот, з іншого боку,- навмисних впливів, у тому числі, кібератак, створюваних зловмисником з метою руйнування, радіоелектронного подавлення діючих систем [1-2]. Об'єктивно існують загрози кібер - і інформаційної безпеки, а саме можливість: несанкціонованого доступу до інформаційних активів, порушення цілісності, конфіденційності, доступності даних, фальсифікація повідомлень з боку зловмисників тощо. Вищезазначене може призвести до суттєвого погіршення показників функціонування ТКС. Тому, до ТКС, особливо, таких, що функціонують на об’єктах критичної інфраструктури, пред'являються все більш жорсткі вимоги щодо забезпечення ефективності їх функціонування: достовірності і швидкості передачі інформації, живучості, завадозахищеності, кібер- і інформаційної безпеки. У таких умовах особливого значення набуває наявність і застосування захищених ТКС. У істотній мірі такі системи повинні базуватися на застосуванні захищених радіоканалів. Під захищеністю систем необхідно розуміти, в широкому сенсі, перш за все, їх здатність забезпечувати необхідні показники з завадозахищеності, імітостійкості, інформаційної, енергетичної і структурної скритності, швидкості передавання інформації, частотної і енергетичної ефективності. Завдання побудови захищеної ТКС – створити систему, стійку до впливу безлічі різноманітних, актуальних для даної системи, впливів, у тому числі кібератак. При цьому, об'єктивно існує суперечність між жорсткими вимогами щодо забезпечення достовірності, скритності, конфіденційності, цілісності, справжності даних, що зберігаються та передаються по провідних та бездротових лініях зв'язку ТКС, з одного боку, і існуючими моделями, методами та технологіями управління телекомунікаційними мережами, інформаційною безпекою, якістю обслуговування, з іншого боку [3-4].

Основними шляхами вирішення даної суперечності є підвищення завадозахищеності та кібер і інформаційної безпеки ТКС на основі удосконалення методологічних основ побудови ТКС шляхом отримання нових наукових підходів до оцінки реального стану захищеності ТКС, і створення моделей, методів та технологій захисту від існуючих кіберзагроз і загроз інформаційної безпеки.

Основні результати досліджень

Широке застосування хмарних обчислень, засобів віддаленого підключення з мобільних та віддалених стаціонарних пристроїв через мережі загального призначення призводять до «зникнення периметра» критичних систем та значного ускладнення забезпечення їхнього безпечного функціонування. Тому забезпечення безпеки телекомунікаційних систем стало одним із пріоритетних завдань у сучасному світі. В умовах внутрішніх та зовнішніх несанкціонованих дій порушників щодо ТКС фактично для будь-якого повідомлення, блоку даних або програмного коду необхідно реалізувати ряд послуг (функцій) безпеки.

До основних функцій (послуг) інформаційної безпеки слід віднести такі [5].

Конфіденційність інформації - властивість захищеності інформації (із наперед заданою якістю (ймовірністю)) від несанкціонованого доступу до неї та спроб розкриття (отримання змісту) неавторизованими користувачами та (або) процесами.

Цілісність інформації - властивість захищеності інформації, яке полягає в тому, що інформація практично не може бути змінена випадково чи навмисно неавторизованими суб'єктами (порушниками) або об'єктами (процесами), причому факт можливості порушення цілісності може бути визначений наперед заданою ймовірністю.

Справжність (автентичність) - властивість об'єктів/суб'єктів (зокрема інформації, ресурсів, повідомлень, даних, користувачів тощо.) забезпечити встановлення достовірності твердження у тому, що суб'єкт чи об'єкт має заявлені (очікувані) властивості.

Доступність - властивість ресурсу системи (інформації, послуги, об'єкта інформаційної та (або) телекомунікаційної системи), яке полягає в тому, що авторизований користувач та (або) процес, наділений відповідними повноваженнями, може використовувати ресурс відповідно до правил та певної якості.

Невідмовність – властивість, пов'язана із запобіганням можливості заперечення реальними суб'єктами (користувачами) та об'єктами (процесами) фактів повного чи часткового брати участь в інформаційному обміні чи інформаційній взаємодії. Як правило, включає формування, надання та передачу доказів реального участі в інформаційному обміні або інформаційній взаємодії.

Спостереженість - властивість ресурсу системи (комп'ютерної системи, об'єкта комп'ютерної системи тощо), що дозволяє реєструвати (фіксувати) дії користувачів та процесів, використання ресурсу системи, однозначно встановлювати ідентифікатори (імена) причетних до певних подій користувачів та процесів, а також реагувати на ці події з метою мінімізації можливих втрат у системі здійснюється, у тому числі, за рахунок використання криптографічних перетворень.

Зазначені послуги повною мірою можуть бути реалізовані за допомогою використання симетричних та асиметричних криптографічних перетворень та протоколів.

До основних механізмів забезпечення справжності, цілісності, автентичності повідомлень відносять алгоритми шифрування даних, електронні цифрові підписи, коди автентифікації повідомлень (MAC коди) та ін.

MAC код [5] - це функція відображення h: $K \times D \to R$, где $K = \{0,1\}^n$ – простір ключів, $D = \{0,1\}^*$ – простір повідомлень, а $R = \{0,1\}^n$ – простір MAC значень для k, $n \geq 1$. Для заданих значень ключа $k \in K$ і повідомлення $X \in D$, функція виробляє MAC значення $Y \in R$.

Наведемо визначення та сформулюємо пропозиції щодо забезпечення стійкості кодів автентифікації повідомлень до різних атак з боку станції протидії. Покажемо можливість застосування наведених результатів задля забезпечення істинності та цілісності повідомлень.

Розглянемо випадок, коли зловмисник може підробити повідомлення для MAC коду, якщо, не знаючи випадкового ключа, він здатний створити нове повідомлення X та MAC значення Y таке, що $h(K, X) = Y$.

Введемо визначення: MAC код $h: K \times M \to R$ є $(t; \varepsilon; q)$ секретним, якщо, при випадково взятому ключі K, зловмисник не може підробити нове повідомлення за час t з ймовірністю вище за ε, навіть якщо він (на свій вибір) має можливість отримати q значень MAC кодів інших повідомлень.

Залежно від інформації, доступної зловмиснику, розрізняють такі типи атак на коди автентифікації повідомлень [5].

1. Атака із відомим текстом. Зловмисник має можливість досліджувати деякі відкриті тексти та відповідні значення коду автентифікації повідомлень.

2. Атака із вибраним текстом. Порушник має можливість вибирати набори текстів та згодом отримувати значення кодів автентифікації повідомлень, що відповідають вибраним текстам.

3. Атака із адаптивним вибором тексту. Це найбільш загальна атака, коли зловмисник вибирає текст і негайно набуває відповідних значень коду автентифікації повідомлення.

4. Угадування коду автентифікації повідомлення (Guessing of the MAC). Це пряма атака на алгоритм MAC коду і полягає у виборі будь-якого нового повідомлення і, згодом, вгадування значення коду автентифікації повідомлення. Вона може бути виконана такими способами:

– вгадування ключа, з наступним обчислення значення MAC коду, з ймовірністю успіху 2^{-n}, n-позначає розмір (у бітах) значення MAC коду.

– вгадування ключа, з наступним обчислення значення MAC коду, з ймовірністю успіху 2^{-k}, k - довжина (в бітах) секретного ключа.

Цей тип атаки не піддається перевірці і, отже, порушник апріорі не знає, чи він вгадав значення MAC коду. Успіх атаки (досягнення очікуваного результату) залежить від кількості спроб здійснення атак.

Вичерпний пошук ключа (Exhaustive Key Search). Атака вимагає приблизно k/n відомих пар тексту MAC для фіксованого ключа. Намагаючись визначити ключ, крипто аналітик перебирає один за одним усі можливі ключі. Очікуване число випробувань, яке призведе до злому алгоритму MAC, дорівнює k/n . На відміну від попередньої атаки, цю атаку можна здійснювати поза сеансом зв'язку (off-line).

Підробка, заснована на внутрішній колізії (Internal Collision Based Forgery). Наслідок цієї атаки полягає в тому, що якщо виявити внутрішню колізію (збіг проміжних результатів при обчисленні значень MAC кодів), її можна використовувати для підробки MAC коду окремо вибраного тексту.

Виконаємо оцінку стійкості MAC кодів при імітації та заміні.

Аналіз показує, що з метою заміни повідомлень, порушник повинен сформувати повідомлення x' та відповідний повідомленню автентифікатор $y' = f(x')$. Це може бути виконано двома способами: шляхом імітації та шляхом підміни.

У разі імітації порушник формує автентифікатор $y = f(x)$ є дійсним [6]:

$$\mathrm{P_{им}} = \mathrm{P}\left(\mathrm{y} = \mathrm{f}\left(\mathrm{x}\right) - \text{истинно}\right), \left(\mathrm{x}, \mathrm{y}\right) \in \mathrm{A} \times \mathrm{B},\ \mathrm{f} \in \mathrm{H} \tag{1}$$

При рівно ймовірному виборі ключа, що еквівалентно вибору $f \in H$, необхідно враховувати розподіл MAC значень y конкретного повідомлення по ключовому простору. Для ймовірності імітації, позначимо її як ймовірність імітації за ключем $\mathrm{P_{имКл}}$, справедливо наступне вираз:

$$\mathrm{P_{имКл}} = \frac{\left|\left\{\mathrm{f} \in \mathrm{H} : \mathrm{y} = \mathrm{f}\left(\mathrm{x}\right)\right\}\right|}{\left|\mathrm{H}\right|}, (\mathrm{x}, \mathrm{y}) \in \mathrm{A} \times \mathrm{B}, \tag{2}$$

де $\left|\left\{f \in H : y = f(x)\right\}\right|$ - кількість хеш-функцій f, які породжують повідомлення x значення MAC коду y.

Очевидно, що

$$\mathrm{P_{имКл}} \geq \frac{1}{\left|\mathrm{H}\right|}. \tag{3}$$

Крім того, всі записи в стовпцях масиву МАС кодів зустрічаються однакову кількість разів і тому маємо: $P_{\text{имКл}} \geq \frac{1}{|B|}$.

Тому верхня межа ймовірності імітації МАС коду по ключу визначається максимальним значенням $P_{\text{имКл}} \geq \frac{1}{|B|}$ по всьому просторі повідомлень, а значення ймовірності $P_{\text{им}Кл}$ визначається наступним співвідношенням:

$$P_{\text{имКл}_{x\in A}} \leq \max \frac{\left|\left\{f \in H : y = f(x)\right\}\right|}{|H|}, (x, y) \in A \times B. \quad (4)$$

Якщо не зважати на розподіл МАС значень y для даного повідомлення по ключовому простору, тоді ймовірність імітації позначимо як ймовірність імітації за МАС значенням $P_{\text{имМАС}}$. Імітація за допомогою нав'язування МАС значення визначається тим, що з множини передбачуваних МАС кодів вибирається одне. Імовірність успіху визначатиметься виразом:

$$P_{\text{имМАС}} = \frac{1}{\left|\left\{y \in B : y = f(x)\right\}\right|}, (x, y) \in A \times B. f \in H, \quad (5)$$

де $\left|\{y \in B : y = f(x)\}\right|$ - потужність безлічі можливих МАС значень для повідомлення x.

Якщо МАС значення для повідомлення x набувають повної кількості значень $|B|$, отримаємо

$$P_{\text{имМАС}} = \frac{1}{|B|}. \quad (6)$$

У загальному випадку справедлива така нижня межа:

$$P_{\text{имМАС}} \geq \frac{1}{|B|}. \quad (7)$$

Якщо для повідомлення відомий статистичний розподіл МАС значень, оцінка ймовірності імітації за МАС значенням зводиться до оцінки ймовірності імітації за ключем. Верхня межа для ймовірності імітації за МАС значенням визначатиметься максимальним значенням по всьому просторі повідомлень:

$$P_{\text{имМАС}} \leq \max \frac{1}{\left|\left\{y \in B : y = f(x)\right\}\right|}, y \in B. f \in H \cdot \quad (8)$$

Атака підміни полягає в тому, що порушник спостерігає (x, y) і змінює його на (x', y'), де $x \neq x'$. Імовірність заміни визначатиметься умовною ймовірністю:

$$P_{\text{под}} = P(f(x') = y' - \text{истинно} \,|\, f(x) = y), \quad (x,y), (x',y') \in A \times B, x \neq x', f \in H \quad (9)$$

Вираз для ймовірності заміни з використанням формули повної ймовірності та статистики спостережень виглядатиме як:

$$P_{\text{под}} = \frac{\left|\left\{f \in H : y = f(x), y' = f(x')\right\}\right|}{\left|\left\{f \in H : y = f(x)\right\}\right|}, (x, y), \left(x', y'\right) \in A \times B, x \neq x', f \in H. \quad (9)$$

Верхня межа ймовірності нав'язування шляхом підміни повідомлень та МАС визначається максимальною ймовірністю успіху для всіх пар повідомлень, але за умови рівно ймовірного вибору ключа.

Аналіз показує, що можливі два випадки, коли заміна повідомлення x на x', якщо $x \neq x'$ здійснюється з тим самим автентифікатором $y = y'$, (заміна першого роду) і з різними $y \neq y'$ (підміна другого роду).

Імовірність заміни за умови рівності $y = y'$ визначається ймовірністю колізії МАС коду та оцінюється виразом:

$$P_{под1} \leq P_{кол} = \max \frac{\left|\left\{f \in H : y = f(x), y' = f(x')\right\}\right|}{\left|\left\{f \in H : y = f(x)\right\}\right|}, (x,y),(x',y') \in A \times B, x \neq x', f \in H. \quad (10)$$

Для ймовірності заміни другого роду маємо:

$$P_{под2} \leq \max \frac{\left|\left\{f \in H : y = f(x), y' = f(x')\right\}\right|}{\left|\left\{f \in H : y = f(x)\right\}\right|}, (x,y),(x',y') \in A \times B, x \neq x', y \neq y', f \in H. \quad (11)$$

Таким чином, для точного обчислення імітаційної та колізійної стійкості МАС кодів за наведеними формулами необхідно використовувати статистику спільних розподілів МАС кодів за ключами для дійсних та підроблених повідомлень. Для МАС кодів визначення такої статистики видається проблематичним через дуже великий розмір масиву можливих МАС. Нижні межі для ймовірностей імітації та підміни не враховують статистичні властивості масивів автентифікаторів, і ґрунтуються на моделі псевдовипадковості функції f(x) та визначають мінімальні вимоги до розміру ключового простору та простору МАС значень.

Верхні межі для ймовірностей імітації та підміни пов'язані з комбінаторними властивостями МАС масивів та оцінюють значення колізій у просторі А х В для найгіршого випадку вибору ключів та повідомлень.

Розглянемо колізійні властивості МАС кодів.

Під стійкістю до колізій розуміють обчислювальну складність знаходження двох повідомлень M_i і M_j таких, що [1]:

$$H(M_i) = H(M_j), \quad (12)$$

де Н є відповідним перетворенням.

У [6] наводяться оцінки ймовірності створення колізій, причому вважається, що для реалізації колізії необхідно виконати не менше $\sqrt{n}$ експериментів із загальної кількості можливих значень n.

Математична постановка завдання ймовірнісної оцінки колізій формулюється в такий спосіб.

Нехай є деяка функція перетворення Н повідомлення М

$$h = H(M), \quad (13)$$

де М - це повідомлення довільної довжини l_M, причому h може набувати значення $n = 2^m$ незалежно від довжини l_M. Необхідно визначити число випадкових повідомлень k, які необхідно подати на вхід перетворювача Н, щоб з ймовірністю $P_з$ відбувся хоча б один збіг виду (12), тобто колізія.

Оцінка кількості випробувань появи колізій

Проведений аналіз показав, що при розв'язанні даної задачі має місце вибірка з значень цілісної випадкової величини з рівноймовірним законом розподілу, що приймає значення від 1 до $n = 2^m$, а $k \le n$.

У таких умовах необхідно знайти ймовірність $P(n,k)$ того, що з значень H(M) вибірки, по крайній мірі, дві збігаються, тобто: $H(M_i) = H(M_j)$.

Для вирішення сформульованої задачі знайдемо ймовірність того, що в групі з подій не відбудеться колізія, тобто співвідношення (12) не виконається жодного разу. Позначимо цю можливість як $R(n,k)$. Зрозуміло, що $P(n,k)$ і $R(n,k)$ становлять повну групу подій, тобто: $P(n,k)+R(n,k)=1$, і

$$P(n,k)=1-R(n,k). \tag{14}$$

Далі знайдемо загальну кількість N різних способів, якими можна отримати значень без повторень. Для першого елемента маємо n значень без повторень, для другого n - 1, для третього – n - 2 тощо, для k - го – (n-k+1). Тому загальна кількість способів, за яких немає збігів може бути розраховано як:

$$N = n\cdot(n-1)(n-2)\ldots(n-k+1) = \frac{n!}{(n-k)!}. \tag{15}$$

Оскільки при кожній з подій з однаковою ймовірністю може відбуватися кожна з подій, то загальну кількість подій можна оцінити як

$$N_{\sum} = n^k. \tag{16}$$

Імовірність відсутності збігів можна оцінити ставленням числа варіантів без збігів (15) до загального числа варіантів (16), тобто

$$R(n,k) = \frac{\frac{n!}{(n-k)!}}{n^k} = \frac{n!}{(n-k)!n^k}. \tag{17}$$

Тоді, вираз для визначення $P(n,k)$ буде мати вигляд:

$$P(n,k)=1-\frac{n!}{(n-k)!n^k}. \tag{18}$$

Бажано отримати загальне рішення рівняння (18), наприклад, для значення k. З цією метою представимо $P(n,k)$ у вигляді:

$$P(n,k)=1-\frac{n(n-1)\ldots(n-k+1)}{n^k}=1-\left[\frac{n-1}{n}\,\frac{n-2}{n}\ldots\frac{n-k+1}{n}\right]=$$

$$=1-\left[\left(1-\frac{1}{n}\right)\left(1-\frac{2}{n}\right)\ldots\left(1-\frac{k-1}{n}\right)\right]. \tag{19}$$

Далі скористаємося тим, що всіх $1 > x \ge 0$ [2] справедливим є:

$$(1-x) \le e^{-x}.$$

З огляду на це, отримаємо:

$$\mathrm{P}\left(\bar{\mathrm{n}},\mathrm{k}\right)=1-\left(\mathrm{e}^{-\frac{1}{\mathrm{n}}}\mathrm{e}^{-\frac{2}{\mathrm{n}}}\ldots\mathrm{e}^{-\frac{\mathrm{k}-1}{\mathrm{n}}}\right)=1-\mathrm{e}^{-\left(\frac{1}{\mathrm{n}}+\frac{2}{\mathrm{n}}+\ldots+\frac{\mathrm{k}-1}{\mathrm{n}}\right)}=1-\mathrm{e}^{-\frac{\mathrm{k}(\mathrm{k}-1)}{2\mathrm{n}}}. \quad (20)$$

Позначимо $P(n,k)=P_з$, тобто значенням ймовірності, з якої має виникнути колізія. В результаті маємо:

$$P_з=1-e^{-k(k-1)/2n},$$

або

$$1-P_з=e^{-k(k-1)/2n}. \quad (21)$$

Виконавши логарифмування (21), отримаємо:

$$\ln(1-P_з)=-k(k-1)/2n. \quad (22)$$

Перетворюючи (22), маємо:

$$\frac{k(k-1)}{2n}=-\ln(1-P_з)$$

або

$$\mathrm{k}\left(\mathrm{k}-1\right)=-2\mathrm{n}\ln\left(1-\mathrm{P}_з\right).$$

У кінцевому вигляді отримуємо:

$$\mathrm{k}^2-\mathrm{k}+2\mathrm{n}\ln\left(1-\mathrm{P}_з\right)=0. \quad (23)$$

У останньому рівнянні пов'язані три величини: число подій k, загальна кількість подій n та ймовірність P(n, k), з якою має виникати колізія. Знаючи відповідне значення $\mathrm{P}_з$ і n, можна отримати точне рішення щодо знаходження k.

Нехай $\mathrm{P}_з=0{,}5$, тоді з використанням (23) отримаємо:

$$\mathrm{k}^2-\mathrm{k}+2\mathrm{n}\ln 0.5=\mathrm{k}^2-\mathrm{k}-2\mathrm{n}\ln 2=0. \quad (24)$$

Якщо $\mathrm{n}=2^{\mathrm{m}}$, то рівняння (24) матиме вигляд:

$$\mathrm{k}^2-\mathrm{k}-2^{m+1}\ln 2=0. \quad (25)$$

Дамо оцінку значення k. З урахуванням (23), отримаємо:

$$\mathrm{k}^2=-2\mathrm{n}\ln\left(1-\mathrm{P}_з\right) \quad (26)$$

При $\mathrm{P}_з=0{,}5$, маємо:

$$\mathrm{k}^2=-2\mathrm{n}\ln\left(1-0{,}5\right)=2\mathrm{n}\ln 2.$$

Тоді оцінка k матиме значення:

$$\mathrm{k}=\sqrt{2\mathrm{n}\ln 2}\approx 1{,}41\sqrt{\mathrm{n}}. \quad (27)$$

Для довільного значення з рівняння (26) отримаємо:

$$k = \sqrt{2\ln\left(\frac{1}{1-P_3}\right)\cdot n} = 1,41\sqrt{\ln\left(\frac{1}{1-P_3}\right)\cdot n}\,. \qquad (28)$$

Співвідношення (28) дозволяє оцінити кількість перетворень (експериментів), які необхідно здійснити для виникнення колізії з ймовірністю $P_з$. Порівнюючи отримані для k значення ((27) - (28)) з оцінкою, яка наводиться в [6]:

$$k = \sqrt{n}\,, \qquad (29)$$

можна оцінити ступінь близькості оцінки та можливість її застосування.

Розглянемо приклад оцінки стійкості МАС. Нехай в якості H використовується хеш-функція SHA-1, в якій $n = 2^{160}$, і нехай: $P'_з = 0,5$ и $P''_з = 0,99$. Скориставшись виразом (28), отримуємо:

$$k_{0.5} = 1,41\sqrt{n} = 1,41\sqrt{2^{160}} = 1,41\cdot 2^{80} \approx 1,7\cdot 10^{24};$$

$$k = 1,41\sqrt{\ln\left(\frac{1}{1-0.99}\right)\cdot 2^{160}} = 2^{80} \approx 3\cdot 10^{24}.$$

Висновки

Таким чином, у роботі визначені типи атак на коди автентифікації повідомлень, у залежності від інформації, доступної зловмиснику. Сформульовані наукові підходи, отримані вирази, які дозволяють виконати оцінку стійкості МАС кодів при імітації та заміні. Показано, що для точного обчислення імітаційної та колізійної стійкості МАС кодів необхідно використовувати статистику спільних розподілів МАС кодів за ключами для дійсних та підроблених повідомлень. Доведено, що нижні межі для ймовірностей імітації та підміни не враховують статистичні властивості масивів автентифікаторів, і ґрунтуються на моделі псевдовипадковості функції f(x) та визначають мінімальні вимоги до розміру ключового простору та простору МАС значень, а верхні межі для ймовірностей імітації та підміни пов'язані з комбінаторними властивостями МАС масивів та оцінюють значення колізій у просторі МАС значень і повідомлень для найгіршого випадку вибору ключів та повідомлень. Розглянуті колізійні властивості МАС кодів. Отримані рівняння, які дозволяють точно розв'язати задачу визначення кількості експериментів (подій) k, які необхідно виконати для створення колізії з ймовірністю $P_з$ на безлічі значень МАС коду. Із застосуванням отриманих рівнянь виконані оцінки стійкості МАС для одного з типів хеш-функцій. Наведені у роботі результати дозволяють отримати як залежність числа подій k від значень ймовірності, з якої може виникнути колізія, і загальної кількості подій n, так і залежність ймовірності виникнення колізії від k і n.

Список літератури:

1. Gorbenko, I., Zamula, A., Ho, T.L., Rodionov, S. Derived Signals Systems for Information Communication Systems Applications: Synthesis, Formation, Processing and Properties 2020 IEEE International Conference on Problems of Info communications Science and Technology, PIC S and T 2020 – Proceedings this link is disabled, 2021, стр. 13–18, 9468058.

2. Gorbenko, I., Zamula, O. Devising Methods to Synthesize Discrete Complex Signals with required Properties for Application in Modern Information and Communication Systems. Eastern-European Journal of Enterprise Technologies this link is disabled, 2021, 3, стр. 16–26.

3. Gorbenko, I.D., Zamula, A.A. Information security and noise immunity of telecommunication systems under conditions of various internal and external impacts Telecommunications and Radio Engineering (English translation of Elektrosvyaz and Radiotekhnika), 2017, 76(19), стр. 1705-1717.

4. Gorbenko, I., Kudryashov, I., Malieieva, H. Comparative Analysis of Candidates for a Post-Quantum CPU Based on MQ Cryptographic Transformation. 2018 International Scientific-Practical Conference on Problems of Info communications Science and Technology, PIC S and T 2018 - Proceedings, 2019, стр. 442–446, 8632070.

5. Горбенко, І.Д. Прикладна криптологія. Монографія / І.Д. Горбенко, Ю.І. Горбенко. – Харків: ХНУРЕ, 2012 р. - 868 с.

6. Горбенко Ю.І. Побудова, аналіз, стандартизація та застосування криптографічних систем. Під загальною редакцією професора Горбенка І.Д. Харків.: Видавництво «Форт», 2015. – 959 с.

Надійшла до редколегії 10.01.2022

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

УДК 621.391.15: 519.7 **DOI:10.30837/rt.2022.1.208.02**

A.V. BESSALOV

ON CORRECTNESS OF IMPLEMENTATION CONDITIONS CSIDH ALGORITHM ON EDWARDS CURVES

INTRODUCTION

The reason for writing this article was the work of Japanese scientists [1]. Our attention was drawn to the title of this paper, which includes the keywords CSIDH (Commutative Supersingular Isogeny Diffie-Hellman [2]) and Edwards curves [3, 4]. This topic intersects, in particular, with works [5, 6, 7] and our research [8 - 14].

The most interesting results in this topic, in our opinion, were obtained in [5], which offers the fastest today arithmetic for computing odd-degree isogenies on complete Edwards curves [3] using the Farasakhi-Hosseini -coordinates [6] and the theorems of [7].

Since the term "Edwards curves", first defined in [4] for all curves E_d with one parameter d, is ambiguous (does not take into account the values of the quadratic character $\chi(d)$), the question arises: what kind of Edwards curves are we talking about in [1]? The authors of [1] removed this question with the new term "*purely* Edwards curves", meaning by it *all curves* E_d *with one parameter, except the complete Edwards curves*. For them obviously $\chi(d)=1, d\neq 1$.

In our classification [11, 12], such curves are called “quadratic Edwards curves” (Section 1). Within this class of Edwards curves there are no quadratic twist pairs on which the CSIDH algorithm is based. Thus, we found a contradiction already in the title of [1], which proves its fallacy. The purpose of this article is a critical analysis of the incorrect statements and conditions of the theorems in [1], a refutation of its concept, and, as a constructive, a proof and illustration of the correct solution of the problem.

In [8], we proved two theorems adapting formulas of odd degree isogenies for Edwards curves [7] to twisted Edwards curves and to their computing in Farasakhi-Hosseini $(W:Z)$-coordinates [6]. In the next paper [9], using a simple model, it was shown how the CSIDH algorithm works on the basis of supersingular quadratic and twisted Edwards curves connected as quadratic twist pairs, some estimates of the calculation cost in projective $(W:Z)$ Farasakhi-Hosseini coordinates were detailed.

This article is, to a certain extent, a continuation of the previous work [9]. Supersingular quadratic and twisted Edwards curves with the same order $N_E = p+1 = 2^m n, m\geq 3,$ (n – odd) exist only for $p\equiv 7 \bmod 8$. The minimum even cofactor of the order of such curves is 8, then for the CSIDH algorithm with an odd $n=\prod_{i=1}^{K} l_i$ the field modulus, we should choose $p=8n-1.$ In order to adapt the definitions for the arithmetic of Edwards curves isogenies and curves in the Weierstrass form, we use the modified point addition law [11, 12] with the change of coordinates $x\leftrightarrow y$.

Section 1 gives a brief overview of the properties of complete, quadratic, and twisted supersingular Edwards curves (SEC) [13,14]. In Section 2, specific aspects of the implementation of the CSIDH algorithm model on quadratic and twisted SEC are considered, and a modification of the algorithm [2] is given. Since all the necessary calculations in the CSIDH algorithm are reduced only to field operations for calculating the isogenic curve parameter and scalar point multiplications, it is proposed to abandon the calculation of the isogenic function $\phi(R)$ of random point R. In section 3, we give critical analysis of theorems, lemmas and statements of article [1], their incorrectness and fallacy, substantiate the conclusion about the inconsistency of the concept and title of the article. The implementation of the CSIDH algorithm in [1] (section 6.2) relies on complete Edwards curves, which does not correspond to the problem posed in the paper. Instead of hypothetical curves $E_d[\pi-1]$ with one parameter in [1], one should actually use the known twisted SEC with two pa-

rameters and other existence conditions. The proof of Theorem 2 on quadratic twist of curves in the generalized Edwards form is given. In support of our conclusions, further in Section 4, an example of Alice and Bob's calculations in the Diffie-Hellman secret sharing scheme on quadratic and twisted SEC is given. Omitting the problem of computational cost, in this paper we mainly use affine coordinates.

1. PROPERTIES OF SUPERSINGULAR CURVES IN EDWARDS FORM

Let us consider some specific properties of supersingular Edwards curves (SEC) [13, 14]. An elliptic *curve in generalized Edwards form* [11] over a prime field F_p is defined by the equation

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

If a quadratic character $\chi(ad) = -1$, curve (1) is isomorphic to the *complete Edwards curve* [3, 4] with one parameter d

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

SEC of this class exist for $p \equiv 3 \bmod 4$, and their order is $N_E = p + 1 \equiv 0 \bmod 4$.
Let $\chi(ad) = 1, \chi(a) = \chi(d) = 1$, then the curve (1) is isomorphic to the *quadratic Edwards curve* [11]

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

In contrast to (2), the parameter d of curve (3) is a square. SEC of class (3) have an order $N_E = p + 1 \equiv 0 \bmod 8$ and exist over a field F_p for $p \equiv -1 \bmod 8$. For both curves (2) and (3) we accept a parameter $a = 1$, and they are called as curves with one parameter. In [4], curve (3) together with curve (2) are defined as *Edwards curves*. At the same time, the difference in the quadratic characters of the parameters d leads to radically different properties of curves (2) and (3) [11, 12]. We discuss this below and in Section 3.

The *twisted Edwards curve* was defined in [11] as a particular case of curve (1) for $\chi(ad) = 1, \chi(a) = \chi(d) = -1$.

The new classification of curves in the generalized Edwards form (1) in [11, 12] divides them into 3 non-intersecting (non-isomorphic) classes of complete, quadratic, and twisted Edwards curves. This avoids the ambiguity and difficulties that arise in the still existing terminology, which allows the inclusion of one class of Edwards curves in another. In the pioneering work [4], in particular, authors define the twisted Edwards curve with two parameters as curve (1). As a result any curve in Edwards form can be called twisted Edwards curve. However, already in [4] itself, statistics are given for the number of complete, twisted Edwards curves and Edwards curves, which cannot be sorted out. Another example of ambiguous terminology is the work [1], the title of which contains the term "Edwards curves", but according to [4], it includes "complete Edwards curves". The question arises: what kind of curves are we talking about?

The logic of classification of curves in the generalized Edwards form (1) in [11, 12] is simple. Since the introduction of a new parameter into the equation (1) in the Edwards form is necessary only in one case: at $\chi(ad) = 1, \chi(a) = \chi(d) = -1$, it is logical to keep the term “twisted Edwards curves” [11] for curves with this condition. In this case, the class "twisted Edwards curves" becomes unique up to isomorphism (it has no curves in other classes). Another such unique class is the class of “complete Edwards curves” [3, 4] with the condition $\chi(ad) = -1$. Finally, the third unique class with the condition $\chi(ad) = 1, \chi(a) = \chi(d) = 1$ is the class of "*quadratic* Edwards curves". This term, proposed by us [11], is justified by the property $\chi(d) = 1$, which is different from the conditions of the other two classes. To a certain extent, it can also be justified by the term “quadratic twist”, which is exactly what the curves of the corresponding classes (quadratic and

twisted curves) are connected. It is important that there are exactly three classes of curves (1), each with its own name, and no confusion.

In the application to the CSIDH algorithm on SEC, we define a pair of quadratic and twisted SEC [11] as a pair of quadratic twist with parameters $\chi(ad)=1, \vec{a}=ca, \vec{d}=cd, \chi(c)=-1.$ (see Theorem 2 in Section 3). Since SEC exist only for $p\equiv 3 \bmod 4$ [13], we can take $c=-1, a=1, \bar{a}=-1, \bar{d}=-d,$ where $a,d-$ are the parameters of a quadratic curve, and respectively, $\bar{a},\bar{d}-$ of a twisted curve. In other words, the transition from a quadratic to a twisted curve and vice versa we can define $E_d = E_{1,d} \leftrightarrow E_{-1,-d}$. Then the twisted SEC equation for $p\equiv 7 \bmod 8$ from (1) we can written as

$$E_{-1,-d}: \quad x^2-y^2=1-dx^2y^2, \quad d\in F_p^*, \quad d\neq 1., \chi(d)=1. \tag{4}$$

Here, the conditions for the modulus p and order of the curve $N_E = p+1\equiv 0 \bmod 8$ are similar to curves (3). For $p\equiv 7 \bmod 8$, of course, also $p\equiv 3 \bmod 4$ holds.

Having fixed the parameter $a=-1$ and running through all admissible values of d, we can determine the set of cardinalities of all $\frac{p-3}{2}$ curves of each of the 3 classes of curves (1) (including isomorphic curves). Any twisted SEC one can reduce to the form (4).

The order $N_E = p+1-t$ of an elliptic curve over a prime field F_p is determined based on the trace t of the characteristic equation $\pi^2+t\pi+p=0$ of the Frobenius endomorphism, where for some point $P=(x.y)$ the Frobenius endomorphism $\pi(P)=(x^p,y^p)$. For a quadratic twist curve, the corresponding order will be $N_E{}^t = p+1+t$. An elliptic curve is supersingular if and only if, over any extension of a prime field F_p, the trace of the Frobenius equation is $t\equiv 0 \bmod p,$ in this case $\pi^2=-p, \ \pi=\pm\sqrt{-p}$ in an imaginary quadratic field [13, 15]. A pair of curves E and E^t is sometimes referred to $E[\pi+1], E[\pi-1]$ as two solutions of the quadratic Frobenius equation. In an algebraic closure $\overline{F}_p$, a supersingular curve does not contain points of order p. Over a prime field F_p, such a curve always has order $N_E = p+1$.

So, quadratic and twisted SEC as a pair of quadratic twist have the same order $N_E = p+1$ but different structure. All their points are different (except two points $(0,\pm 1)$), so isogenies of the same degree have different kernels. Both curves are non-cyclic with respect to points of the 2-nd order (contain 3 points of the 2-nd order each, two of which are exceptional points $D_{1,2}=\left(\pm\sqrt{\frac{a}{d}},\infty\right)$ [4, 11]). Quadratic SEC (3), in addition, contains two exceptional points of the 4-th order $\pm F_1=\left(\infty,\pm\frac{1}{\sqrt{d}}\right)$. The presence of a noncyclic subgroup of the 4-th order containing 3 points of the 2-nd order limits the number 8 to the minimum even cofactor of the order $N_E = 8n \ (n-odd)$ of quadratic and twisted Edwards curves [11]. In general, their order is $N_E = 2^m n, m\geq 3$. The maximum order of points of these curves is $N_E/2 = 4n.$ It is important that points of even orders are not involved in the calculations of the CSIDH algorithm (after the first multiplication of a random point P of maximum order by 4, we have a point of odd order n).

For the curve (1) J -invariant equal [4, 15]

$$J(a,d)=\frac{16(a^2+d^2+14ad)^3}{ad(a-d)^4}, \quad ad(a-d)\neq 0. \tag{5}$$

This parameter distinguishes isogenic (with different J-invariants) and isomorphic (with equal J-invariants) curves. Since the J-invariant retains its value for all isomorphic curves and quadratic twist pairs [15], it is the same for a pair of twisted and quadratic SEC ($a = \pm 1$). It is a useful tool both in finding supersingular curves and in constructing isogeny chain graphs. One of the properties of the $J-$invariant is

$$J(d) = J(d^{-1}).$$

For the considered classes of SEC, the replacement $d \to d^{-1}$ gives an isomorphism, and for complete Edwards curves (2) it gives a quadratic twist.

2. MODIFICATION OF CSIDH ALGORITHM ON QUADRATIC AND TWISTED EDWARDS CURVES

The PQC CSIDH (Commutative SIDH) algorithm proposed by the authors of [2] for solving the same key exchange problem (SIDH), but based on isogenic mappings of supersingular elliptic curves as additive Abelian groups. Such a mapping over a prime field F_p as the class group action is defined [2] and is commutative. In comparison with the well-known original CRS scheme (Couveignes (1997), Rostovtsev, Stolbunov (2004)) on non-supersingular curves, the use of isogenies of supersingular curves made it possible to substantial speed up the algorithm and achieve the smallest known key size (512 bits in [2]).

Let the curve E of order $N_E = p+1$ contain points of small odd orders $l_i, i = 1,2,..., K.$ Then there is an isogenic curve E' of the same order as a l_i-degree map: $E \to E' = [l_i] * E$. The repetition of this operation e_i times we denote $[l_i^{e_i}] * E$. The values of the isogeny exponents $e_i \in Z$ determine the length $|e_i|$ of the chain of isogenies of degree l_i. In [2], an interval of exponential values $[-m \le e_i \le m]$ is accepted ($m = 5$), which provides a security level of 128 bits for a quantum computer attack. Negative values of the exponent mean a transition to a quadratic twist supersingular curve.

The implementation of the CSIDH algorithm mainly uses fast arithmetic of Montgomery elliptic curves $y^2 = x^3 + Cx^2 + x,\ C \ne \pm 2$ containing 2 points of the 4-th order and, accordingly, having an order $N_E = p+1 = 4n(n-odd).$ [2]. In [5], the CSIDH algorithm implemented on complete SEC of the same order. In this paper, we use quadratic and twisted SEC in the CSIDH algorithm, which have the same speed performance as complete Edwards curves [5]. In [8] we proved 2 theorems for implementation such possibility. With a minimum cofactor of 8, the order of twisted and quadratic SEC is $N_E = 8n$. Thus, for these SEC classes with order $N_E = 8n = p+1,\ n = \prod_{i=1}^{K} l_i.$ the field modulus in the CSIDH algorithm we chosen as $p = 8\prod_{i=1}^{K} l_i - 1 \equiv -1 \bmod 8$.

Non-interactive Diffie-Hellman key exchange includes the following steps [2]:

1. **Choice of parameters.** For small odd primes l_i, compute $n = \prod_{i=1}^{K} l_i$, where the value K is determined by the security level (in [2] $K = 74, l_{74} = 587$), and choose an appropriate field modulus $p = 2^m \prod_{i=1}^{K} l_i - 1, m \ge 3$ and a starting elliptic curve E_0 .

2. Calculation of public keys. Alice uses her private key $\Omega_A = (e_1, e_2, .., e_K)$ to build an isogenic mapping $\Theta_A = [l_1^{e_1}, l_2^{e_2}, .., l_K^{e_K}]$ (class group action [2]) and calculates the isogenic curve $E_A = \Theta_A * E_0$ as her public key. Based on the secret key Ω_B and function Θ_B, Bob performs the same calculations and receives his public key $E_B = \Theta_B * E_0$. These curves are defined their parameters d_A, d_B up to isomorphism, which are accepted as public keys known to both parties.

3. Sharing secrets. Here the protocol is similar to item 2 with replacements $E_0 \to E_B$ for Alice and $E_0 \to E_A$ for Bob. Knowing Bob's public key, Alice calculates $E_{BA} = \Theta_A * E_B = \Theta_A \Theta_B * E_0$. Similar actions of Bob give a result $E_{AB} = \Theta_B * E_A = \Theta_B \Theta_A * E_0$ that coincides with the first one due to the commutatively of the group operation. The J-invariant of the curve $E_{AB}(E_{BA})$ is accepted the shared secret.

Below we present a modification of Alice's computational algorithm according to item 2 [2] using isogenies of quadratic and twisted SEC.

Algorithm 1: Evaluating the class-group action on quadratic and twisted SEC.

Input: $d_A \in E_A, \chi(d) = 1$ *and a list of integers* $\Omega_A = (e_1, e_2, ...e_K)$.

Output: d_B *such that* $[l_1^{e_1}, l_2^{e_2}, ...l_K^{e_K}] * E_A = E_B$, *where* $E_{A,B}$: $x^2 + y^2 = 1 + d_{A,B} x^2 y^2$.

1. **While** *some* $e_i \neq 0$ **do**
   2. *Sample a random* $x \in F_p$,
   3. Set $a \leftarrow 1$, $E_A : x^2 + y^2 = 1 + d_A x^2 y^2$ **if** $(1 - x^2)/(1 - dx^2)$ *is a square in* F_p,
   4. **else** $a \leftarrow -1$, $E_A : x^2 - y^2 = 1 - d_A x^2 y^2$,
   5. *Let* $S = \{i \mid ae_i > 0\}$. **If** $S = \varnothing$ *then start over to line 2 while* $a \leftarrow -a$,
   6. *Let* $k = \prod_{i \in S} l_i$, *and compute* $R \leftarrow [(p+1)/2k]P$, $P = (x, y)$,
   7. **For** e*ach* $i \in S$ **do**
      8. *Compute* $Q \leftarrow [k / l_i]R$
      9. **If** $Q \neq (1,0)$ *Compute the parameter* d_B *an isogeny* $\phi : E_A \to E_B$ *with* $\ker \phi = Q$ ***Set*** $d_A \leftarrow d_B$, $e_i \leftarrow e_i - a$ **,**
      10. *Skip* i *in* S *and* $k \leftarrow k / l_i$ **if** $e_i = 0$,
11. **Return** d_A**.**

In comparison with Algorithm 2 in [2], our Algorithm 1, adapted to twisted and quadratic SEC, has some modifications:

1. Checking the square in item 3 use the equation of the quadratic Edwards curve (3).

2. With the order of the twisted Edwards curve $N_E = 8n = p + 1$ with the maximum order $N_E / 2 = 4n$ of the point, to obtain a point of the order n, it is sufficient to double the random point twice. In item 6, this property lied's to reducing one doubling in the scalar product of the point P.

3. Item 9 has been corrected (you cannot reset the index i before zeroing e_i in item 10).

4. In item 9, only the parameter d_B of the isogenic curve is calculated and the function $\phi(R)$ point R is not calculated.

5. Updating the number $k \leftarrow k / l_i$ and reset i in item10 we perform after zeroing e_i.

According to item 10, exactly $|e_i|$ isogenies we calculate for each l_i until the exponent e_i is set to zero. Depending on its sign, isogenies are calculated in the class of quadratic ($e_i > 0$) or twisted SEC ($e_i < 0$).

The ultimate goal of the CSIDH secret sharing algorithm is to find the common curve parameter d_{AB} of curve E_{AB}. For each step in the chain of isogenies $E \to E'$, it is only necessary to calculate the parameter $d' = \psi(d, Q)$ based on the parameters d and the kernel $< Q >$ of the curve E. This calculation involves two SM (Scalar Multiplication) of random points R and $(s-1)$ recurrent dou-

blings of points of kernel $< Q >$. Thus, the construction and calculation of a sufficiently complex function $\phi(R)$ is not necessary for the implementation of the CSIDH algorithm. Part of the calculations in the algorithm related to the calculation of the function $\phi(R)$ can be saved and significantly speed up the algorithm.

The construction of isogenies of odd prime degrees for quadratic Edwards curves based on Theorem 2 [7], and for twisted Edwards curves - Theorem 1 [8]. In the last work, for the first time, mapping $\phi(P)$ formulas for the curve (1) are given, depending on two parameters a and d . We formulate it below.

Theorem 1[1]. Let $G = \{(1,0), \pm Q_1, \pm Q_2, ..., \pm Q_s\}$ – subgroup of odd order $l = 2s+1$ of points $\pm Q_i = (\alpha_i, \pm\beta_i)$, of curve $E_{a,d}$ (1) over field F_p .
Define

$$\phi(P) = (x', y') = \left(\prod_{Q \in G} \frac{x_{P+Q}}{x_Q} \frac{x_{P-Q}}{x_{Q,}}, \prod_{Q \in G} \frac{y_{P+Q}}{x_Q} \frac{y_{P-Q}}{x_{-Q,}} \right).$$

Then $\phi(x, y)$ is l -isogeny with kernel G from the curve $E_{a,d}$ to the curve $E_{a',d''}$ with parameters

$$a' = a^l, \quad d' = d^l A^8, \quad A = \prod_{i=1}^{s} \alpha_i, \tag{6}$$

and the mapping function

$$\phi(x, y) = \left(\frac{x}{A^2} \prod_{ii=1}^{s} \frac{(\alpha_i x)^2 - (a\beta_i y)^2}{1 - (d\alpha_i \beta_i xy)^2}, \frac{y}{A^2} \prod_{i=1}^{s} \frac{(\alpha_i y)^2 - (\beta_i x)^2}{1 - (d\alpha_i \beta_i xy)^2} \right), \tag{7}$$

or

$$\phi(x, y) = \left(\frac{x}{A^2} \prod_{ii=1}^{s} \frac{x^2 - a\beta_i^{\,2}}{1 - d\beta_i^{\,2} x^2}, \frac{-y}{A^2} \prod_{i=1}^{s} \frac{x^2 - \alpha_i^{\,2}}{a - d\alpha_i^{\,2} x^2} \right). \tag{8}$$

The proof of theorem in [8] is given.

Here, functions (7) and (8) include parameters a, d , which makes it possible to construct isogenies of twisted Edwards curves.

3. CRITICAL ANALYSIS OF INCORRECT IMPLEMENTATION CONDITIONS OF CSIDH ALGORITHM ON EDWARDS CURVES IN WORK [1]

Let us turn to the results of [1]. The main concept of this article is the construction of the CSIDH algorithm using one class - Edwards curves E_d (3) (the authors call it "*purely* Edwards curve", according to our classification [11] - "quadratic Edwards curve") over a prime field F_p . Since the CSIDH algorithm is based on isogenies of supersingular curves using the quadratic twist of these curves, the question arises: is the problem posed in [1] solvable?

All theorems of this work use one Farashakhi-Hoseini coordinate $w(P) = dx_1^{\,2} y_1^{\,2}$ for each point $P = (x_1, y_1)$. It is clear that the quadratic character $\chi(w(P)) = \chi(d)$. The neutral element $O = (1,0)$ of curve (3) in theorems [1] designated as 0_d , although for all curves (1) it does not depend on the parameter d .

The key theorem in [1] is Theorem 4. Let us formulate it according to the original.

Theorem 4[1]. *Let* $p \equiv 3 \bmod 8$. *Let* P *be a point on an Edwards curve* E_d *such that the* P *w-coordinate* $w(P) \in F_p$, *the order of* P *is not a power of* 2, *and* $w(P)$ *is square. If* $w(2P)$ *is square, there exists* P' *such that* $P' \in E_d[\pi_p + 1]$, $w(2P) = w(P')$, *and* $\frac{p+1}{4} P' = 0_d$. *If* $w(2P)$ *is not square, there exists* P' *such that* $P' \in E_d[\pi_p - 1]$, $1/w(2P) = w(P')$ *and* $\frac{p+1}{4} P' = 0_d$.

Formulation of the theorem. The first error in the formulation of the theorem: for $p \equiv 3 \bmod 8$ there are no curves E_d (3) that satisfied all conditions of the theorem. Indeed, in this case the order of the curve $N_E = p + 1 \equiv 4 \bmod 8$ is not divisible by 8. They exist only for $p \equiv 7 \bmod 8$ [13, 14]. The order of such curves with the minimum even cofactor 8 is $N_E = 8n = p + 1$, where $p \equiv -1 \bmod 8$. For example, $p = 11 \equiv 3 \bmod 8$ it sets a condition for the SEC of order $N_E = 12$, which does not contain the factor 8. It is clear that it is impossible to prove such a theorem.

On the proof of theorems [1]. In total, in Section 4 of [1], 10 lemmas and 7 theorems are proved. The condition $p \equiv 3 \bmod 8$ is specified in Lemmas 1,2,4, 5, 9, 10 and Theorems 3, 4, 5 and 7 with references to the lemmas and to the points of the curve (3), which does not exist under this condition, as well as its quadratic twist - twisted SEC (4). The proof of theorems and lemmas with incorrect conditions in the formulation does not make sense.

Further, the conditions of Theorem 4 define only one curve E_d (3) with the parameter d being a square ($\chi(d) = 1, d \neq 1$). For a random point $P = (x_1, y_1)$ and a point $2P$ on this curve, their respective w-coordinates are

$$w(P) = d x_1^{\,2} y_1^{\,2}, \quad w(2P) = d \left(\frac{x_1^{\,2} - y_1^{\,2}}{1 - d x_1^{\,2} y_1^{\,2}} \right)^2 \left(\frac{2 x_1 y_1}{1 + d x_1^{\,2} y_1^{\,2}} \right)^2 .$$

It follows that for $x_1 y_1 \neq 0, \infty$, the quadratic character $\chi(w(P)) = \chi(w(2P)) = \chi(d)$ is determined exclusively by the parameter d and, by the definition of curve E_d (3), is a square. This property is the same for both points P and $2P$, which contradicts the second assumption of the theorem. While the first assumption of the theorem is always true, the second assumption is always false for a given curve E_d (3), since it replaces $\chi(d) = 1$ with $\chi(d) = -1$. This means a transition to another class of SEC: complete Edwards curve (2) or twisted Edwards curve (4).

The transition to the class of complete SEC (2) with $\chi(d) = -1$ we exclude, since:

- The class (2) does not meet the first condition of Theorem 4 ($\chi(d) = 1$);
- All pairs of quadratic twist connected by parameters $d^{\pm 1}$ lie inside this class;
- Sets parameters d of SEC (2) and (3) are different (in the sense of $d_i^{(2)} \neq -d_k^{(3)}$);
- The class (2) does not contain points at infinity on which the proof of the theorem based.

Exceptional points (points at infinity) exist only in the classes of quadratic SEC (which are excluded by the second assumption of Theorem 4) and twisted SEC [4, 11]. Thus, instead of the curve $E_d[\pi_p - 1]$ in the statement of Theorem 4, there should be a twisted curve $E_{a,d}[\pi_p - 1]$ with conditions $\chi(a) = \chi(d) = -1$. It is important that this is no longer a curve E_d, but its quadratic twist $\chi(d) = 1$. Below we present our Theorem 2 with the proof of this assertion.

On SEC E_d (3) with order $N_E = 8n = p + 1$, $n = \prod_{i=1}^{K} l_i$ there is a unique subgroup $< Q >= G$ of points of prime order l_i as the kernel of a unique isogeny $[l_i]$. Over a prime field F_p,

there is a unique SEC of the same order, defined as a quadratic twist $E_d{}^t$ of the curve (3), which has its own subgroup $< Q >^t$ of points of the order l_i as isogeny kernels $[l_i]^{-1}$. All points (except points $O = (1,0), D_0 = (-1,0)$) the pair of curves E_d and $E_d{}^t$ are distinct, as are the corresponding kernels $< Q >$ and $< Q >^t$ l-isogenies. According to Theorem 2 $E_d{}^t = E_{a,ad}$, $\chi(a) = -1$. This is a twisted SEC, but not the Edwards curve, stated in the problem statement and in the title of the article [1].

Exceptional points at infinity of the 2-nd and 4-th orders of the curve (1) we can written [11, 12]

$$D_{1,2} = \left(\pm \sqrt{\frac{a}{d}}, \infty \right), \quad \pm F_1 = \left(\infty, \frac{\pm 1}{\sqrt{d}} \right), \tag{9}$$

where the symbol "∞" we put when dividing by 0. Over a prime field F_p, all 4 points contain quadratic curves E_d (3), and the first 2 points of the 2-nd order are twisted curves (1) under the conditions $\chi(a) = \chi(d) = -1$. The latter generate a non-cyclic subgroup of points of the 2-nd order $G_4 = \{O = (1,0), D_0 = (-1,0), D_1, D_2\}$. According [11] the sums of a random point $P = (x_1, y_1) \notin G_4$ with exceptional points of the 2-nd order give the points

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

From here

$$w(P + D_{1,2}) = \frac{1}{dx_1^2 y_1^2} = \frac{1}{w(P)}. \tag{10}$$

For a similar sum with ordinary point of the 2-nd order $D_0 = (-1,0)$ we have

$$(x_1, y_1) + (-1,0) = (-x_1, -y_1) \quad \Rightarrow \quad w(P + D_0) = w(P) \tag{11}$$

The sum of a random point $P = (x_1, y_1) \notin G_4$ with a 2-nd order point gives an even-order point, which on the curve order $N_E = 8n$ is at least 8 times greater than the number of odd-order points. Of these, for (2/3) points, the coordinate $w(P)$ is inverted according to (10), for the rest, according to (11), no. This is true for two classes - quadratic and twisted Edwards curves. However, this is not a reason to replace one curve with another [1], not forgetting that the quadratic characters $\chi(d)$ of their parameters are inverse. It also follows from this that the second assertion of Theorem 4 is valid only for twisted Edwards curves, but not for curves E_d (3) with one parameter. It is no less important that the condition $\chi(d) = -1$ of this assertion is necessary but not sufficient. A condition $\chi(a) = -1$ and the connection between the parameters of the curves $E_{a,d}$ and $E^t{}_{a,d}$ should be determined (see our Theorem 2).

Theorem 2. For the curve $E_{a,d}$ (1) in the generalized Edwards form $x^2 + ay^2 = 1 + dx^2 y^2$, defined over a prime field, there is a unique quadratic twist curve $E_{\bar{a},\bar{d}}{}^t$ with parameters $\bar{a} = ca$, $\bar{d} = cd$, $c \in F_p{}^*$.

Proof. From equation (1) we have

$$y^2 = \frac{1-x^2}{a-dx^2}. \qquad (12)$$

Let $\chi(d) = -1,\ \chi(a) = 1,\ a = d^2 = c^{-1}$. Quadratic twist (12) be given by transforming a square into a quadratic non-residue

$$dy^2 = \frac{1-x^2}{d^2-dx^2}\cdot d = \frac{1-x^2}{1-d^{-1}x^2}\cdot d^{-1} \quad \Rightarrow \quad \chi\left(\frac{1-x^2}{1-d^{-1}x^2}\right) = 1.$$

Then for the curve of quadratic twist we can write the equation

$$E_{\bar{a},\bar{d}}{}^t = E_{d^{-1}}: \quad x^2 + y^2 = 1 + d^{-1}x^2y^2, \quad \chi(d) = -1.$$

The above conditions are valid for the class of complete Edwards curves with one parameter for $a = d^2 = c^{-1},\ \bar{a} = 1,\ \bar{d} = d^{-1}$. This result [3] is known.

Let now $\chi(a) = \chi(d) = 1$, $\chi(c) = -1$. In this case, quadratic twist (12) we can written as

$$c^{-1}y^2 = \frac{1-x^2}{a-dx^2} \Rightarrow \quad y^2 = \frac{1-x^2}{ca-cdx^2} = \frac{1-x^2}{\bar{a}-\bar{d}x^2}.$$

This implies that the quadratic twist of a curve $E_{a,d}$ with parameters satisfying the condition $\chi(a) = \chi(d) = 1$ (a quadratic curve isomorphic to (3)) gives a curve of the class of twisted Edwards curves (1) after substituting $\bar{a} = ca,\ \bar{d} = cd.\ \chi(c) = -1$. In other words, the quadratic twist of a curve E_d is a twisted Edwards curve $E_d^t = E_{c,cd},\ \chi(d) = 1,\ \chi(c) = -1.$. The inverse mapping is given by multiplying both parameters by $c^{-1}: E_{c,cd},{}^t = E_d \quad \chi(d) = 1,\ \chi(c) = -1.$ The theorem is proved.

Corollary 1. For quadratic Edwards curves E_d ($\chi(d) = 1$) there are no quadratic twist curves within this class.

Corollary 2. For complete Edwards curves E_d ($\chi(d) = -1$) there exist quadratic twist curves $E_{d^{-1}}$ inside this class.

Corollary 1 is obvious from the uniqueness of the mapping of quadratic twist as a bijection. It eliminates the curves $E_d\ [\pi - 1]$ in [1].

Note that this result is well known from [4] (hence the term twisted Edwards curves), but with a different proof from our proof of Theorem 2.

So, in the class of complete Edwards curves E_d (2), the quadratic twist pairs $E_d \leftrightarrow E^t{}_{d^{-1}}$ lies inside this class and has multiplicatively inverse parameters $d^{\pm 1}$. On the contrary, for the class of quadratic Edwards curves (3), for $p \equiv 3 \bmod 4$ and $c = -1$, quadratic twist $E_d{}^t \to E_{-1,-d}$ gives a curve from the class of twisted Edwards curves with additively opposite parameters a and d .

We consider it proved that for the class of SEC $E_d[\pi_p + 1]$ defined in Theorem 4 [1], there are no curves of the same class $E_d[\pi_p - 1]$ as quadratic twist pairs, the formulation of Theorem 4 is incorrect, and the concept of [1] is untenable. Strictly speaking, a unique transition of curve E_d (3) with the condition $\chi(d) = 1$ to its quadratic twist is possible only in the class of twisted SEC with parameters $\bar{a} = ca,\ \bar{d} = cd,\ \chi(c) = -1$. Any SEC of this class is isomorphic to curve (4).

Interestingly, the implementation of the CSIDH algorithm in [1] (Section 6.2) uses the parameters of [2] for cyclic curves in the Montgomery form with one point of the 2-nd order and the field modulus $p = 4 \cdot l_{1i} \cdot l_2 \cdot \ldots \cdot l_{74} - 1,\ l_{74} = 587,\ p \equiv 3 \bmod 4$, therefore the algorithm also works on complete Edwards curves E_d (2) , isomorphic to cyclic curves in the Montgomery form. This does not

correspond to the task, and does not confirmed by theoretical results. In addition, such an implementation of the CSIDH, is known [5].

4. MODEL OF IMPLEMENTATION OF THE CSIDH ALGORITHM ON QUADRATIC AND TWISTED SEC

To illustrate the above conclusions, consider a simple model of the CSIDH algorithm on quadratic and twisted SEC that form quadratic twist pairs with the same order [9]. Let such a pair of curves contain kernels of the 3-rd and 5-th order at the smallest value $n=15$, then the minimum prime $p=239$ and the order of these curves $N_E=16n=240$. The parameter d of the entire family of 118 quadratic Edwards curves can be taken as squares $d=r^2 \bmod p, r=2..119.$. Of these, 30 pairs of quadratic and twisted SKE were found with parameters $a=\pm 1$ and $\chi(ad)=1$. The quadratic SEC (3) is denoted by E_d, and the twisted SKE (4) is denoted as $E_{-1,-d}$. Table 1 shows the parameter d values for pairs of quadratic and twisted SEC. We written they as squares $d=r^2 \bmod p,, r=5..119.$

Table 1

Parameter d values of quadratic and twisted SEC $(a=\pm 1)$ for $p=239$ and $N_E=240$

25	64	121	196	50	183	5	10	87	176
24	153	11	110	48	187	120	193	27	160
213	44	2	201	61	3	206	192	80	62

In the CSIDH algorithm, an isogenic mapping $\Theta_A=[l_1^{e_1}, l_2^{e_2}, .., l_K^{e_K}]$ (class group action) from some base curve E_0 defines an isogenic curve $E_A=\Theta_A * E_0$. The sign of the degree e_i isogeny exponent specifies, in our case, a quadratic (e_i >0) or twisted (e_i < 0) SEC. At one step of the degree $[l_i^{e_i}], e_i=\pm 1$ isogeny chain, the coordinates $\alpha_k, k=1..s=(l-1)/2$ of the points of the curve (3) kernel or the curve (4) kernel of order l_i are calculated, then using formula (6) l_i - isogenic curve E' parameter d'. Two chains of isogenies with opposite signs of the exponents $\pm e_i$ give a neutral element of the mapping $[l_i^{e_i} \cdot l_i^{-e_i}]=[l_i^0]$, and then we get the original curve $E_0=[l_i^0]*E_0$. For example, for a pair of quadratic twist (3), (4) at $e_i=\pm 1$, one can calculate a 3-isogeny curve $E_{25}^{(0)} \to E_{110}^{(1)}$, then a transition to quadratic twist (4) $E_{110}^{(1)} \to E_{-1,-110}^{(1)}$, then a 3-isogeny of curve (4) $E_{-1,-110}^{(1)} \to E_{-1,-25}^{(2)}$, and return to curve (3) $E_{-1,-25}^{(2)} \to E_{25}^{(0)}$. This implies an important property: the sequences of parameters $d^{(i)}$ of isogenic quadratic and twisted SEC on a period have a reverse character. In other words, if such a sequence is calculated for quadratic SEC, then for twisted SEC it is not required to recalculate it, but it is enough to reverse it on a period (in the opposite order).

Tables 2 and 3 show the results of calculation the parameters $d^{(i)}$ of chains of 3- and 5-isogenic quadratic SEC for module $p=239$. For twisted SEC, the sequences $d^{(i)}$ should be read backwards on the period T. The period of 3-isogeny is $T=5$, and 5-isogeny $T=15$. To completeness in table 2 there are still 4 rows missing, and in table 3 - 2 rows with the parameters of table 1, however, the given data is sufficient for an example.

Table 2

Parameter $d^{(i)}$ values of two chains of 3-isogenic quadratic SEC ($a=1$) for $p=239$ (period $T=5$)

i	**0**	**1**	**2**	**3**	**4**	**5**
$d^{(i)}$	25	110	50	10	3	25
$d^{(i)}$	193	62	61	2	5	193

Table 3

Parameter $d^{(i)}$ values of the chain of 5-isogenic quadratic SEC ($a=1$) for $p=239$, (period $T=15$)

i	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
$d^{(i)}$	25	201	62	10	121	5	110	183
i	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
$d^{(i)}$	61	3	187	193	50	11	2	25

Let us take the secret keys of the exponents $\{e_i\}$ isogenies of Alice and Bob's $\Omega_A=(3,-4)$, $\Omega_B=(-4,5)$, their functions of isogenic mappings, respectively $\Theta_A=[3^3,5^{-4}],\Theta_B=[3^{-4},5^5]$, Let's calculate their public keys d_A, d_B . As the starting curve of the chain of isogenies, we will take the curve $E^{(0)}=E_{25}$. Alice calculates the parameters of 7 isogenic curves $E^{(i)}$: three 3-isogenuc quadratic SEC and 4 5-isogenic twisted SEC in an arbitrary order. According to tables 2 and 3, her calculations generate a chain of length 7 isogeny curves

$$E^{(0)}=E_{25}\to E_{110}\to E_{50}\to E_{10}\Rightarrow E_{-1,-10}\to E_{-1,-62}\to E_{-1,-201}\to E_{-1,-25}\to E_{-1,-2}\Rightarrow E_2.$$

So, Alice's public key $d_A=2.$. Similar calculations of Bob with a secret key $\Omega_B=(-4,5)$ form a chain of length 9 isogeny curves

$$E_{25}\to E_3\to E_{10}\to E_{50}\to E_{110}\Rightarrow E_{-1,-110}\to E_{-1,-183}\to E_{-1,-61}\to E_{-1,-3}\to E_{-1,-187}\to E_{-1,-193}\Rightarrow E_{193},$$

which gives the value of its public key $d_B=193.$

Further, in the secret-sharing scheme, Alice, knowing Bob's public key, calculates the isogenic curve $E_{BA}=[3^3,5^{-4}]*E_{193}=E_{187}$. Bob gets the same result using the function $E_{AB}=[3^{-4},5^5]*E_2=E_{187}$. The shared secret is the parameter $d_{AB}=187.$ If we know the sum key of Alice and Bob $\Omega_A+\Omega_B=(-1,1),$ using tables 2, 3, it is easy to check this result: $d^{(0)}=25\to d^{(1)}=3\to d^{(2)}=187.$ Keys of opposite sign make the work of Alice and Bob fruitless.

In principle, the CSIDH algorithm can be perform with exponents $\{e_i\}$ of the same sign and doubling their values to preserve security, but such a prospect, which halves the number of curves in the algorithm, is hardly interesting.

The results of the implementation of the Edwards-CSIDH model [5] in projective coordinates $(W:Z)$ state that it is faster than the Montgomery-CSIDH model in coordinates $(X:Z)$ by 20%. Note that this model is construct on complete Edwards curves with order $N_E=4n(n-odd)$. On the basis of Theorems 1 and 2 in [8], in [9], and in this paper, we have shown how to implement such a model on quadratic and twisted SEC that form pairs of quadratic twist. The advantage of these 2 classes of curves over the complete Edwards curves is the doubling of the number of curves used in the CSIDH algorithm with a corresponding increase in security. In addition, the time-consuming inversion $d\to d^{-1}$ of the parameter is not required when going to the complete quadratic twist curve.

It can be concluded that the work [4], Theorem 2 and the illustration of the CSIDH model in this work will convince the authors of [1] of the erroneousness of their concept, that it is possible to implement the CSIDH algorithm using a single class "*purely* Edwards curves". In further research, we will consider the problems of constant-time CSIDH [16, etc.] and sampling of points.

References:

1. Tomoki Moriya, Hiroshi Onuki, and Tsuyoshi Takagi. How to construct CSIDH on Edwards curves. In *Cryptographers' Track at the RSA Conference–CT-RSA 2020*, pages 512–537. Springer, 2020.
2. Castryck, W., Lange, T., Martindale, C., Panny, L., Renes, J.: CSIDH: An efficient post-quantum commutative group action. In: Peyrin, T., Galbraith, S. (eds.) Advances in Cryptology { ASIACRYPT 2018. pp. 395{427. Springer International Publishing, Cham (2018).
3. 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.
4. 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, PP. 1-1
5. Suhri Kim, Kisoon Yoon, Young-Ho Park, and Seokhie Hong. Optimized Method for Computing Odd-Degree Isogenies on Edwards Curves. In *Advances in Cryptology–ASIACRYPT 2019*, pages 273–292. Springer, 2019.
6. Farashahi, R.R., Hosseini, S.G.: Differential addition on twisted Edwards curves. In: Pieprzyk, J., Suriadi, S. (eds.) Information Security and Privacy. pp. 366{378. Springer International Publishing, Cham (2017).
7. Moody D., Shumow D. Analogues of Velus formulas for isogenies on alternate models of elliptic curves. Mathematics of Computation, vol. 85, no. 300, pp. 1929–1951,(2016).
8. Bessalov, A., Sokolov, V., Skladannyi, P., Zhyltsov, O. Computing of odd degree isogenies on supersingular twisted Edwards curves. CEUR Workshop Proceedings, 2021, 2923, pp. 1–11.(2021)
9. Бессалов А.В., Цыганкова О.В. Абрамов С.В. Оценка вычислительной сложности алгоритма CSIDH на суперсингулярных скрученных и квадратичных кривых Эдвардса. Радиотехника, 2021. – вып..207, С.40-51.
10. A. Bessalov, V. Sokolov, P. Skladannyi. Modeling of 3- and 5-Isogenies of Supersingular Edwards Curves // Proceedings of the 2nd International Workshop on Modern Machine Learning Technologies and Data Science (MoMLeT&DS'2020), June 2–3, 2020: abstracts. — No. I, vol. 2631. — Aachen: CEUR, 2020. — P. 30–39.
11. Бессалов А.В. Эллиптические кривые в форме Эдвардса и криптография. Монография. «Политехника», Киев, 2017. - 272с.
12. Bessalov A.V., Tsygankova O.V. Number of curves in the generalized Edwards form with minimal even cofactor of the curve order. Problems of Information Transmission, Volume 53, Issue 1 (2017), Page 92-101. doi:10.1134/S0032946017010082
13. Bessalov, A.V., Kovalchuk, L.V. Supersingular Twisted Edwards Curves Over Prime Fields. I. Supersingular Twisted Edwards Curves with j-Invariants Equal to Zero and 12^3. Cybernetics and Systems Analysis, 2019, 55(3), Page 347–353.
14. Bessalov, A.V., Kovalchuk, L.V.Supersingular Twisted Edwards Curves over Prime Fields.* II. Supersingular Twisted Edwards Curves with the j-Invariant Equal to 66^3. Cybernetics and Systems Analysis, 2019, 55(5), Page 731–741.
15. Washington L,C.. Elliptic Curves. Number Theory and Cryptography. Second Edition. CRC Press, 2008.
16. A. Jalali, R. Azarderakhsh, M. M. Kermani, D. Jao.: Towards optimized and constant-time CSIDH on embedded devices. IACR Cryptology ePrint Archive 2019/297; https://eprint.iacr.org/2019/297. (to appear at COSADE 2019).

Received 05.01.2022

Відомості про авторів:

Бессалов Анатолій Володимирович – д-р техн. наук, професор, Київський університет імені Бориса Грінченка, професор кафедри інформаційної та кібернетичної безпеки, факультет інформаційних технологій та управління, Україна; email: bessalov@ukr.net; ORCID: https://orcid.org/0000-0002-6967-5001

RADIOLOCATION AND RADIONAVIGATION
РАДІОЛОКАЦІЯ І РАДІОНАВІГАЦІЯ

УДК 621.396.967.2 **DOI: 10.30837/rt.2022.1.208.03**

М.Г. ТКАЧ, І.В. СВИД, канд. техн. наук, О.В. ВОРГУЛЬ, канд. техн. наук,
С.В. СТАРОКОЖЕВ, О.С. МАЛЬЦЕВ, А.О. ГЛУЩЕНКО

ОЦІНКА ВІДНОСНОЇ ПРОПУСКНОЇ ЗДАТНОСТІ ЗАПИТАЛЬНИХ СИСТЕМ СПОСТЕРЕЖЕННЯ ПОВІТРЯНОГО ПРОСТОРУ

Вступ

Запитальні системи радіолокаційного спостереження повітряного простору, до яких відносяться системи вторинної радіолокації [1-4] та системи ідентифікації повітряних об'єктів за принципом «свій-чужий» [5-8] відіграють істотну роль в інформаційному забезпеченні, як системи контролю повітряного простору [9] і управління повітряного руху [10]. В даний час існують два принципи побудови вищевказаних систем: суміщені та розподілені за частотами запиту та відповіді [11]. Структура запитальних радіолокаційних систем складається з каналу запиту та каналу відповіді, і є двоканальною системою передачі даних [12]. Кожен з каналів передачі даних вторинних радіолокаційних систем спостереження повітряного простору має певну пропускну здатність [13-16], яка обмежується впливом значної кількості дестабілізуючих факторів, до яких відносяться, як акти несанкціонованого використання літакового відповідача [17] для отримання бортової інформації повітряного об’єкту, так і акти перекручування передаваємих польотних даних.

Побудова літакового відповідача запитальних систем радіолокаційного спостереження повітряного простору на принципах відкритої одноканальної системи масового обслуговування з відмовами [18-20], а також використання в якості інформаційних сигналів примітивних інтервально-часових та позиційних кодів [21-23] дозволяє зацікавленій стороні реалізувати несанкціоноване використання літакового відповідача з метою отримання польотної інформації і, навіть, повну паралізацію літакових відповідачів аналізованих систем шляхом випромінювання сигналів запиту необхідної інтенсивності.

Можна стверджувати, що існуючі запитальні системи радіолокаційного спостереження повітряного простору утворені двома каналами передачі даних, пропускна здатність яких значною мірою визначає якість інформаційного забезпечення споживачів системи контролю використання повітряного простору. При цьому слід зазначити, що смуга частот даних систем сильно перевантажена. Це викликає значну щільність внутрісистемних завад як у каналі запиту, так і в каналі відповіді. І це, як наслідок, істотно знижує пропускну здатність [24] систем спостереження.

Про перевантаженість частотного діапазону 1030/1090 МГц аналізованих інформаційних систем і вплив цього на якість передачі даних відзначається, зокрема, в роботах [25-26]. У роботі [26] показано, що у смузі частот 1030/1090 МГц, яка розподілена для спостереження за повітряним рухом, відчуваються значні навантаження, а також представлені альтернативні методи використання змінних потужностей для зменшення навантаження спектру, запропонований метод збільшення пропускної здатності каналу за допомогою інноваційних методів передачі та декодування та показано, що смуга 1090 МГц використовується все більшою кількістю повітряних суден, додатків і типів обладнання і може досягти критичних рівнів внутрісистемних завад. Втрата даних через перекриття повідомлень або спотворень певною мірою допустима у всіх протоколах, але є побоювання, що ця втрата продуктивності незабаром стане неприйнятною, коли щільність повідомлень зросте.

Питанням оцінки пропускної здатності як літакового відповідача, так і всієї запитальної системи радіолокаційного спостереження повітряного простору присвячена значна кількість

робіт [13, 14, 16, 27, 28]. Так, у роботі [27] показано, що відносна пропускна здатність вторинних радіолокаторів значно знижується як за рахунок конструкції вторинного радіолокатора, так і за рахунок принципів обслуговування сигналу запиту в літаковому відповідачі. Проведені розрахунки дозволили оцінити відносну пропускну здатність вторинного радіолокатора, як функцію відносної пропускної здатності літакового відповідача за даними, які, у свою чергу, визначаються інтенсивністю потоків сигналів запиту, навмисних та внутрісистемних завад, щільністю шуму в каналі у відповідь, а також критерієм обробки польотної інформації.

У статті [28] показано, що зважаючи на суттєві недоліки, що існують у запитальних радіолокаційних систем спостереження повітряного простору, розробка нових запитальних систем спостереження повітряного простору повинна здійснюватися шляхом удосконалення структури форматів сигналів запиту та відповіді, а також використанням шифрування, що дозволить забезпечити кращу практичну продуктивність, високу безпеку та незначні внутрісистемні завади.

Роботи [29-31] присвячені розробці методів підвищення інформаційних можливостей літакових відповідачів запитних систем спостереження повітряного простору та оптимальному виміру параметрів прийнятих сигналів у аналізованих інформаційних системах. Також показано, що підвищення якості інформаційних смроможностей та оптимізації вимірювання параметрів сигналів відповіді можливі шляхом зміни структури сигналів запиту і відповіді, і підвищенням пропускної здатності каналів запиту і відповіді запитальних вторинних радіолокаційних систем.

У представленій роботі розглядається метод підвищення пропускної здатності запитальних вторинних радіолокаційних систем спостереження повітряного простору, в якому у сигналах запиту і відповіді використовуються широкосмугові сигнали, що дозволяє значно знизити дальність виявлення таких сигналів відповіді з необхідними показниками якості засобами радіорозвідки, що практично виключає можливість зацікавленій стороні використовувати сигнали відповіді літакового відповідача для далекого виявлення повітряних об'єктів і вимірювання їх координат і, як наслідок, дозволяє виключити акт несанкціонованого використання інформації літакового відповідача запитальних систем спостереження повітряного простору зацікавленою стороною, а, отже, підвищити відносну пропускну здатність розглядаємих інформаційних систем.

Метод підвищення пропускної здатності запитальних систем спостереження повітряного простору

Як зазначено вище, існуюча мережа запитувачів та літакових відповідачів запитальних систем спостереження повітряного простору побудована на принципі несинхронної мережі, а сам літаковий відповідач – на принципі відкритої одноканальної системи масового обслуговування з відмовами. Така побудова запитальних систем спостереження повітряного простору виключає різницю між корисними і навмисними завадами і, як наслідок, не дозволяє виключити з обслуговування навмисні корельовані завади якими, зазвичай, виступають діючі сигнали запиту інших запитувачів.

Використання у сигналах відповіді запитальних систем спостереження повітряного простору примітивного кодування і простих прямокутних імпульсів без внутріімпульсної модуляції дозволяють зацікавленій стороні несанкціоноване використання літакових відповідачів, існуючих запитальних систем спостереження повітряного простору з метою отримання інформації (системи радіорозвідки) на значному видаленні. При цьому слід зазначити, що зацікавлена сторона може використовувати не тільки сигнали відповіді літака для оцінки координат повітряного об'єкта [5, 11, 16], а також використовувати несанкціонований запит літака, використовуючи базу діючих сигналів запиту, що дозволяє спростити обчислення координат повітряного об'єкта. Цей режим може бути використаний зацікавленою стороною і з

метою повної паралізації літакового відповідача, що дозволяє здійснити перекручування інформації літакового відповідача.

Оцінимо пропускну здатність літакових відповідачів запитальних систем спостереження повітряного простору за критерієм дальності виявлення сигналів відповіді. Система радіотехнічної розвідки здатна вирішити координатну задачу при виявленні на всіх приймальних пунктах одного імпульсу сигналу відповіді. Ці обставини дозволяють зацікавленій стороні здійснювати виявлення не тільки окремих імпульсів сигналу відповіді запитальних систем спостереження повітряного простору, а також сигналу відповіді в цілому, при використанні, наприклад, багатоканальних виявлювачів, за рахунок апріорно відомих сигналів відповіді.

Позначимо довжину електромагнітної хвилі випромінюваного сигналу λ, потужність передавача літакового відповідача P, коефіцієнт підсилення антени літакового відповідача G, ефективну площу приймальної антени A, граничну чутливість приймача $P_{\min}$. Сигнали літакового відповідача збуджуються у приймальній антені системи радіотехнічної розвідки, що розташована на відстані r від літакового відповідача, щільність потоку потужності електромагнітної хвилі, яка визначається $S_{pr} = PG / 4\pi r^2$. В цьому випадку потужність сигналу на вході приймача без урахування поляризаційних втрат складатиме

$$P_{pr} = S_{pr} A = \frac{PGA}{4\pi r^2}. \quad (1)$$

Для виявлення сигналу відповіді необхідно, щоб відношення сигнал/шум перевищувало граничний рівень. При цьому порогове відношення сигнал/шум можна, як правило, оцінити виходячи з наступного співвідношення

$$q = \sqrt{P_{pr} / N_0}, \quad (2)$$

де $N_0 = kT(K_{ch} - 1)$ – спектральна щільність потужності шумів, k – постійна Больцмана, K_{ch} – коефіцієнт шуму приймача, T =290 К – температура в Кельвінах.

Використовуючи наведені співвідношення (1) і (2) можна оцінити, що дальність виявлення сигналів відповіді типових літакових відповідачів запитальних систем спостереження повітряного простору системою радіотехнічної розвідки становить 360 км. при ймовірності правильного виявлення $D = 0.9$ та ймовірності помилкової тривоги $F = 10^{-6}$, що відповідає дальності прямої видимості на висоті 12,4 км (при висоті підйому антени 10 м). Таким чином, можна зазначити, що зони виявлення сигналів відповіді літакового відповідача запитальних систем спостереження повітряного простору, як правило, обмежуються відстанню прямої видимості й значно перевищують зони виявлення первинних радіолокаторів.

Виходячи з вищевикладеного можна зазначити, що принцип побудови літакового відповідача існуючих запитальних систем спостереження повітряного простору і використовувані інформаційні сигнали дозволяють їх використовувати, як для далекого виявлення повітряного об'єкта, так і для перекручування інформації про державну приналежність виявленого повітряного об'єкта постановкою навмисних корельованих завад необхідної інтенсивності.

Оцінка відносної пропускної здатності радіолокаційних систем спостереження повітряного простору при використанні широкосмугових сигналів

Вважатимемо, що сигнали запиту запитальних систем спостереження повітряного простору і сигнали літакового відповідача зазначених інформаційних систем кодуються широкосмуговими сигналами. Вважатимемо, що на вхід відповідача надходять:

- потік сигналів запиту, утворений із сигналів запиту сусідніх запитальних систем спостереження повітряного простору та навмисних корельованих завад, імітованих зацікавленою стороною;
- потік хаотичних імпульсних завад.

Розрахунки відносної пропускної здатності літакового відповідача проведемо при роботі запитальних систем спостереження повітряного простору в режимі ідентифікації повітряних об'єктів для сумарного потоку сигналів неімітостійких та імітостійких режимів роботи. Як показано вище, основний вплив на пропускну здатність запитальних систем спостереження повітряного простору здійснюють ті несприятливі ситуації, які призводять до паралізації відповідача на час прийому та декодування сигналів запиту, формування та випромінювання сигналів відповіді. Тому обмежимо аналіз лише ними.

При надходженні на вхід літакового відповідача сумарного потоку сигналів запиту та хаотичної імпульсної завади літаковий відповідач не сформує сигнали відповіді, якщо складеться хоча б одна з наступних ситуацій:

- сигнал запиту розглядаємого запитувача подавиться через випереджаючі сигнали запиту сусідніх запитувачів або запитувачів зацікавленої сторони, що призводять до спрацьовування схеми подавлення бічних пелюсток або випромінювання сигналу відповіді;

- сигнал запиту розглядаємого запитувача подавиться через випереджаючі помилкові сигнали запиту, утворені в результаті взаємодії першого імпульсу коду запиту розглянутого запитувача з випереджальними на базу коду імпульсами хаотичних імпульсів завад або потоку сигналів запиту (хибні тривоги другого роду), що призводять до спрацьовування схеми подавлення бічних пелюсток або випромінювання сигналу відповіді.

Визначимо ймовірності цих подій у припущенні, що потоки сигналів запиту та хаотичних імпульсних завад незалежні та кількість джерел, які формують загальний потік сигналів запиту, досить велика, що дозволяє вважати його пуасонівським.

Вважатимемо, що на вхід літакового відповідача надходять:

- потік хаотичних імпульсних завад інтенсивністю λ_0 ;

- потік сигналів запиту по основним пелюсткам діаграми спрямованості антени запитувачів інтенсивністю λ_1;

- потік сигналів запиту з бокових пелюсток діаграми спрямованості запитувачів інтенсивністю λ_2.

Припускаємо, що тривалість імпульсів сигналів запиту однакова і дорівнює тривалості імпульсів корисного сигналу τ_0, а сумарний потік сигналів запиту складається з k_n часток неімітостійкого режиму та $(1-k_n)$ часток імітостійкого режиму.

Імовірність того, що хоча б один із сигналів запиту потрапить в випереджальний інтервал і подавить сигнал запиту розглядаємого запитувача за рахунок часу паралізації t_1 літакового відповідача в неімітостійкому режимі під час випромінювання сигналу відповіді літаковим відповідачем визначається:

при дії потоку хаотичних імпульсних завад

$$P_1^1 = 1 - \exp\left(-\lambda_x t_1\right), \tag{3}$$

при дії потоку сигналів запиту

$$P_1^2 = 1 - \exp\left(-k_n \lambda_x t_1\right), \tag{4}$$

де λ_x – середня кількість хибних n-імпульсних кодів сигналів, які призводять до випромінювання сигналу відповіді; $k_n = \lambda_n / \left(\lambda_1 + \lambda_2\right)$ – відносна частка сигналів неімітостійкого режиму потоку сигналів запиту; λ_n – інтенсивність потоку сигналів запиту неімітостійкого режиму.

Середня кількість помилкових n-імпульсних кодів сигналів запиту, які призводять до випромінювання сигналу відповіді, можна оцінити виходячи з наступного співвідношення

$$\lambda_x = \tau_0^n \lambda_0^{n-1} \left(1 - \frac{\tau_s}{\tau_0}\right), \tag{5}$$

де τ_s – задана тривалість імпульсів їхньої часової селекції.

Імовірність того, що хоча б один сигнал запиту потрапить у випереджальний інтервал і подавить сигнал запиту розглядаємого запитувача через час паралізації t_2 літакового відповідача в імітостійкому режимі за час випромінювання сигналів відповіді визначається:

при дії хаотичних імпульсних завад

$$P_1^3 = 1 - \exp(-\lambda_x t_2), \tag{6}$$

при дії потоку сигналів запиту

$$P_1^4 = 1 - \exp(-(1-k_n)\lambda_1 t_2). \tag{7}$$

У цьому випадку результуюча ймовірність подавлення розглядаємих сигналів запиту через паралізацію літакового відповідача під час випромінювання сигналу відповіді можна оцінити виходячи з наступного співвідношення

$$P_1 = 1 - \prod_{i=1}^{4}(1 - P_1^i). \tag{8}$$

Імовірність того, що хоча б один сигнал запиту надійде в випереджальний інтервал і подавить сигнал запиту розглядаємого запитувача за рахунок часу паралізації t_3 літакового відповідача під час спрацьовування схеми подавлення бічних пелюсток в неімітостійкому режимі визначається:

від хаотичних імпульсних завад

$$P_2^1 = 1 - \exp(-\lambda_x t_3), \tag{9}$$

від потоку сигналів запиту

$$P_2^2 = 1 - \exp(-k_n \lambda_2 t_3). \tag{10}$$

Імовірність того, що хоча б один сигнал запиту надійде в випереджальний інтервал і подавить сигнал запиту розглянутого запитувача за рахунок часу паралізації t_4 відповідача при спрацьовуванні схеми подавлення бічних пелюсток в імітостійкому режимі визначається відповідно до потоку сигналів запиту:

від хаотичних імпульсних завад

$$P_2^3 = 1 - \exp(-\lambda_x t_4), \tag{11}$$

від потоку сигналів запиту

$$P_2^4 = 1 - \exp(-(1-k_n)\lambda_2 t_4). \tag{12}$$

Результуюча ймовірність подавлення розглядаємих сигналів запиту через паралізацію відповідача при прийомі сигналів відповіді за бічними пелюстками діаграми спрямованості антени запитувача становить

$$P_2 = 1 - \prod_{i=1}^{4}(1 - P_2^i). \tag{13}$$

Сигнали запиту розглядаємого запитувача можуть бути подавлені випереджальними помилковими сигналами запиту, які утворюються в результаті взаємодії першого імпульсу коду запиту з випереджальними імпульсами потоку сигналів запиту і призводять до спрацьовування схеми подавлення бічних пелюсток або випромінювання сигналу. Імовірність помилкової тривоги другого роду визначається формулою

$$P_3 = (1 - P_{01})\left[1 - (1 - P_{10})^{n-1}\right]. \quad (14)$$

де $P_{01} = 1 - \exp(-\lambda_0 \tau_0)$, $P_{10} = 1 - \exp(-\lambda_0 \tau_p)\left[1 - \gamma(1 - \exp(1 - \lambda_0 \tau_0))\right]$, τ_p - час паралізації приймального пристрою після проходження крізь нього імпульсу завади, γ - коефіцієнт, який визначає ймовірність інтерференціального подавлення імпульсу прийнятого сигналу при його збігу в часі з імпульсом завади.

Результуюча ймовірність випромінювання сигналів відповіді літаковим відповідачем на сигнали запиту розглядаємого запитувача становить:

$$\text{при } (\lambda_1 + \lambda_2) < \lambda_M \qquad P_0 = \prod_{i=1}^{3} (1 - P_i), \quad (15)$$

$$\text{при } (\lambda_1 + \lambda_2) > \lambda_M \qquad P_0 = P_{AR} \prod_{i=1}^{3} (1 - P_i), \quad (16)$$

де P_{AR} - пропускна здатність літакового відповідача.

Залежності пропускної здатності літакового відповідача від часової бази сигналів відповіді наведено на рис. 1-3.

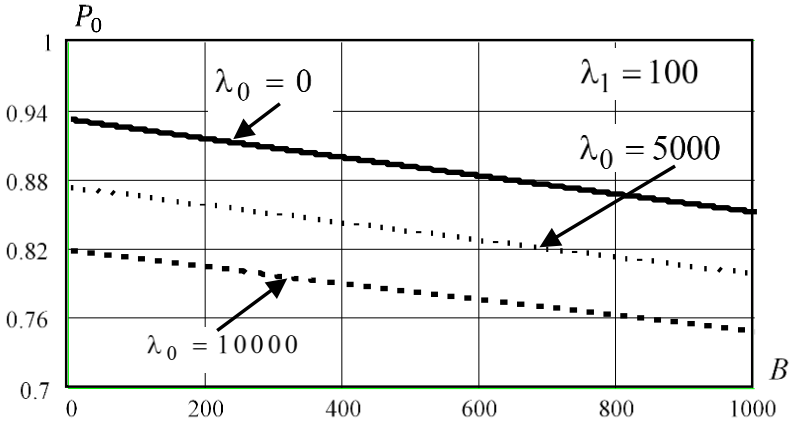


Рис. 1. Вплив бази сигналів відповіді на пропускну здатність літакового відповідача при $\lambda_1 = 100$

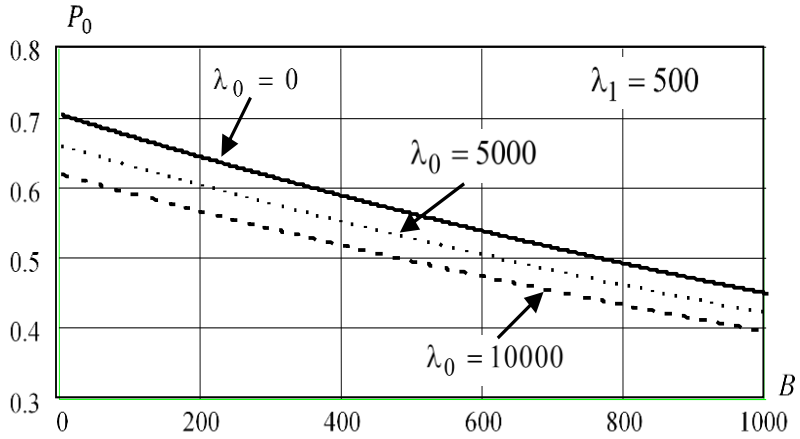


Рис. 2. Вплив бази сигналів відповіді на пропускну здатність літакового відповідача при $\lambda_1 = 500$

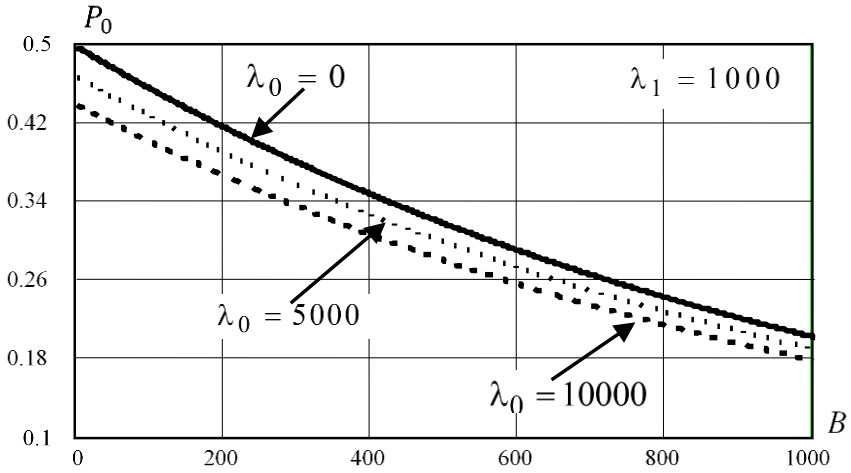


Рис. 3. Вплив бази сигналів відповіді на пропускну здатність літакового відповідача при $\lambda_1 = 1000$

Розрахунки виконані для імітостійкого режиму та фіксованих інтенсивностей потоків сигналів запиту за основними пелюстками діаграми спрямованості антени запитувачів λ_1 і хаотичних імпульсних завад λ_0 за умови, що інтенсивність λ_1 у п'ять разів менше інтенсивності λ_2 потоку сигналів запиту з бокових пелюсток діаграми спрямованості антени запитувача. Наведені залежності дозволяють робити такі висновки:

- збільшення часової бази сигналів відповіді призводить до зменшення пропускної здатності літакового відповідача за будь-яких інтенсивностей потоків сигналів запиту та хаотичних імпульсних завад, що пояснюється зростанням сумарного часу паралізації літакового відповідача при формуванні та випромінюванні тривалих сигналів відповіді;

- в умовах низької інтенсивності потоку сигналів запиту за основними пелюстками діаграми спрямованості антени запитувачів ($\lambda_1 = 100$) збільшення часової бази сигналів відповіді призводить до порівняно незначного зменшення пропускної здатності літакового відповідача. Наприклад, збільшення часової бази сигналів відповіді з 200 до 1000 при $\lambda_0 = 0$ призводить до зменшення пропускної здатності літакового відповідача з 0,92 до 0,86, тобто зменшення в 1,07 рази. Це пояснюється тим, що при незначній інтенсивності потоку сигналів запиту відповідач встигає обслуговувати переважну більшість сигналів запиту;

- за умови інтенсивнішого потоку сигналів запиту збільшення часової бази сигналів відповіді призводить до більш значного зменшення пропускної здатності літакового відповідача. Так, за інтенсивністю потоку сигналів запиту $\lambda_1 = 100$ і відсутність хаотичних імпульсних завад збільшення бази сигналів з 200 до 1000 призводить до зменшення пропускної здатності літакового відповідача з 0,65 до 0,46 (в 1,4 рази), а при інтенсивності $\lambda_1 = 500$ коефіцієнт готовності зменшується з 0,54 до 0,2 (у 2,2 рази);

- збільшення інтенсивності хаотичних імпульсних завад призводить до зменшення пропускної здатності літакового відповідача через утворення помилкових сигналів запиту та паралізації відповідача на час їх обслуговування, у тому числі формування та випромінювання тривалих сигналів відповіді.

Для оцінки відносної пропускної здатності запитальних систем спостереження повітряного простору аналізованою системою вважатимемо, що:

- апаратура обробки сигналів відповіді в запитувачах реалізує алгоритм квазіоптимального виявлення пачки сигналів відповіді;

- відносна пропускна здатність літакового відповідача постійна в межах усієї пачки сигналів відповіді.

При такій постановці питання ймовірність виявлення пачки сигналів відповіді в запитувачі, а отже і виявлення повітряного об'єкта запитальною системою спостереження повітряного простору за логікою «k з m» можна записати як

$$P_c = \sum_{i=k}^{m} C_m^i P_0^i \left(1 - P_0\right)^{m-i}, \tag{17}$$

На рис. 4 і рис. 5 наведено залежності ймовірності виявлення повітряного об'єкта розглянутою запитальною системи спостереження повітряного залежно від часової бази сигналу відповіді у відповідності до виразу (17).

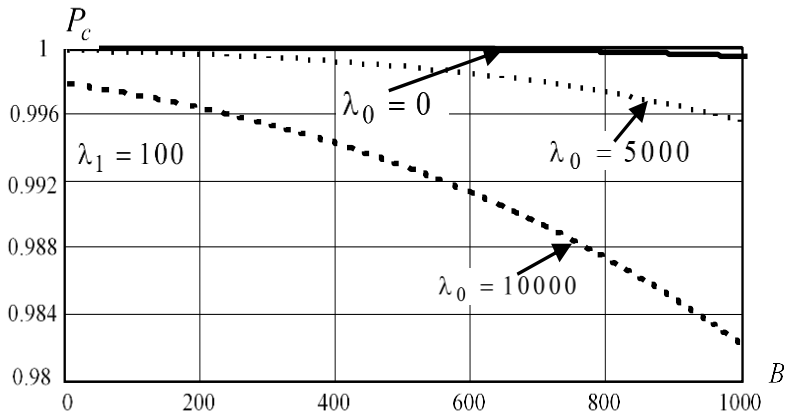


Рис. 4. Вплив бази сигналів відповіді на відносну пропускну здатність запитальних систем спостереження повітряного простору при $\lambda_1 = 100$

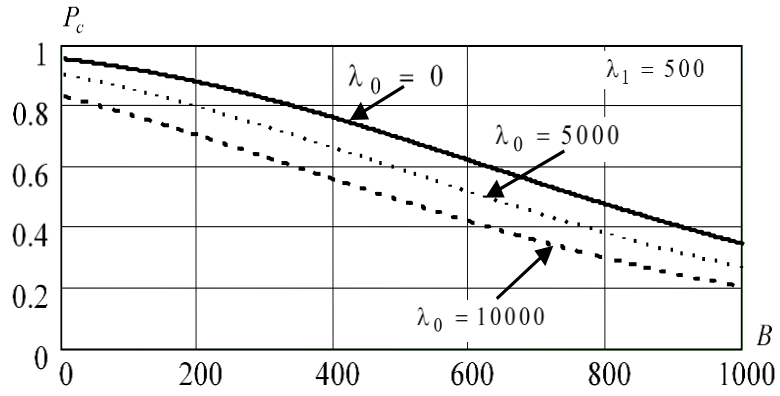


Рис. 5. Вплив бази сигналів відповіді на відносну пропускну здатність запитальних систем спостереження повітряного простору при $\lambda_1 = 500$

Подані залежності показують відносно прийнятні результати ймовірності ідентифікації повітряних об'єктів при використанні широкосмугових сигналів, як сигналів відповіді. Повертаючись до дальності виявлення повітряного об'єкта при використанні широкосмугових сигналів, як сигналів відповіді, можна показати, що при базі використовуємих сигналів відповіді, яка дорівнює 500 дальність виявлення засобами радіорозвідки при зазначених вище параметрах виявлення складе приблизно 16 км.

Висновки

За результатами проведеного дослідження можна зробити наступні висновки:

- спадкоємний перехід від існуючих запитальних радіолокаційних систем спостереження повітряного простору, у яких використовуються інтервально-часовий та позиційний коди з використанням вузькосмугових сигналів у каналі відповіді, до запитальних систем спостере-

ження повітряного простору, в яких кодування сигналів запиту та відповіді здійснюється широкосмуговими сигналами, дозволяє суттєвим чином знизити дальність виявлення зацікавленою стороною таких сигналів відповіді і, як наслідок, виключити акт несанкціонованого використання даних літакового відповідача запитальних систем спостереження повітряного простору зацікавленою стороною;

- виключення можливості несанкціонованого впливу на літаковий відповідач дозволяє виключити акт перекручування інформації запитальних систем спостереження повітряного простору та дозволяє підвищити інформаційну безпеку даних інформаційних систем за рахунок виключення порушення цілісності інформації;

- представлені розрахунки відносної пропускної здатності літакового відповідача запропонованого методу реалізації вторинного радіолокатора та ймовірності ідентифікації повітряних об'єктів загалом показали підвищення ефективності інформаційної безпеки.

Список літератури:

1. X. Du, K. Liao and X. Shen, "Secondary Radar Signal Processing Based on Deep Residual Separable Neural Network", 2020 IEEE International Conference on Power, Intelligent Computing and Systems (ICPICS), 2020. doi: 10.1109/icpics50287.2020.9202372.

2. G. Jiang, Y. Fan and H. Yuan, "Assessing the Capacity of Air Traffic Control Secondary Surveillance Radar System", 2019 Cross Strait Quad-Regional Radio Science and Wireless Technology Conference (CSQRWC), 2019. doi: 10.1109/csqrwc.2019.8799146.

3. V. Andrusevich and I. Obod, "Assessment of the Quality of Information Support by Air Radar Surveillance Systems", Advanced Information Systems, vol. 5, no. 2, pp. 78-82, 2021. Available: 10.20998/2522-9052.2021.2.10.

4. I. Obod, "Integrated Coordinate-and-Time Support for the Address Inquiry in the Secondary Radar Systems", Telecommunications and Radio Engineering, vol. 53, no. 3, pp. 54-56, 1999. doi: 10.1615/telecomradeng.v53.i3.100.

5. І. Свид, І. Обод. Завадостійкість радіолокаційних систем ідентифікації за ознакою «свій-чужий». Харків: Друкарня Мадрид, 2021, с. 253. doi: 10/30837/978-617-7988-76-1.

6. P. Poornima, B. Roja Reddy and B. Anantha Murthy, "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), 2018. doi: 10.1109/rteict42901.2018.9012646.

7. O. Strelnytskyi, I. Svyd, I. Obod, O. Maltsev, O. Voloshchuk and G. Zavolodko, "Assessment Reliability of Data in the Identification Friend or Foe Systems", 2019 IEEE 39th International Conference on Electronics and Nanotechnology (ELNANO), 2019. doi: 10.1109/elnano.2019.8783397.

8. I. Svyd, I. Obod, O. Maltsev, I. Shtykh and G. Zavolodko, "Model and Method for Detecting Request Signals in Identification Friend or Foe Systems", 2019 IEEE 15th International Conference on the Experience of Designing and Application of CAD Systems (CADSM), 2019. doi: 10.1109/cadsm.2019.8779322.

9. I. Ashurkov, V. Kakaev and N. Leshko, "Multiposition Radar System Space Structure Optimization", Informatsionno-upravliaiushchie sistemy (Information and Control Systems), vol. 6, no. 79, pp. 81-85, 2015. doi: 10.15217/issn1684-8853.2015.6.81.

10. W.C. Young; Ming-Ten Tsai; Li-Min Chuang. Air traffic control system management. Proceedings of the IEEE 2000 National Aerospace and Electronics Conference. NAECON 2000. Engineering Tomorrow (Cat. No.00CH37093). doi: 10.1109/NAECON.2000.894952.

11. Маляренко А.С. Системы вторичной радиолокации для управления воздушным движением и государственного радиолокационного опознавания [Справочник], ХУПС, 2007, 78 с.

12. І.І. Обод, В.В. Шевцова, "Порівняльний аналіз запитальних систем передачі інформації системи контролю повітряного простору", Збірник наукових праць Харківського національного університету Повітряних Сил, № 1(34), 2013, С. 123-125.

13. І.І. Обод, В.В. Шевцова, "Відносна пропускна спроможність запитальних систем передачі інформації системи контроля повітряного простору", Системи обробки інформації, № 2(109), 2013, С. 74-76.

14. V. Zhyrnov, S. Solonskaya, and I. Shubin, “Evaluation of radar image processing efficiency based on intelligent analysis of processes”, RT, vol. 4, no. 207, pp. 83–88, 2021. doi: 10.30837/rt.2021.4.207.09.

15. Обод И.И. Помехоустойчивые системы вторичной радиолокации. М.: ЦИНТ, 1998. 118 с.

16. І.І. Обод, В.В. Шевцова, "Пропускна спроможність відповідачів запитальних систем передачі польотної інформації", Системи обробки інформації, № 1(108), 2013, С. 105-108.

17. M. Strohmeier, "Large-Scale Analysis of Aircraft Transponder Data", IEEE Aerospace and Electronic Systems Magazine, vol. 32, no. 1, pp. 42-44, 2017. doi: 10.1109/maes.2017.160149.

18. Б.В. Бакуменко, І.І. Обод, "Методи підвищення завадозахищеності запитувальних радіотехнічних систем", Системи обробки інформації, № 9(58), 2006, С. 10-12.

19. І.І. Обод, О.О. Стрельницький, В.А. Андрусевич, "Структура та показники якості обробки інформації систем спостереження повітряного простору", Системи обробки інформації, № 8 (115), 2013, С. 80-83.

20. I. Obod, I. Svyd, O. Maltsev and S. Starokozhev, "The Effect of Masking Interference on the Quality of Request Signal Detection in Aircraft Responders of the Identification Friend or Foe Systems", 2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T), 2020. doi: 10.1109/picst51311.2020.9467955.

21. И.И. Обод, "Управление потоками сигналов в несинхронных сетях запросных систем вторичной локации", Радиоэлектроника и информатика, № 2, 1998, С. 4-5.

22. I. Svyd, I. Obod, O. Maltsev, I. Shtykh, G. Zavolodko and G. Maistrenko, "Model and Method for Request Signals Processing of Secondary Surveillance Radar", 2019 IEEE 15th International Conference on the Experience of Designing and Application of CAD Systems (CADSM), 2019. doi: 10.1109/cadsm.2019.8779347.

23. І.І. Обод, І.В. Свид, "Порівняльний аналіз якості виявлення повітряних об'єктів запитальними системами спостереження", Системи обробки інформації, № 9 (90), 2010, С. 74-76.

24. R. Morales-Ferre, P. Richter, E. Falletti, A. de la Fuente and E. S. Lohan, "A Survey on Coping With Intentional Interference in Satellite Navigation for Manned and Unmanned Aircraft," in IEEE Communications Surveys & Tutorials, vol. 22, no. 1, pp. 249-291, Firstquarter 2020, doi: 10.1109/COMST.2019.2949178.

25. T. Otsuyama, J. Honda, J. Naganawa and H. Miyazaki, "Analysis of signal environment on 1030/1090MHz aeronautical surveillance systems", 2018 IEEE International Symposium on Electromagnetic Compatibility and 2018 IEEE Asia-Pacific Symposium on Electromagnetic Compatibility (EMC/APEMC), 2018. doi: 10.1109/isemc.2018.8394048.

26. E. Valovage, "A method to measure the 1090 MHz interference environment", 2009 Integrated Communications, Navigation and Surveillance Conference, 2009. doi: 10.1109/icnsurv.2009.5172866.

27. I. Obod, I. Svyd, G. Zavolodko, O. Maltsev, B. Bakumenko and V. Chumak, "Assessing SSR Relative Data Capacity", 2021 IEEE 3rd Ukraine Conference on Electrical and Computer Engineering (UKRCON), 2021. doi: 10.1109/ukrcon53503.2021.9575971.

28. И.И. Обод, "Сравнительная оценка помехоустойчивости несинхронных и синхронных сетей запросных систем вторичной локации", Вестник ХГПУ, № 15, 1998, С. 58-61.

29. И.И. Обод, В.В. Глущенко, И.В. Коваль, "Методы повышения помехоустойчивости самолетных ответчиков запросных систем вторичной локации", Вестник ХГПУ, № 34, 1999, С. 84-86.

30. И.И. Обод, "Повышение эффективности систем управления воздушного движения за счет реализации разнесенных систем вторичной радиолокации", Радиоэлектроника и информатика: науч.-техн. журн., Вып. 1, 1997, С. 63-64.

31. М. Ткач, «Оцінка відносної пропускної здатності літакових відповідачів вторинних радіолокаційних систем спостереження повітряного простору», Радіотехніка, № 207, 2021, С. 123-131.

Надійшла до редколегії 17.02.2022

Відомості про авторів:

Ткач Марія Геннадіївна – аспірант кафедри мікропроцесорних технологій і систем, Харківський національний університет радіоелектроніки, Україна; email: mariia.zavorotna@nure.ua; ORCID: http://orcid.org/0000-0002-4248-7633

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

Воргуль Олександр Васильович – кандидат технічних наук, доцент, доцент кафедри мікропроцесорних технологій і систем, Харківський національний університет радіоелектроніки, Україна; email: oleksandr.vorgul@nure.ua; ORCID: https://orcid.org/0000-0002-7659-8796

Старокожев Святослав Валерійович – аспірант кафедри мікропроцесорних технологій і систем, Харківський національний університет радіоелектроніки, Україна; email: sviatoslav.starokozhev@nure.ua; ORCID: https://orcid.org/0000-0002-1600-1337

Мальцев Олександр Сергійович – старший науковий співробітник кафедри мікропроцесорних технологій і систем, Харківський національний університет радіоелектроніки, Україна; email: aleksandr.maltsev@nure.ua; ORCID: http://orcid.org/0000-0003-1520-9280

Глущенко Артем Олександрович – аспірант кафедри мікропроцесорних технологій і систем, Харківський національний університет радіоелектроніки, Україна; email: artem.hlushchenko@nure.ua; ORCID: https://orcid.org/0000-0003-2197-216X

УДК 621.396.96, 621.397.48:004.932.2 **DOI:10.30837/rt.2022.1.208.04**

В.М. КАРТАШОВ, д-р техн. наук, В.А. КИЗКА, В.А. ТИХОНОВ, д-р физ-мат. наук

ИСПОЛЬЗОВАНИЕ БПЛА-ПЕРЕХВАТЧИКОВ ДЛЯ УВЕЛИЧЕНИЯ ДАЛЬНОСТИ ОБНАРУЖЕНИЯ ДРОНОВ-НАРУШИТЕЛЕЙ

Вступление

Охрана критически важных индустриальных объектов от террористических атак с использованием беспилотных летательных аппаратов (БПЛА) является важной современной задачей. Усиление террористических организаций за счет их объединения с организованными преступными группировками, в частности, с наркобизнесом, существенно увеличивает финансирование террористических структур, позволяя им приобретать современное оружие [1]. Учитывая публичный, открытый характер террористических преступлений, направленных на произведение общественного резонанса с целью демонстрации своих возможностей и выставления требований, атака критически важного индустриального объекта причинит не только нарушение функционирования социально-экономического и промышленного комплекса, но и будет эффективно воздействовать на психику людей, чтобы их запугать, создать панику в обществе [2]. В странах со слабой экономикой, увеличивающейся бедностью, неразвитой медицинской службой велико число психопатических личностей, шизофреников, закомплексованных и просто бедных, которые составляют основу террористических организаций, поэтому любая атака на крупный промышленный объект в такой стране, будет выглядеть для таких людей хорошей рекламой, тем более широко освещённой средствами массовой информации, и приведет к вливанию их в ряды террористов с целью улучшить свое социальное положение, самоутвердиться и т.д. или же к обострению течения психических болезней, что приведет к увеличению преступности [2]. Эффективная защита критически важного объекта от террористической атаки БПЛА, которые доступны по цене, но способны причинить серьёзный вред промышленному объекту, т.к. способны переносить контейнеры с поражающими веществами, является насущной современной проблемой.

Имеющиеся системы обнаружения БПЛА вблизи критически важных индустриальных объектов базируются на дистанционных и мобильных наземных комплексах (автомобили и бронетехника) [3], оснащенных радиолокационными, оптическими, инфракрасными и акустическими средствами обнаружения [4-10], а также на использовании дронов-перехватчиков [18], [19], [24]. Последние оснащаются акустической системой обнаружения дрона-нарушителя по шуму его двигателей, оптической и инфракрасной системами обнаружения, средствами уничтожения или перехвата дрона-нарушителя. Использование РЛС для обнаружения дрона-нарушителя с помощью дронов-перехватчиков в литературе неизвестно, прежде всего из-за отсутствия малогабаритных РЛС комплексов, пригодных для этих целей.
В данной статье проводится обзор малогабаритных РЛС, используемых для обнаружения БПЛА, которые могут быть установлены на БПЛА-перехватчики, что обеспечит существенное увеличение дальности обнаружения дрона-нарушителя и уменьшит время его идентификации. Рассматриваются также методы патрулирования/облета территории вблизи критически важного индустриального объекта.

Обзор существующих малогабаритных РЛС

Цифровые радиолокационные комплексы L-диапазона с массой 48 кг, которые предполагается размещать на автомобилях и бронетехнике, позволяют обнаружить малоподвижные мини- и микро-БПЛА с эффективной поверхностью рассеяния радиоволн 0.01 м^2 на дальности от 100 м до 5500 м, по высоте - от 50 м до 500 м [3]. Мощность излучения изделия 60 Вт, чувствительность приемника $2 \cdot 10^{-17}$Вт. Авторы публикации указывают на отсутствие аналогов за рубежом.

В [11] приведен обзор многофункциональных бортовых РЛС (МБРЛС) Ku-диапазона массой от 30 до 60 кг для БПЛА, применяемых для боевых задач и картографирования местности на дальностях до 100 км с разрешением от 0.25 м, селекции радиоконтрастных наземных/надводных целей на дальностях до 300 км в любых погодных условиях и при наличии дымовых и пылевых завес на поле боя, оценки метеобстановки на дальности до 200 км, радиомониторинга. Масса созданной авторами [11] МБРЛС для выше указанных целей - 30.5 кг. БПЛА на которых используются МБРЛС имеют максимальную массу целевой нагрузки от 45 до 120 кг. Высота полета БПЛА, оснащенных МБРЛС, до 7км, скорость - до 220 км/ч, дальность полета – до 350 км. Следовательно, на них может быть установлена цифровая РЛС из [3]. Авторы [11] не обсуждают возможность использования МБРЛС для обнаружения БПЛА.

В [12] описаны стационарные малогабаритные РЛС X- и L-диапазонов массой 40 кг и 10 кг соответственно, для обнаружения и сопровождения БПЛА. Излучаемая импульсная мощность до 10 и 30 Вт соответственно для L- и X-диапазонов. Обе РЛС работают в связке, они разнесены на некоторое расстояние для ликвидации провалов в отраженном сигнале из-за интерференции с мощными отраженными сигналами от подстилающей поверхности. РЛС позволяют обнаружить микро-БПЛА на дальности до 3-5 км, но авторы не рассматривают возможность установки таких РЛС на БПЛА-перехватчики. Разрабатываются РЛС бокового обзора с синтезированной апертурой для БПЛА с целью мониторинга местности и для нахождения дефектов в трубопроводах [13]. Рассматривается интеграция бортовой РЛС с другими информационными каналами, установленными на БПЛА [14]. РЛС с синтезированной апертурой [13] формирует на выходе сигнал в виде изображения, несущего доступную для человеческого глаза информацию. Качество изображения не зависит от погодных условий и времени суток. Интеграция бортовой РЛС с другим бортовым оборудованием повышает эффективность решения общей задачи при оптимальном использовании ресурсов [14].

Разработана система радиолокационной съемки местности малогабаритной (3-4 кг) РЛС с синтезированной апертурой антенны, установленной на БПЛА самолетного типа или мультикоптере [15]. Реализована в L/X/C-диапазоне, мощности излучаемого сигнала 200 мВт, 1 Вт для L- и C/X-диапазонов, соответственно. Отмечается возможность уменьшения массы РЛС до 0.5 кг. Дальность действия станции 4-5 км при отсутствии “мертвой зоны”. Наилучшая разрешающая способность обеспечивается в X-диапазоне - 0.15 м. Радиоизображение формируется на борту БПЛА и передается по радиолинии на наземный пункт наблюдения в реальном масштабе времени. Эта система вполне пригодна для установки на БПЛА-перехатчик, но авторы [15] такой возможности не обсуждают.

В [16] рассмотрены малогабаритные радарные системы, установленные на двух БПЛА, объединенных в двухпозиционную систему за счет обмена данными между ними, с целью улучшения углового разрешения при обнаружении физического объекта (в статье, человека) в заданной области. Предусмотрен алгоритм выбора длительности радиоимпульсов, относительной траектории двух дронов в зависимости от размеров объекта обнаружения для получения наилучшего углового разрешения по азимуту: $\Delta\varphi=0.3°$ при расстоянии до объекта 5 км. Описанный комплекс вполне пригоден для обнаружения дрона-нарушителя парой дронов-перехватчиков, но авторы [16] рассматривают применение разработки только для спасательных целей или мониторинга техногенных объектов.

Предложен метод борьбы с противорадиолокационными ракетами (ПРР) за счет запуска БПЛА, оснащенного передающим устройством, имитирующим излучение РЛС [17]. Излучаемый передатчиком БПЛА отвлекающий сигнал должен быть на уровне чувствительности приёмника головки самонаведения ППР, если предполагается отключение РЛС при обнаружении ПРР. Для прикрытия работающей РЛС отвлекающий передатчик БПЛА должен излучать сигнал мощностью, сравнимой с мощностью сигнала РЛС на входе приемника головки самонаведения ППР. Такой БПЛА запускается при обнаружении ППР, радиус его облета РЛС по азимуту составляет до 500 м, что достаточно для обеспечения невозможности разре-

шения (распознавания) по угловым координатам РЛС и БПЛА системой наведения ракеты и превышает радиус разлета осколков ракеты.

Особенности существующих и перспективных дронов-перехватчиков

Комплексные наземные системы обнаружения БПЛА могут дополняться дронами-перехватчиками, способные автоматически наводиться, например, по шуму двигателей на преследуемый дрон, или по его изображению в системе «компьютерного зрения» дрона-перехватчика. Они имеют гораздо более мощные дизельные двигатели, оснащены защищенным корпусом и устройствами для разрушения других дронов [18]. Дроны-перехватчики ведут поиск дронов-нарушителей в заданной области или находят их по целеуказанию от комплексной системы. Вероятность обнаружения нарушителя при этом существенно повышается. Оснащены эти дроны оптическим и акустическими каналами обнаружения.

В [19] предложена концепция автоматизированного визуального обнаружения БПЛА-нарушителей и отправления им на перехват БПЛА-перехватчика, обладающего автономной бортовой системой управления для нейтрализации нарушителя путем тарана или захвата с применением кевларовых нитей. Авторы [19] отмечают, что сегодня в качестве средств уничтожения БПЛА наиболее часто используются либо средства радиоподавления (блокирование и искажение каналов спутниковой навигации, блокирование каналов управления и связи), либо средства огневого, электромагнитного или лазерного поражения. Авторами [19] разработана система наземного оборудования, включающая видеокамеру, тепловизионную камеру, дальномер и систему обработки информации. Дрон-перехватчик получает целеуказание от данной системы и отправляется на перехват или уничтожение, получая периодически обновленную информацию о координатах цели, или решает задачу автономно, используя бортовую видеокамеру и бортовой блок управления.

В [20] получена вероятность обнаружения и распознавания БПЛА оператором наземного комплекса цели, изображение которой передано по радиоканалу с БПЛА, оснащенном оптико-электронной системой (видео- и инфракрасные камеры). Вероятность зависит от параметров оптико-электронной системы, размеров цели и кинематики полета БПЛА. Полученная авторами формула для вероятности обнаружения применена к случаю обнаружения дроном спасательной службы пропавшего человека или объекта в труднодоступных районах. Никаких ограничений для применения формулы с целью оценки вероятности обнаружения дрона-нарушителя нет.

В [21] рассмотрены методы перехвата управления роем дронов злумышленниками с использованием различных уязвимостей: отказ в обслуживании (дрон заваливается флудом и становится невидимым для оператора дрона), деаутентификация (злоумышленник выявляет MAC-адреса оператора и дрона и отключает их от точки доступа), человек-посередине (злоумышленник вклинивается между оператором и дроном, используя свое устройство, например, Wi-Fi Pineapple, перехватывая управление дроном, а оператор получает имитацию SSID дрона от устройства злоумышленника, не подозревая о нападающем среднего уровня), несанкционированный доступ с полномочиями суперпользователя (злоумышленник подключается к дрону напрямую через открытый порт, выявляемый сканированием IP-сети некоторыми свободными утилитами, например, Nmap) и осуществляет подмену пакетов (злоумышленник генерирует IP-пакеты, выдающие себя за контроллер дрона). Эти методы можно применить и наоборот – вместо злоумышленника рассмотреть дрон-перехватчик, осуществляющий в автономном режиме один из способов перехвата управления дроном-нарушителем. Рассмотренный подход используется пока только дистанционными наземными средствами [19].

В [22] рассмотрены методы облета дронами, оснащенными видеокамерами, местности сельскохозяйственного назначения. Эти методы можно перенести на дроны-перехватчики, проводящие облет местности вокруг критически важного объекта в поисках дронов-нарушителей. Например, один дрон находится на подзарядке, а второй делает облет местно-

сти. Для подзарядки дронов предполагается использовать специально подобранные для этого места – гнёзда подзарядки, в пределах области облета. Дроны управляются из центра управления, относительно которого гнёзда могут быть расположены на разном расстоянии.

Проведена оценка параметров сканирующих лазерных дальномеров на борту БПЛА в интересах повышения безопасности движения транспортных средств [23]. Разработанная авторами [23] схема позволяет обнаруживать и распознавать объект на расстоянии до 240 м с помощью лазерных импульсных дальномеров. Эта схема вполне применима для использования на БПЛА-перехватчиках.

Разработаны БЛА-перехватчики с сетями-ловушками, оснащённые датчиками обнаружения (видеокамерами) и устройствами определения расстояния до объекта перехвата [24]. В [24] предложено устройство обнаружения БПЛА-нарушителя в виде малогабаритного радиолокатора “обнаружения активного типа, полуактивного (двухпозиционного) со специальным передатчиком или с передатчиком систем сотовой связи, устанавливаемых на перехватчике”. В патенте описана конструкция устройства с ловчей сетью на БПЛА-перехватчике, направляемом с земли к нарушителю по данным, получаемым от РЛС.

Оценка дальности обнаружения дрона-нарушителя с помощью бортовых локационных средств БПЛА-перехватчика

С целью выполнения оценок дальности обнаружения дрона-нарушителя с помощью БПЛА-перехватчика будем использовать следующие характеристики бортовой аппаратуры оптического и акустического каналов обнаружения и идентификации БПЛА:

- дальность обнаружения и идентификации БПЛА в дистанционном оптико-электронном канале достигает $r_{оэ}$=2[км] при наличии сложного неоднородного фона [25];

- дальность обнаружения в дистанционном акустическом канале - до $r_з$=200[м] (примерно равна минимальной дальности обнаружения в радиолокационном канале) достигается при наличии фона, обусловленного ветром [26].

Принимаем за основу идею из [17], [22], – облет БПЛА-перехватчиком зоны вокруг критически важного объекта на расстоянии R (до 16 км) от индустриального объекта, равной дальности обнаружения БПЛА с помощью РЛС. Предполагаем, что на борту перехватчика размещена малогабаритная РЛС, подобная описанной в [15], - РЛС с синтезированной апертурой антенны массой до 4[кг] и дальностью r=5[км]. В этом случае получаем увеличение дальности обнаружения БПЛА в секторе 1О2, образованном пересечением двух зон обнаружения - дистанционной системой и перехватчиком (Рис.1). Угол сектора α определяется по дальностям r и R обнаружения обеих РЛС: $\alpha=4\cdot\arcsin(r/(2R))$. Дальность обнаружения в секторе α по радиолокационному каналу теперь будет составлять R+r (до 21 км). Дальность идентификации по акустическому каналу теперь определяется акустической зоной действия БПЛА-перехватчика (окружность штрих-пунктирная) и равна $R+r_з$=16[км]+200[м], если установленная на перехватчике акустическая система аналогична описанной в [26]. Дальность обнаружения по оптическому каналу комплексной системой определяется дальностью обнаружения по тому же каналу для БПЛА-перехватчика (штрихованная окружность): $R+r_{оэ}$=16[км]+2[км]=18[км], если на перехватчик установлена оптико-электронная система, аналогичная описанной в [25].

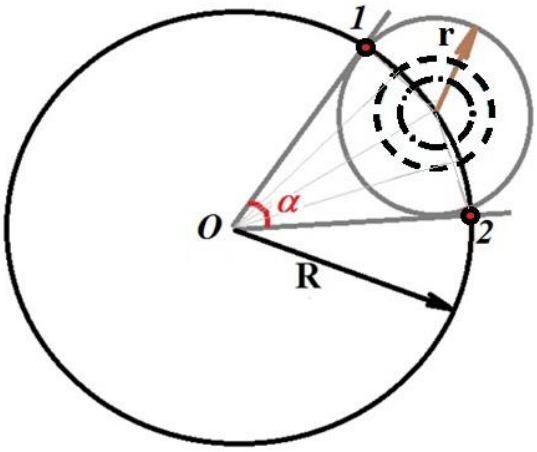


Рис.1. Зоны дальностей обнаружения БПЛА-нарушителей вблизи критически важного индустриального объекта с использованием наземных информационных каналов и каналов, расположенных на БПЛА-перехватчике

Выводы

В статье показана возможность увеличения дистанции обнаружения и идентификации БПЛА-нарушителя вблизи критически важного индустриального объекта путем использования БПЛА-перехватчика, оснащенного малогабаритной РЛС. Это позволит увеличить эффективность работы установленных на перехватчике оптического и акустических каналов идентификации дрона-нарушителля. Показано, что дальность обнаружения по радиолокационному, оптическому и акустическому дистанционным информационным каналам при комплексном их использовании с информационными каналами, расположенными на БПЛА-перехватчике ,становится одного порядка или даже равными между собой.

Список литературы:

1. Ошеев А. В. Современный терроризм: основные тенденции развития и поиск действенных методов борьбы с ним // Актуальные проблемы борьбы с преступлениями и иными правонарушениями. 2018. № 18-1. С. 291-292.

2. Ливанова Л. О., Чикишева В.А. Психология современного терроризма // Colloquium-journal. 2020. № 11-9 (63). С. 22-24.

3. Зайцев А. В., Кичулкин Д. А., Красавцев О. О., Шищенков М. Ю. Многофункциональная малогабаритная цифровая радиолокационная станция “Фасет” обнаружения БПЛА с трёхмерным электронным сканированием пространства // Вестник Ярославского высшего военного училища противовоздушной обороны. 2019. № 3 (6). С. 4-10.

4. V. Kartashov, V. Oleynikov, O. Zubkov, S. Sheiko, "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.

5. Kartashov V.M., Tikhonov V.A., Voronin V.V. and Tymoshenko L.P. Complex model of random signal in problems of acoustic sounding of atmosphere // Telecommunications and Radio Engineering, V. 75, Iss. 20, 2016; pp.1885–1892.

6. Карташов В.М. и др. Обработка сигналов в радиоэлектронных системах дистанционного мониторинга атмосферы. - Харьков: ХНУРЭ, 2014. - 312 с.

7. V. N. Oleynikov, O. V. Zubkov, V. M. Kartashov, I. V. Korytsev, S. I. Babkin, S. A. Sheiko. Investigation of detection and recognition efficiency of small unmanned aerial vehicles on their acoustic emission. Telecommunications and Radio Engineering, V. 78, Issue 9, 2019; pp. 759–770.

8. 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.

9. 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.

10. 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, V. 79, №9. 2020, pp.769–780.

11. Ильин Е. М., Репников Д. А., Савостьянов В. Ю., Самарин О. Ф., Полубехин А. И., Черевко А. Г. Режимы функционирования многофункциональной бортовой РЛС БЛА малой и средней дальности // Вестник СибГУТИ. 2019. № 2.

12. Быстров Н. Е., Жукова И. Н., Кунец Н. А., Реганов В. М., Чеботарёв С. Д. Малогабаритная РЛС X/L-диапазона для обнаружения/сопровождения малоразмерных БПЛА // Вестник Новгородского государственного университета. 2019. № 4 (116). С. 65-71.

13. Литвинов В. С. РЛС бокового обзора для беспилотных летательных аппаратов // Радиотехнические системы: материалы 53-й научной конференции аспирантов, магистрантов и студентов – Минск: БГУИР. 2017. С. 50 - 51.

14. Брайткрайц С. Г., Ильин Е. М., Полубехин А. И., Прищеп Д. В., Юрин А. Д., Хомяков К. А. Проблемы и пути создания радиолокационных систем для БПЛА тактического и оперативно-тактического назначения // Известия ТулГУ. Технические науки. 2018. Вып. 11.

15. Купряшкин И. Ф., Лихачев В. П., Рязанцев Л. Б. Краткий опыт создания и первые результаты практической съемки поверхности малогабаритной РЛС с синтезированием апертуры антенны с борта мультикоптера // Журнал радиоэлектроники. 2019. № 4. 3с.

16. Shepeta A. P., Nenashev V. A. Accuracy characteristics of object location in a two-position system of small onboard radars // Information and Control Systems. 2020. № 2 (105). С. 31-36.

17. Исмаилов Д. А., Синельников В. И., Бровкин Ю. А. Защита РЛС от противорадиолокационных ракет за счет размещения на борту БПЛА дополнительного источника излучения // Аллея науки. 2019. Т. 1. № 5 (32). С. 273-277.

18. Артюшенко В. М., Воловач В. И., Васильев Н. А. Вероятность обнаружения БПЛА системами дистанционного обнаружения // Информационно-технологический вестник. 2017. № 1 (11). С. 25-44.

19. Каляев А. И., Коровин Я. С. Комплекс обнаружения и поражения БПЛА-нарушителей с помощью БПЛА-перехватчиков // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2021. № 3-4 (153-154). С. 101-107.

20. Тищенко А. И., Артыщенко С.В. Математическая модель вероятности обнаружения точечной цели оператором полезной нагрузки оптико-электронной системы БПЛА // Журнал Сибирского федерального университета. Серия: Техника и технологии. 2020. Т. 13. № 3. С. 328-337.

21. Довгаль В. А., Довгаль Д. В. Анализ уязвимостей и угроз безопасности роя дронов с поддержкой Wi-Fi, противостоящего атакам злоумышленников // Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки. 2020. № 3 (266). С. 67-73.

22. Красовский А. Н., Суслова О. А. Облет дронами-квадрокоптерами сельскохозяйственных угодий // Аграрный вестник Урала. 2016. № 1 (143). С. 29-32.

23. Ерин А. А., Хомоненко А. Д. Расчет предельно измеряемой дальности лидара на БПЛА для задач распознавания объектов // Бюллетень результатов научных исследований. 2020. № 2. С. 45-59.

24. Борисов Е. Г., Сидоров Н. М., Морозова Е.В. Устройство перехвата беспилотных летательных аппаратов // Патент на изобретение 2738383 C2, 11.12.2020. Заявка № 2020127599 от 19.08.2020.

25. Черников А. А., Пуртов А. И., Прокофьев И. В. Алгоритм обнаружения беспилотного летательного аппарата на неоднородном фоне // Интерэкспо Гео-Сибирь. 2020. Т. 8. № 2. С. 94-99.

26. Пузанов А. Д., Нефёдов Д. С. Синтез алгоритма обнаружения беспилотных летательных аппаратов по акустическим шумам // Доклады Белорусского государственного университета информатики и радиоэлектроники. 2021. Т. 19. № 2. С. 65-73.

Поступила в редколлегию 04.10.2021

Сведения об авторах:

Карташов Владимир Михайлович – д-р техн. наук, профессор, Харьковский национальный университет радиоэлектроники, заведующий кафедрой медиаинженерии и информационных радиоэлектронных систем, Украина; e-mail: volodymyr.kartashov@nure.ua; ORCID: https://orcid.org/0000-0001-8335-5373

Кизка Валерий Александрович – Харьковский национальний университет радиоелектроники, аспирант кафедры медиаинженерии и информационных радиоэлектронных систем, Украина; e-mail: kizkavaleri@gmail.com; ORCID: https://orcid.org/0000-0003-1007-5295

Тихонов Вячеслав Анатолиевич – д-р физ-мат. наук, Харьковский национальный университет радиоэлектроники, профессор кафедры медиаинженерии и информационных радиоэлектронных систем, Украина; e-mail: vyacheslav.tykhonov@nure.ua; ORCID: https://orcid.org/0000-0002-4618-4787

УДК 621.396.967.2 **DOI: 10.30837/rt.2022.1.208.05**

І.В. СВИД, канд. техн. наук, І.Ю. ВОРГУЛЬ, канд. техн. наук, С.В. СТАРОКОЖЕВ, М.Г. ТКАЧ, О.С. МАЛЬЦЕВ, І.О. ШЕВЦОВ

ПОРІВНЯЛЬНИЙ АНАЛІЗ ЗАВАДОСТІЙКОСТІ КАНАЛУ ПЕРЕДАЧІ ІНФОРМАЦІЇ ВТОРИННИХ РАДІОЛОКАЦІЙНИХ СИСТЕМ

Вступ

Інформаційне забезпечення систем контролю повітряного простору та управління повітряного руху [1] значною мірою забезпечується за рахунок вторинних радіолокаційних систем спостереження повітряного простору [2, 3]. Це обумовлено тим, що вторинні радіолокаційні системи [4, 5] забезпечують як радіолокаційне спостереження за повітряними об'єктами, обладнаними літаковими літакового відповідачами [6], так і забезпечують двосторонню передачу інформації за каналами запиту та відповіді [7, 8], тобто передачу інформації між повітряними об'єктами та наземними вторинними радіолокаційними станціями. До вторинних радіолокаційних систем відносяться вторинні оглядові радіолокатори [9-12] та системи ідентифікації за ознакою «свій-чужий» [13-18]. При цьому слід зазначити, що у теперішній час існують два принципу побудови зазначених інформаційних систем [19]. Перший принцип передбачає єдиний частотний діапазон роботи зазначених інформаційних систем – це 1030 МГц для передачі сигналів запиту, а 1090 МГц для передачі сигналів відповіді. Для другого принципу характерне те, що частотний діапазон роботи систем ідентифікації за ознакою «свій-чужий» використовує передачу сигналів запиту на частоті 1532 МГц, а для передачі сигналів відповіді використовує частотні діапазоні 1452 МГц та 1470 МГц [19].

Однак можливо стверджувати, що розглядаємі вторинні радіолокаційні системи за принципом побудови є двочастотною системою передачі інформації [20, 21]. Вторинні радіолокаційні системи мають режими роботи 1, 2, 3, 4 та 5 (для військового призначення) та A, B, C, D та S (для цивільного призначення). Однак режим 4, в теперішній час не схвалений для використання в військовій сфері, а режим 5 є беззапитальним та більш безпечним. При цьому слід зазначити, що основні концепції режиму S були воєнізовані як режим 5 [22], який являє собою просто криптографічно закодовану версію даних режиму S та ADS-B [23].

При цьому можливо стверджувати, що найбільш вразливим місцем у інформаційних системах, що розглядаються є літаковий відповідач [24-27]. Так, побудова літакового відповідача за принципом одноканальної відкритої системи масового обслуговування з відмовами призводить до повної паралізації останнього при постановці потоків внутрісистемних і навмисних корельованих завад в каналі запиту потрібної інтенсивності. Таким чином, побудова літакового відповідача викликає суттєві недоліки в інформаційній безпеці як його, так і безпеки всієї розглядаємої системи. Це зазначається в значній кількості робіт, зокрема в [28-32]. Крім того, використання єдиної частоти у каналі запиту в розглядаємих радіолокаційних системах призводить до високої щільності сигналів запиту і, як наслідок, до внутрісистемних завад значної інтенсивності [32-35]. Зазначені фактори призводять як до зниження якості обробки сигнальних даних і пропускної спроможності літакового відповідача [36-38], так і до суттєвого зниження завадостійкості [39-43] інформаційних систем спостереження повітряного простору, що розглядаються.

Метою даної роботи є оцінка завадостійкості каналів передачі як сигналів запиту, так і сигналів відповіді вторинних радіолокаційних систем спостереження повітряного простору.

Оцінка завадостійкості каналу передачі сигналів запиту вторинних радіолокаційних систем спостереження повітряного простору

У якості завадостійкості каналу передачі сигналів запиту вторинних радіолокаційних систем спостереження повітряного простору може розглядатися коефіцієнт готовності літакового відповідача [12], що є відносною пропускною здатністю літакового відповідача [32, 33].

Оцінка коефіцієнта готовності літакового відповідача при роботі в режимах ідентифікації повітряних об'єктів розглянуті в роботі [20]. Проведемо оцінку завадостійкості каналів передачі польотної інформації при роботі в режимі управління повітряного руху. Із принципу функціонування існуючих вторинних радіолокаційних систем можливо заключити, що обмін інформацією запитувачі й відповідачі можуть робити, працюючи в неімітостійкому або імітостійкому режимах, а також у режимі запиту й видачі додаткової польотної інформації (бортового номера, висоти польоту, запасу палива) [19]. Потоки сигналів запиту цих режимів утворюють сумарний потік сигналів запиту, що надходить на вхід літакових відповідачів. Крім цього, на вхід літакових відповідачів надходить потік сигналів, випромінених за бічними пелюстками діаграми спрямованості антени запитувача, а також потоки навмисної некорельованої імпульсної завади й несанкціонованих сигналів запиту, сформованих зацікавленою стороною, структура яких подібна до сигналів запиту своїх засобів вторинних радіолокаційних систем. На виході літакового відповідача при цьому формується потік сигналів відповіді на запити в імітостійкому і неімітостійкому режимах і потік сигналів відповіді польотної інформації, а на виході запитувача потік сигналів виявлення повітряних об'єктів й польотної інформації.

Виходячи з вищесказаного, можна зробити висновок, що сумарний потік сигналів запиту, що надходять на вхід літакового відповідача можна представити у вигляді наступного виразу

$$\lambda_{pi} = \sum_{i=1}^{I} \lambda_i + \sum_{j=1}^{J} \lambda_j + \lambda_0 + \sum_{k=1}^{K} \lambda_k \ , \qquad (1)$$

де λ_i – інтенсивність потоку сигналів запиту, які випромінюють свої вторинні радіолокаційні системи за основною пелюсткою діаграми спрямованості антени запитувача (загальна кількість таких вторинних радіолокаційних систем I); λ_j – інтенсивність потоку сигналів запиту, які випромінюють сусідні вторинні радіолокаційні системи за бічними пелюстками діаграми спрямованості антени запитувача (загальна кількість таких систем J); λ_0 – інтенсивність некорельованих імпульсних завад; λ_k – інтенсивність потоку сигналів запиту несанкціонованого використання літакових відповідачів зацікавленою стороною (загальна кількість запитувачів зацікавленою стороною K).

Проведемо дослідження завадостійкості літакового відповідача вторинних радіолокаційних систем у вигляді відкритої одноканальної системи масового обслуговування з відмовами при спільній дії на його вході потоку сигналів запиту і потоку сигналів запиту, навмисних корельованих і некорельованих завад [19, 24].

При цьому слід зазначити, що частотний діапазон роботи вторинних радіолокаційних систем відомий і перебудові не підлягає. Це дозволяє іншій стороні легко ставити навмисні завади вторинним радіолокаційним системам з метою отримання несанкціонованого доступу до інформації літакового відповідача, а також для повної паралізації літакового відповідача.

Найбільш ефективною завадою для подавлення вторинних радіолокаційних систем є навмисна корельована завада, тобто завада аналогічна за структурою сигналам запиту своїх запитувачів. Все це приводить до небажаних явищ роботи літакового відповідача вторинних радіолокаційних систем.

Розглянемо вплив потоку сигналів запиту і навмисних корельованих і некорельованих завад на коефіцієнт готовності літакового відповідача вторинних радіолокаційних систем при передачі польотної інформації в режимі управління повітряного руху. При дослідженні коефіцієнта готовності літакового відповідача будемо також ураховувати ймовірності обслуговування сигналів запиту. Як математичну модель потоку завад та сигналів будемо розглядати розподіл Пуассона.

При дії на вході літакового відповідача одночасно завад та потоку сигналів запиту будуть спостерігатися наступні небажані явища, які приводять до неможливості формування сигналів відповіді:

- подавлення кодів запиту і запитів польотної інформації даного запитувача через появу випереджальних кодів запиту своїх запитувачів, а також запитувачів зацікавленої сторони, що несанкціоновано використовують відповідач;
- високочастотне подавлення імпульсів кодів запиту даного запитувача при збігу за часом імпульсів завади й потоку сигналів запиту в несприятливих фазових співвідношеннях;
- подавлення кодів запиту даного запитувача через появу випереджальних хибних кодів запиту, що утворяться в результаті взаємодії першого імпульсу коду запиту даного запитувача з випереджальними (на базу коду) імпульсами завад або потоку сигналів запиту, що викликає випромінювання коду відповіді або спрацьовування схеми подавлення бокових пелюсток (фіктивна тривога другого роду);
- подавлення запиту в результаті інерційності схем вхідних формувачів дешифратора й обмеження завантаження літакового відповідача.

Визначимо ймовірності цих подій у припущенні, що імпульси завади й потоку сигналів запиту діють на запитальні коди даного запитувача незалежно друг від друга.

Будемо враховувати, що на вході літакового відповідача присутні:

- навмисна некорельована завада із сумарною інтенсивністю λ_0;
- потік сигналів запиту, що викликає випромінювання кодів відповіді в імітостійкому та неімітостійкому режимах і режимі передачі польотної інформації λ_1;
- потік сигналів запиту, що викликає спрацьовування схеми подавлення бокових пелюсток, інтенсивністю λ_2.

При цьому будемо вважати, що тривалість імпульсів потоків завади й потоку сигналів запиту однакова й дорівнює тривалості імпульсів корисного сигналу τ_0.

Спільна дія завад та потоку сигналів запиту приводить до високочастотного подавлення окремих імпульсів потоку сигналів запиту при несприятливих фазових співвідношеннях, у результаті чого зменшується інтенсивність потоку сигналів запиту. Імовірність того, що хоча б один імпульс завади збіжиться з імпульсом потоку сигналів запиту і подавить його можна визначити з наступного співвідношення

$$P_p = \gamma[1 - \exp(-\lambda_0 \tau_0)]. \tag{2}$$

Виходячи із цього, потік кодів запиту з урахуванням високочастотного подавлення, що викликає випромінювання кодів відповіді, може бути визначений як:

$$\lambda_{11} = \lambda_1 (1 - P_p)^n, \tag{3}$$

а зумовлюючих спрацьовування схеми подавлення бокових пелюсток, можна визначений як:

$$\lambda_{12} = \lambda_2 (1 - P_p)^n. \tag{4}$$

Як вказувалося вище, запитальний сигнал не може бути обслугований у той момент часу коли, відповідач зайнятий обслуговуванням іншого сигналу запиту, отже, імовірність подавлення або неможливості обслуговування чергового запиту буде визначатися часом паралізації літакового відповідача зайнятого обслуговуванням іншого запитального сигналу. Час паралізації літакового відповідача буде залежати від режимів роботи системи запиту-відповіді.

Імовірності того, що хоча б один код запиту потрапить у випереджальний інтервал і подавить запит даного запитувача за рахунок часу паралізації літакового відповідача t_1 й t_2 при випромінюванні коду відповіді, визначаються відповідно:

- при утворені із завад хибного коду запиту (хибних кодів запиту) неімітостійкого режиму

$$P_{11} = 1 - \exp(-\lambda p \cdot t_1), \tag{5}$$

де t_1 – час паралізації літакового відповідача при обслуговуванні коду запиту неімітостійкого режиму,

- при утворенні із завад хибних кодів запиту імітостійкого режиму

$$P_{12} = 1 - \exp(-\lambda_p \cdot t_2), \tag{6}$$

де λ_p – середнє число хибних кодів запиту, що утворилися з завад і викликають випромінювання коду відповіді, визначаємо як [19]

$$\lambda_p = n\lambda_0^{\,n}(\tau_0 - \tau_s)^{n-1}, \tag{7}$$

де n – кількість імпульсів коду запиту (значність коду); τ_s – задана величина селекції імпульсів за тривалістю; t_2 – час паралізації літакового відповідача при обслуговуванні коду сигналу запиту імітостійкого режиму;

- при впливі потоку сигналів запиту неімітостійкого режиму

$$P_{13} = 1 - \exp(-q_1 \cdot \lambda_{11} \cdot t_1), \tag{8}$$

- при впливі потоку сигналів запиту імітостійкого режиму

$$P_{14} = 1 - \exp(-q_2 \cdot \lambda_{11} \cdot t_2), \tag{9}$$

де q – коефіцієнт, що характеризує внесок у загальний потік сигналів запиту кодів запиту відповідного режиму.

Сумарна ймовірність того, що хоча б один сигнал запиту потрапить у випереджальний інтервал і подавить запит даного запитувача за рахунок часу паралізації літакового відповідача t_1, при випромінюванні сигналу відповіді в неімітостійкому режимі, визначається як:

$$P_{1n} = 1 - (1 - P_{11})(1 - P_{13}). \tag{10}$$

Сумарна ймовірність того, що хоча б один сигнал запиту потрапить у випереджальний інтервал і подавить запит даного запитувача за рахунок часу паралізації літакового відповідача t_2 при випромінюванні сигналу відповіді в імітостойкому режимі, визначається як:

$$P_{1i} = 1 - (1 - P_{12})(1 - P_{14}). \tag{11}$$

Імовірності того, що хоча б один сигнал запиту потрапить у випереджальний інтервал і подавить сигнал запиту даного запитувача за рахунок часу паралізації $t_3 \approx t_4$ при спрацьовуванні схеми подавлення бокових пелюсток, визначаються відповідно:

- при утворенні із завад хибних кодів запиту неімітостійкого режиму

$$P_{21} = 1 - \exp(-\lambda p \cdot t_3), \tag{12}$$

- при утворенні з завад хибних кодів запиту імітостійкого режиму

$$P_{22} = 1 - \exp(-\lambda p \cdot t_4), \tag{13}$$

- при впливі потоку сигналів запиту неімітостійкого режиму

$$P_{23} = 1 - \exp(-q_1 \cdot \lambda_{12} \cdot t_3), \tag{14}$$

- при впливі потоку сигналів запиту імітостійкого режиму

$$P_{24} = 1 - \exp(-q_2 \cdot \lambda_{12} \cdot t_4), \tag{15}$$

де t_3, t_4 – час паралізації літакового відповідача при спрацьовуванні схеми подавлення бокових пелюсток у неімітостійкому та імітостійкому режимах.

Сумарна ймовірність подавлення кодів запиту даного запитувача, зумовлена часом паралізації літакового відповідача при спрацьовуванні схеми подавлення бокових пелюсток становить:

- у неімітостійкому режимі

$$P_{2n} = 1-(1-P_{21})(1-P_{23}), \tag{16}$$

- в імітостійкому режимі

$$P_{2i} = 1-(1-P_{22})(1-P_{24}). \tag{17}$$

Імовірності того, що хоча б один запит польотної інформації потрапить у випереджальний інтервал і подавить запит даного запитувача за рахунок часу t_5 при передачі польотної інформації, визначаються відповідно:

- при утворенні хибних кодів запиту із завад

$$P_{31} = 1-\exp(-\lambda_p \cdot t_5), \tag{18}$$

- при впливі потоку сигналів запит

$$P_{32} = 1-\exp(-(q_3 \cdot \lambda_{11}) \cdot t_5). \tag{19}$$

Сумарна ймовірність подавлення кодів запиту даного запитувача за рахунок часу паралізації літакового відповідача при передачі польотної інформації визначається як:

$$P_{31} = 1-\exp(-\lambda_p \cdot t_5). \tag{20}$$

Імовірність того, що хоча б один імпульс із потоку навмисної некорельованої завади й потоку сигналів запиту накладеться на імпульс коду запиту даного запитувача й подавить його, становить

$$P_{10} = \gamma[1-\exp(-\lambda_c \tau_0)], \tag{21}$$

а величина сумарного потоку визначається як

$$\lambda_c = \lambda_{11} + \lambda_{12} + \lambda_0. \tag{22}$$

З урахуванням n-імпульсів коду запиту ймовірність подавлення сигналу запиту буде становити

$$P_4 = 1-(1-P_{10})^n. \tag{23}$$

Імовірність подавлення кодів запиту даного запитувача через появу випереджальних хибних кодів запиту, що утворяться в результаті взаємодії першого імпульсу коду запиту розглядаємого запитувача з випереджальними імпульсами завад або потоку сигналів запиту та призведе до випромінювання сигналу відповіді або спрацьовування схеми подавлення бокових пелюсток, визначається як:

$$P_5 = (1-P_{10})^n[1-(1-P_{10})^{n-1}], \tag{24}$$

другий співмножник у цьому виразі враховує можливі ситуації утворення хибних випереджальних кодів запиту: n-імпульсів коду сигналу запиту, що приводять до випромінювання сигналу відповіді; $(n-1)$-імпульсів коду сигналу запиту, що приводять до випромінювання сигналу відповіді або спрацьовуванню схеми подавлення бокових пелюсток.

Імовірність появи на позиції сигналу помилкового імпульсу подавлення, що утворився із завад, визначається як

$$P_6 = (1 - P_{10})^n P_{01}^{n-1}, \tag{25}$$

де в свою чергу імовірність P_{01} можливо визначити як

$$P_{01} = 1 - \exp(-\lambda_0 \cdot \tau_0). \tag{26}$$

Імовірність подавлення кодів запиту внаслідок інерційності вхідних формувачів літакового відповідача може бути визначена як

$$P_7 = 1 - (1 - P_f)^n, \tag{27}$$

де P_f – імовірність подавлення одиночного імпульсу коду запиту з-за інерційності формувача.

Імовірність того, що хоча б один імпульс завади потрапить у випереджальний небезпечний інтервал і подавить імпульс корисного сигналу, становить

$$P_f = 1 - \exp(-\lambda_c \tau_f). \tag{28}$$

Імовірність передачі сигналу відповіді польотної інформації на запит даного запитувача буде відповідно складати

$$P_0 = \prod_{i=1}^{7} (1 - P_i). \tag{29}$$

Імовірність обслуговування сигналів запиту польотної інформації (коефіцієнт готовності літакового відповідача чи відносна пропускна спроможність літакового відповідача) можна визначити із наступного виразу:

$$P_{0i} = P_0 / g, \tag{30}$$

де $g = 2{,}8...3{,}2$ – коефіцієнт розрядки літакових відповідачів, що використовується для зменшення імовірності накладення сигналів відповіді польотної інформації від повітряних об'єктів, що знаходяться на одному азимуті з-за значної часової бази сигналів відповіді. Оцінку коефіцієнту готовності літакових відповідачів у режимі передачі польотної інформації представлено на рис. 1 та рис. 2.

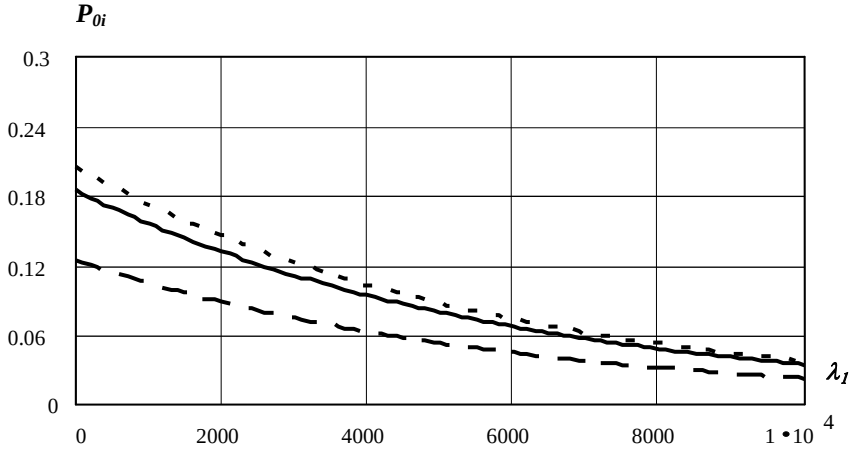


Рис. 1. Коефіцієнт готовності літакового відповідача при передачі польотної інформації в режимі управління повітряного руху q_1=0,5; q_2=0,4; q_3=0,1

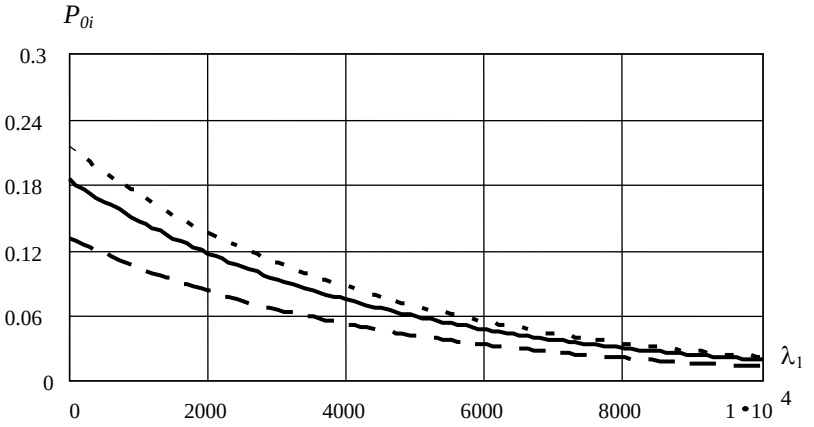


Рис. 2. Коефіцієнт готовності літакового відповідача при передачі польотної інформації в режимі управління повітряного руху q_1=0,3; q_2=0,4; q_3=0,3

Значення коефіцієнта готовності літакового відповідача були отримані для інтенсивності потоку сигналів запиту, що викликає спрацьовування схеми подавлення бокових пелюсток, у п'ять разів більшою за інтенсивність потоку сигналів запиту за основними пелюстками діаграми спрямованості антени, що приводить до випромінювання сигналів відповіді.

Для розрахунків були обрані наступні інтенсивності завади, що діють в каналі запиту: $\lambda_0 = 20 \cdot 10^3$, $\lambda_0 = 50 \cdot 10^3$, $\lambda_0 = 100 \cdot 10^3$. Крім того, ураховувалось те, що загальний вхідний потік сигналів запиту складається з сумарного потоку неімітостійкого режиму (q_1), імітостійкого режиму (q_2) та запиту польотної інформації - (q_3).

Як видно з представлених залежностей імовірність передачі польотної інформації на конкретний сигналів запиту є незначною. При збільшенні числа сигналів запиту польотної інформації в загальному потоці сигналів запиту імовірність їхнього обслуговування зменшується.

Оцінка завадостійкості каналу відповіді для режиму управління повітряного руху вторинних радіолокаційних систем спостереження повітряного простору

Як видно з отриманих результатів, коефіцієнт готовності літакових відповідачів в режимі передачі польотної інформації виявляється незначним. У зв'язку із цим розглянемо його вплив на загальну імовірність отримання польотної інформації з урахуванням обробки її в наземній апаратурі та наявності у каналі відповіді навмисних некорельованих (хаотично імпульсних) завад.

У каналі відповіді вторинних радіолокаційних систем інформаційний код управління повітряного руху [19], при передачі польотної інформації передається кодованими сигналами координатної мітки й польотної інформації (45-імпульсний позиційний код). До складу кодової посилки відповіді польотної інформації входять:

- 2-імпульсний код координатної мітки;
- 3-імпульсний код ознаки переданої інформації (бортового номера, висоти польоту, запасу палива);
- 20 двійкових розрядів польотної інформації.

Таки чином, при впливі завад у каналі відповіді, можуть виникати спотворення польотної інформації, що передається внаслідок подавлення частини імпульсів сигналу відповіді. Для отримання польотної інформації необхідною умовою є декодування імпульсів синхрогрупи, що складається з 2-х імпульсів координатного коду й 3-х імпульсів ознаки польотної інформації, що передається. У зв'язку з цим визначимо імовірність декодування й проходження імпульсів синхрогрупи з урахуванням подавлення хоча б одного імпульсу внаслідок впливу навмисної некорельованої завади.

Для каналу відповіді імовірність високочастотного подавлення імпульсу корисного сигналу навмисною некорельованою завадою за розподілом Пуассона може бути визначена у відповідності за наступним математичним виразом

$$P_{10} = \gamma[1 - \exp(-\lambda_0 \tau_0)]. \tag{31}$$

Імовірність вірного прийому імпульсів синхрогрупи з урахуванням можливості подавлення хоча б одного з них буде визначатися як

$$P_{pi} = 1 - \sum_{i=1}^{n} C_n^i (1 - P_{10})^i P_{10}^{n-i}, \tag{32}$$

де n – число часових позицій імпульсів синхрогрупи; i – число часових позицій, які можуть бути подавлені завадою; C_n^i – число сполучень із n по i.

З урахуванням коефіцієнту готовності літакових відповідачів імовірність проходження декількох видів польотної інформації при отриманні пачки сигналів відповіді можна визначити як

$$P_{pi1} = \left[\sum_{i=1}^{M} C_M^i (P_{oi} P_{pi})^i (1 - P_{oi} P_{pi})^{M-i} \right]^V, \tag{33}$$

де M – число імпульсів у пачці; V – число видів польотної інформації.

Залежності, отримані відповідно до виразу (33), представлені на рис. 3 і рис. 4. Як видно з представлених залежностей, імовірність отримання польотної інформації режиму управління повітряного руху є незначною. При зменшенні кількості кодів відповіді у пачці імовірність отримання польотної інформації зменшується.

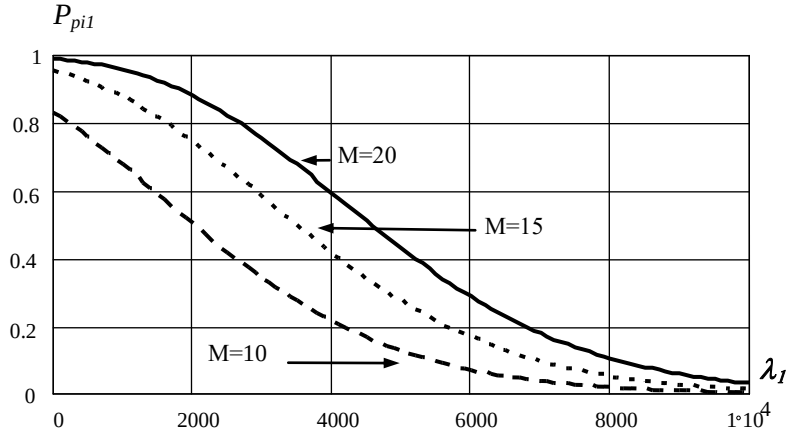


Рис. 3. Імовірність отримання польотної інформації режиму управління повітряного руху при $\lambda_0 = 20 \cdot 10^3$ у каналі запиту

Розрахунки зроблені для $V = 3$, а так само з урахуванням імовірності обслуговування коду запиту польотної інформації, отриманого вище та інтенсивності навмисної некорельованої завади у каналі відповіді $\lambda_0 = 50 \cdot 10^3$.

З проведених досліджень видно, що значний час паралізації літакового відповідача й наявність розрядки при обслуговуванні коду запиту польотної інформації веде до істотного зниження коефіцієнту готовності літакових відповідачів в умовах високої щільності потоку сигналів запиту і завад, що у свою чергу впливає на імовірності отримання польотної інформації на наземній апаратурі.

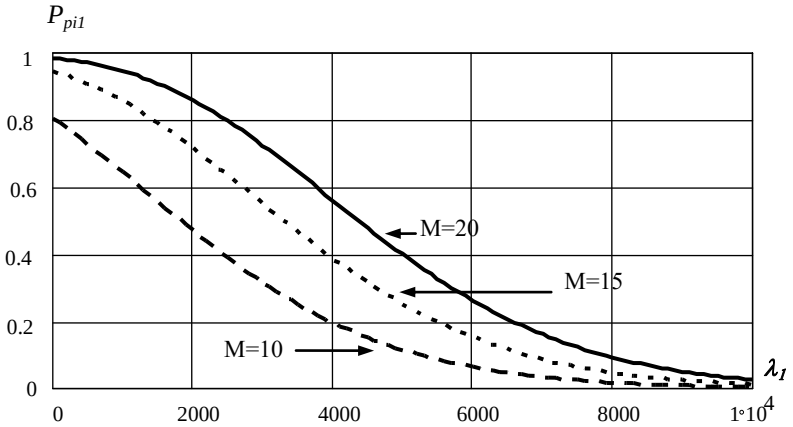


Рис. 4. Імовірність отримання польотної інформації режиму управління повітряного руху при $\lambda_0=50\cdot10^3$ у каналі запиту

Висновки

За результатами проведеного дослідження можна зробити наступні висновки: розроблено методику оцінки завадостійкості каналів передачі польотної інформації в існуючих запитальних радіолокаційних системах спостереження повітряного простору у режимі управління повітряного руху, яка містить оцінку завадостійкості каналу запиту при дії потоків сигналів запиту різних режимів сусідніх запитальних радіолокаційних систем, випроменених як за основними пелюстками діаграми спрямованості антени запитувача, так і за бічним, а також потоку навмисних корельованих і некорельованих завад, а також і оцінку завадостійкості каналу відповіді (передачі польотної інформації) з урахуванням дії у каналі відповіді потоків сигналів відповіді та потоків навмисних некорельованих завад.

Як показали розрахунки, за розробленою методикою, імовірність отримання польотної інформації при дії в каналі запиту корельованих завад інтенсивністю 10 кГц для режиму управління повітряного руху становить усього 0,05 при пачці сигналів відповіді що дорівнює 20.

Показано, що принцип побудови літакового відповідача (відкрита система масового обслуговування з відмовами) та принцип обслуговування сигналів запиту передачі інформації (перший прийнятий) не дозволяють забезпечити допустимі ймовірності отримання польотної інформації.

Наведені розрахунки показують, що при модернізації запитальних систем радіолокаційного спостереження повітряного простору можливо збільшити розрядність передачі польотної інформації з борта повітряного об’єкта на наземні пункти управління.

Список літератури:

1. G. Benelli, D. Giuli, E. Mese and S. Pardini, "Characterization of ATC environment for performance evaluation of modern SSR systems", 29th IEEE Vehicular Technology Conference, 1979. doi: 10.1109/vtc.1979.1622720.

2. Обод И.И. Помехоустойчивые системы вторичной радиолокации. М.: ЦИНТ, 1998. 118 с.

3. Ткачев В.В., Даник Ю.Г., Жуков С.А., Обод І.І., Романенко І.О. Комплексне інформаційне забезпечення систем управління польотами авіації та протиповітряної оборони. Київ: МОУ, 2004. 342 с.

4. E. Kim and K. Sivits, "Blended secondary surveillance radar solutions to improve air traffic surveillance", Aerospace Science and Technology, vol. 45, pp. 203-208, 2015. doi: 10.1016/j.ast.2015.05.018.

5. I. Svyd, I. Obod, O. Maltsev, M. Tkach, S. Starokozhev, A. Hlushchenko, V. Chumak, "Method for increasing noise immunity of radar "friend or foe" identification systems under the action of intentional correlated interference", Radiotekhnika, no. 205, pp. 154-160, 2021. doi: 10.30837/rt.2021.2.205.16.

6. M. Strohmeier, "Large-Scale Analysis of Aircraft Transponder Data", IEEE Aerospace and Electronic Systems Magazine, vol. 32, no. 1, pp. 42-44, 2017. doi: 10.1109/maes.2017.160149.

7. І. Обод, О. Стрельницький, "Захист інформації в мережі систем спостереження повітряного простору", Системи обробки інформації, № 2(139), С. 47-49, 2016.

8. І. Обод, В. Шевцова, "Методи підвищення швидкості передачі запитальних систем передачі інформації", Системи обробки інформації, № 4(111), С. 23-26, 2013.

9. G. Jiang, Y. Fan and H. Yuan, "Assessing the Capacity of Air Traffic Control Secondary Surveillance Radar System", 2019 Cross Strait Quad-Regional Radio Science and Wireless Technology Conference (CSQRWC), 2019. doi: 10.1109/csqrwc.2019.8799146.

10. I. Svyd, I. Obod, O. Maltsev, I. Shtykh, G. Zavolodko and G. Maistrenko, "Model and Method for Request Signals Processing of Secondary Surveillance Radar", 2019 IEEE 15th International Conference on the Experience of Designing and Application of CAD Systems (CADSM), 2019. doi: 10.1109/cadsm.2019.8779347.

11. I. Svyd, I. Obod, O. Maltsev and A. Hlushchenko, "Secondary Surveillance Radar Response Channel Information Security Improvement Method", 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), 2020. doi: 10.1109/dessert50317.2020.9125018.

12. I. Obod, I. Svyd, G. Zavolodko, O. Maltsev, B. Bakumenko and V. Chumak, "Assessing SSR Relative Data Capacity", 2021 IEEE 3rd Ukraine Conference on Electrical and Computer Engineering (UKRCON), 2021. doi: 10.1109/ukrcon53503.2021.9575971.

13. Обод І.І., Стрельницький О.О., Андрусевич В.А. Інформаційна мережа систем спостереження повітряного простору. Харків: ХНУРЕ, 2015. 270 с.

14. I. Svyd, I. Obod, O. Maltsev, O. Strelnytskyi, O. Zubkov and G. Zavolodko, "Method of Increasing the Identification Friend or Foe Systems Information Security", 2019 3rd International Conference on Advanced Information and Communications Technologies (AICT), 2019. doi: 10.1109/aiact.2019.8847853.

15. I. Svyd, I. Obod, O. Maltsev, I. Shtykh and G. Zavolodko, "Model and Method for Detecting Request Signals in Identification Friend or Foe Systems", 2019 IEEE 15th International Conference on the Experience of Designing and Application of CAD Systems (CADSM), 2019. doi: 10.1109/cadsm.2019.8779322.

16. V. Semenets, I. Svyd, I. Obod, O. Maltsev and M. Tkach, "Quality Assessment of Measuring the Coordinates of Airborne Objects with a Secondary Surveillance Radar", Data-Centric Business and Applications, pp. 105-125, 2021. doi: 10.1007/978-3-030-71892-3_5.

17. P. Poornima, B. Roja Reddy and B. Anantha Murthy, "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), 2018. doi: 10.1109/rteict42901.2018.9012646.

18. X. Du, K. Liao and X. Shen, "Secondary Radar Signal Processing Based on Deep Residual Separable Neural Network", 2020 IEEE International Conference on Power, Intelligent Computing and Systems (ICPICS), 2020. doi: 10.1109/icpics50287.2020.9202372.

19. Маляренко А.С. Системы вторичной радиолокации для управления воздушным движением и государственного радиолокационного опознавания [Справочник], ХУПС, 2007, 78 с.

20. Б. Бакуменко, І. Обод. "Завадозахищеність запитувальних радіотехнічних систем", Системи озброєння і військова техніка, № 2(6), С. 26-28, 2006.

21. I. Obod, "Integrated Coordinate-and-Time Support for the Address Inquiry in the Secondary Radar Systems", Telecommunications and Radio Engineering, vol. 53, no. 3, pp. 54-56, 1999. doi: 10.1615/telecomradeng.v53.i3.100.

22. M. Strohmeier, V. Lenders and I. Martinovic, "On the Security of the Automatic Dependent Surveillance-Broadcast Protocol", IEEE Communications Surveys & Tutorials, vol. 17, no. 2, pp. 1066-1087, 2015. doi: 10.1109/comst.2014.2365951.

23. L. Kenney, J. Dietrich and J. Woodall, "Secure ATC surveillance for military applications", MILCOM 2008 - 2008 IEEE Military Communications Conference, 2008. doi: 10.1109/milcom.2008.4753368.

24. І. Обод, О. Стрельницький, В. Андрусевич, "Методи підвищення якості інформаційного забезпечення системами спостереження повітряного простору", Системи обробки інформації, № 4(120), С. 53-55, 2014.

25. І. Обод, О. Стрельницький, "Інформаційна безпека інформаційної мережі систем спостереження повітряного простору", Системи обробки інформації, № 9(134), С. 96-98, 2015.

26. I. Obod, I. Svyd, O. Maltsev and B. Bakumenko, "Comparative Analysis of Noise Immunity Systems Identification Friend or Foe", 2020 IEEE 40th International Conference on Electronics and Nanotechnology (ELNANO), 2020. doi: 10.1109/elnano50318.2020.9088856.

27. M. Leonardi and F. Gerardi, "Aircraft Mode S Transponder Fingerprinting for Intrusion Detection", Aerospace, vol. 7, no. 3, p. 30, 2020. Available: 10.3390/aerospace7030030.

28. S. Zhironkin, S. Bliznyuk and A. Kuchin, "Jamming Resistance of the Inbound Channel of an Identification System with Broadband Signals and Error Control Codes in the Conditions of Pulse Noise and Intra-System Jamming", Journal of Siberian Federal University. Engineering & Technologies, pp. 673-682, 2019. doi: 10.17516/1999-494x-0166.

29. V. Andrusevich and I. Obod, "Assessment of the Quality of Information Support by Air Radar Surveillance Systems", Advanced Information Systems, vol. 5, no. 2, pp. 78-82, 2021. doi: 10.20998/2522-9052.2021.2.10.

30. І. Обод, О. Стрельницький, В. Андрусевич, "Порівняльний аналіз двох методів обробки сигналів відповіді запитальних систем спостереження", Системи обробки інформації, № 1(117), С. 41-43, 2014.

31. T. Otsuyama, J. Honda, J. Naganawa and H. Miyazaki, "Analysis of signal environment on 1030/1090MHz aeronautical surveillance systems", 2018 IEEE International Symposium on Electromagnetic Compatibility and 2018

IEEE Asia-Pacific Symposium on Electromagnetic Compatibility (EMC/APEMC), 2018. doi: 10.1109/isemc.2018.8394048.

32. І.І. Обод, В.В. Шевцова, "Пропускна спроможність відповідачів запитальних систем передачі польотної інформації", Системи обробки інформації, № 1(108), 2013, С. 105-108.

33. І. Обод, В. Шевцова, "Відносна пропускна спроможність запитальних систем передачі інформації системи контроля повітряного простору", Системи обробки інформації, № 2(109), С. 74-76, 2013.

34. I. Svyd, I. Obod and O. Maltsev, "Interference Immunity Assessment Identification Friend or Foe Systems", Data-Centric Business and Applications, pp. 287-306, 2021. doi: 10.1007/978-3-030-71892-3_12.

35. V. Zhyrnov, S. Solonskaya and V. Zarytskyi, "Method for dealing with non-stationary natural and simulating interference in intellectual surveillance radars", Radiotekhnika, no. 206, pp. 115-121, 2021. doi: 10.30837/rt.2021.3.206.10.

36. N. Kuzmenko and I. Ostroumov, "Performance Analysis of Positioning System by Navigational Aids in Three Dimensional Space," 2018 IEEE First International Conference on System Analysis & Intelligent Computing (SAIC), 2018, pp. 1-4, doi: 10.1109/SAIC.2018.8516790.

37. R. Burczyk, K. Cwalina, M. Gajewska, J. Magiera, P. Rajchowski, J. Sadowski, J. Stefanski, "Voice Multilateration System", Sensors, vol. 21, no. 11, p. 3890, 2021. doi: 10.3390/s21113890.

38. И. Обод, А. Шматков, А. Михайлин, "Сравнительный анализ помехоустойчивости способов передачи полетной информации в системах вторичной радиолокации", Вестник ХГПУ, № 125, С. 3-6, 2000.

39. М. Ткач, «Оцінка відносної пропускної здатності літакових відповідачів вторинних радіолокаційних систем спостереження повітряного простору», Радіотехніка, № 207, 2021, С. 123-131. doi: 10.30837/rt.2021.4.207.13.

40. D. Margaria, B. Motella, M. Anghileri, J. -J. Floch, I. Fernandez-Hernandez and M. Paonni, "Signal Structure-Based Authentication for Civil GNSSs: Recent Solutions and Perspectives," in IEEE Signal Processing Magazine, vol. 34, no. 5, pp. 27-37, Sept. 2017, doi: 10.1109/MSP.2017.2715898.

41. J. Guo and X. Zhang, "DME pulse interference mitigation for airborne BDS and flight test results", Advances in Space Research, vol. 63, no. 9, pp. 3043-3052, 2019. doi: 10.1016/j.asr.2018.05.012.

42. R. Morales-Ferre, P. Richter, E. Falletti, A. de la Fuente and E. S. Lohan, "A Survey on Coping With Intentional Interference in Satellite Navigation for Manned and Unmanned Aircraft," in IEEE Communications Surveys & Tutorials, vol. 22, no. 1, pp. 249-291, Firstquarter 2020, doi: 10.1109/COMST.2019.2949178.

43. W. Song, P. Ju and A. Jin, Protocol Design and Analysis for Cooperative Wireless Networks. Cham: Springer International Publishing, 2017.

Надійшла до редколегії 02.03.2022

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

Vorgul Irena Yu. – PhD, Associate Professor, Lecturer/Senior Laboratory Demonstrator, University of St Andrews, United Kingdom; email: iv4@st-andrews.ac.uk; ORCID: https://orcid.org/0000-0002-7335-047X

Старокожев Святослав Валерійович – аспірант кафедри мікропроцесорних технологій і систем, Харківський національний університет радіоелектроніки, Україна; email: sviatoslav.starokozhev@nure.ua; ORCID: https://orcid.org/0000-0002-1600-1337

Ткач Марія Геннадіївна – аспірант кафедри мікропроцесорних технологій і систем, Харківський національний університет радіоелектроніки, Україна; email: mariia.zavorotna@nure.ua; ORCID: http://orcid.org/0000-0002-4248-7633

Мальцев Олександр Сергійович – старший науковий співробітник кафедри мікропроцесорних технологій і систем, Харківський національний університет радіоелектроніки, Україна; email: aleksandr.maltsev@nure.ua; ORCID: http://orcid.org/0000-0003-1520-9280

Шевцов Іван Олександрович – асистент кафедри мікропроцесорних технологій і систем, Харківський національний університет радіоелектроніки, Україна; email: ivan.shevtsov@nure.ua; ORCID: https://orcid.org/0000-0003-0597-1589

TELECOMMUNICATIONS MEAS
ЗАСОБИ ТЕЛЕКОМУНІКАЦІЙ

УДК 621.396.004 **DOI:10.30837/rt.2022.1.208.06**

Л.О. ТОКАР, канд. техн. наук

ОСОБЛИВОСТІ ПОБУДОВИ ВІРТУАЛЬНИХ АТС

Вступ

Важливим рішенням для будь-якої корпоративної компанії або офісної структури є вибір якісного та дешевого телефонного зв'язку. На ринку пропонуються готові рішення щодо вибору хмарних АТС, які вимагають додаткові витрати.

Хмарна АТС дає можливість використання багатоканальних номерів, пропонуючи інтелектуальну переадресацію дзвінків, гнучку аналітику, можливість запису й зберігання інформації на надійному зовнішньому сервері. Крім того, надає безліч інших функцій: інтерактивне голосове меню, повідомлення про пропущені виклики, голосова пошта, електронний факс й т.і. Але основна її перевага - це висока якість телефонії, що не досяжне за допомогою підключення стільникового й аналогового зв'язку.

Хмарна АТС дозволяє економити і отримувати телефонію високої якості. Основними вигодами виступають розширення функціоналу, зручність у використанні при істотному скороченні постійних матеріальних витрат. До її плюсів відноситься високий рівень технологічності. Хмарна АТС забезпечує компанії більш високоефективним зв'язком, комфортним управлінням, якісним голосовим каналом, а головне - є недорогою в порівнянні з аналоговою АТС.

Виходячи з того, що впровадження класичної АТС займає тривалий час, вибір рішення на основі IP-телефонії очевидний. На відміну від апаратної міні-АТС, масштабування хмарної АТС виконується в міру необхідності, простим додаванням віртуалізованих ресурсів. Крім того, всі технічні проблеми залишаються на стороні провайдера, а компанія отримує вже готову послугу.

Використання віртуальної АТС не як додаткового сервісу, а як окремої конфігурації виділеного сервера, поєднуючи всі переваги хмарних технологій і систем віртуалізації, дасть можливість отримання гнучкості і повної доступності системи для налаштувань, це і визначає актуальність даної публікації. В роботі проведено аналіз технологій віртуалізації в залежності від складності виконання та області застосування, показано їх переваги та недоліки. Розглянуто конфігурацію налаштування середовища віртуалізації на прикладі Asterisk. Проведено дослідження для порівняння контейнерної віртуалізації з гіпервізорною для визначення економії оперативної пам'яті у хост-системі.

Основна частина

Одним із способів перекладу інфраструктури комп'ютера на динамічний рівень є віртуалізація. Технології віртуалізації набирають більшу популярність, що є слідством росту обчислювальних потужностей комп'ютерів. Віртуалізація являє собою програмну технологію, що дає можливість одночасно виконувати декілька ОС і додатків на одному сервері. Модель віртуалізації показано на рис. 1 [1].

За допомогою віртуалізації створюється віртуальний образ операційної системи комп'ютера, обчислювальної мережі або накопичувального пристрою. Віртуальна машина співіснує «всередині» комп'ютера зі звичайною операційною системою. В результаті розвитку технологій віртуалізації, з'являються багатоядерні процесори, зростає пропускна здатність інтерфейсів комп'ютерів, а також ємність та швидкодія систем зберігання даних [2].

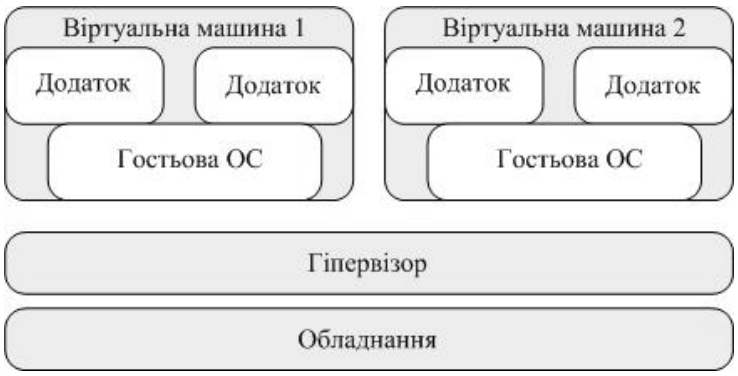


Рис. 1. Модель віртуалізації

Новий аспект віртуалізації було названо командною або бінарною віртуализацією. В цьому випадку віртуальні команди переводяться (транслюються) на фізичні команди основного обладнання. Зазвичай це відбувається динамічно. Якщо відбувається розгалуження, то новий сегмент коду забирається і перекладається [3].

Для організації віртуалізації існує декілька способів, за допомогою яких досягаються однакові результати через різні рівні абстракції. У кожного способу є свої переваги і недоліки, але головне те, що кожен з них знаходить своє місце в залежності від області застосування.

Один з найскладніших методів віртуалізації забезпечується емуляцією апаратних засобів. У цьому методі VM (virtual machine) апаратних засобів для емуляції обладнання створюється на хост-системі [4]. Але головною проблемою при емуляції апаратних засобів визнають суттєве уповільнення при виконанні програм в такому середовищі. Оскільки кожна команда повинна моделюватися на основних апаратних засобах, при цьому уповільнення в 100 разів при емуляції є звичайною справою. Незважаючи на це, такий метод емуляції має суттєві переваги. Наприклад, управління операційною системою для PowerPC на системі з ARM процесором. Також можна управляти численними віртуальними машинами, кожна з яких буде моделювати інший процесор [5]. Модель емуяції обладнання показано на рис. 2.

Рис. 2. Емуляція обладнання

Повна (апаратна) віртуалізація, або «рідна» віртуалізація, є іншим способом віртуалізації. Ця модель використовує менеджер віртуальних машин (гіпервізор), який здійснює зв'язок між гостьовою операційною системою і апаратними засобами системи [6]. Усередині гіпервізора повинно бути встановлено й налаштовано певний захист, так як основні апаратні засоби не належать ОС, а розділяються гіпервізором. При побудові великих корпоративних систем, як правило, використовується саме апаратна віртуалізація, що показано на рис. 3.

Рис. 3. Апаратна віртуалізація

При цьому великі вендори, такі як VMware, IBM й Microsoft, розробляють свої платформи віртуалізації на базі технологій апаратної віртуалізації Intel VT, AMD-V.

Паравіртуалізація - це інший популярний спосіб, який має деяку схожість з повною віртуалізацією. Цей метод використовує гіпервізор для поділу доступу до основних апаратних засобів, але об'єднує код, що стосується віртуалізації, в безпосередньо операційну систему [7]. Паравіртуалізація розділяє процес з гостьовою операційною системою. Паравіртуалізація вимагає, щоб гостьова ОС була змінена для гіпервізора, і це є недоліком методу. Однак, паравіртуалізація пропонує високу продуктивність, майже як у реальної системи. При цьому, як і при повній віртуалізації, одночасно можуть підтримуватися різні операційні системи. Але певним недоліком паравіртуалізації можна вважати обмежену кількість підтримуваних ОС. Оскільки є необхідність вносити зміни в код ядра ОС, що не завжди представляється можливим через закритість деяких ОС.

Віртуалізація рівня операційної системи. Цей метод підтримує єдину операційну систему, що зображено на рис. 4. В найзагальнішому випадку - просто ізолює незалежні віртуальні сервери (контейнери) один від одного. Для поділу ресурсів одного сервера між контейнерами, дана віртуалізація вимагає внесення змін в ядро операційної системи (наприклад, як у випадку з OpenVZ) [8]. При цьому перевагою її є рідна продуктивність, без «накладних витрат» на віртуалізацію пристроїв.

Рис. 4. Віртуалізація рівня операційної системи

PROXMOX VE - система віртуалізації з відкритим вихідним кодом. Управляється за допомогою веб-інтерфейсу або командного рядка Linux. Може працювати як окрема віртуальна машина, а також об'єднуватися в кластер, використовуючи вбудовані можливості гіпервізора. Для гостьових ОС на базі Linux є готові шаблони віртуальних машин, що завантажуються з офіційного сайту. PROXMOX VE є одним з кращих безкоштовних рішень для віртуалізації з відкритим вихідним кодом [9].

В даний час існує безліч причин використання віртуалізації. Найважливішою причиною є, так звана, серверна консолідація. Простіше кажучи, можливість віртуалізувати безліч систем на окремому сервері. Це дає можливість організаціям заощадити на потужності, місці й адмініструванні через наявність меншої кількості серверів. При цьому важливим фактором є абстрагування від обладнання. Наприклад, сервера іноді виходять з ладу. При цьому є можливість перерозподілити навантаження на обладнання. Відсутність прив'язки, до якогось «заліза» істотно полегшує життя IT-відділу й знижує ризик простою підприємства.

Інша причина використання віртуалізації полягає в тому, що буває спочатку важко визначити навантаження на сервер. При цьому процедура віртуалізації підтримує так звану живу міграцію (live migration). Жива міграція дозволяє ОС, яка переміщається на новий сервер, і її додаткам збалансувати навантаження на доступному обладнанні.

Використовуючи можливості сучасних ПК, можна легко розгорнути будь-який віртуальний сервер навіть на домашньому комп'ютері, а потім легко перенести його на інше обладнання. Віртуалізація також важлива для рішень, необхідних розробникам. Наприклад, віртуалізація дозволяє керувати кількома операційними системами, і якщо одна з них зазнає краху через помилки, то гіпервізор й інші операційні системи продовжують працювати. Це дозволяє зробити налагодження ядра системи подібно додаткам, що призначені для користувача.

Одним з методів віртуалізації є контейнеризація. Контейнеризація - це легка віртуалізація та ізоляція ресурсів на рівні операційної системи, яка дозволяє запускати додаток і необхідний йому мінімум системних бібліотек в повністю стандартизованому контейнері, що з'єднують з хостом або чим-небудь зовнішнім по відношенню до нього за допомогою певних інтерфейсів. Контейнер не залежить від ресурсів або архітектури хосту, на якому він працює [10].

Всі компоненти, що необхідні для запуску програми, упаковуються як один образ та можуть бути використані повторно. Додаток в контейнері працює в ізольованому середовищі і не використовує пам'ять, процесор або диск хостової операційної системи. На рис. 5 зображено графічне порівняння віртуалізації та контейнеризації [11].

Рис. 5. Графічне порівняння віртуалізації та контейнеризації

В цілому можна виділити наступні переваги використання віртуалізації:

1) Скорочення витрат на придбання й підтримку обладнання. У сучасних умовах практично в кожній компанії завжди знайдеться один або два сервера мають декілька ролей, наприклад, поштовий сервер, файловий сервер, сервер бази даних й т.і. Безумовно, на одній фізичній машині можна піднімати по кілька програмних комплексів (серверів), що виконують різні завдання. Але дуже часто бувають ситуації, коли встановлення нового ПО вимагає незалежної серверної одиниці. В такому випадку якраз і буде необхідною віртуальна машина з потрібною ОС. Сюди ж можна віднести випадки, коли в мережі необхідно мати кілька незалежних один від одного віртуальних серверів зі своїм набором служб і своїми характеристи-

ками, які повинні існувати як незалежні вузли мережі. Типовий приклад - це послуги хостингу.

2) Скорочення серверного парку. Перевага віртуалізації полягає в тому, що можна значно скоротити кількість фізичних ПК. В результаті менше часу і грошей витрачається на пошук, закупівлю й заміну обладнання. Поряд з цим скорочуються площі, що виділяються під зміст серверної бази.

3) Скорочення штату IT-співробітників. На обслуговування меншої кількості фізичних машин потрібно менше людей. З точки зору керівництва компанії, скорочення штату - це скорочення серйозною статті витрат підприємства.

4) Простота в обслуговуванні. Додати жорсткий диск або розширити існуючий, збільшити кількість оперативної пам'яті, все це займає певний час у разі з фізичним сервером. Відключення, від'єднання зі стійки, підключення нового обладнання, включення - в разі використання віртуалізації всі ці дії опускаються, і операція зводиться до кількох клацань миші або командам адміністратора.

5) Клонування й резервування. Ще одним плюсом віртуалізації є простота клонування віртуальних машин. Наприклад, компанія відкриває новий офіс. При цьому серверна інфраструктура центрального офісу стандартизована та являє собою кілька серверів з однаковими налаштуваннями. Розгортання такої інфраструктури зводиться до простого копіювання образів на сервер нового офісу, конфігурації мережевого обладнання і зміни налаштувань в прикладному ПО.

Використання віртуальної АТС дозволяє поєднувати переваги Інтернет-сервісів з простотою класичної телефонної станції. Віртуальні АТС називають хмарними, оскільки основна частина заліза функціонує на стороні сервіс-провайдера, а клієнт отримує послугу в чистому вигляді. Віртуальна АТС має значно більшу пропускну здатність і ніяк не лімітована по маршрутизації. Її можна налаштувати за різними сценаріями.

Основними рішеннями IP-телефонії є фірмові і відкриті IP-PBX, SIP-провайдери, а також віртуальні і хмарні АТС. На практиці найбільший відсоток займають відкриті АТС. Найбільш відомими безкоштовними програмними продуктами, що розповсюджуються в вихідному коді, сьогодні є: Asterisk, Yate, SipXecs, FreeSWITCH.

Для вибору адекватного рішення розглянемо деякі перспективні підходи до побудови хмарної АТС.

Asterisk являє собою повністю програмну АТС, що працює під управлінням операційної системи Linux та забезпечує підтримку практично всіх популярних протоколів IP-телефонії: SIP, H323, SCCP, ADSI. Крім стандартних і загальновідомих, Asterisk також має свій власний протокол - IAX.

Перевага Asterisk полягає в її розширеному функціоналі, в поєднанні з яким немає аналогів відповідністю стандартам. Знаючи переваги додатків Asterisk, його вибирають фундаментом для роботи віртуальної АТС. Таким чином, функціонал хмарної АТС якісно підкріплений новими сучасними можливостями [12].

Використовуючи систему Asterisk, віртуальна АТС дає можливість:

- розмістити на один SIP-логін кілька телефонних ліній;
- налаштувати голосове привітання за індивідуальними сценаріями;
- створити інтерактивне голосове меню для зв'язку з компетентним відділом;
- записувати і прослуховувати розмови абонентів з вашими співробітниками;
- ставити дзвінки в чергу і розподіляти їх між агентами для якісної обробки.

PROXMOX VE підтримує новітні функції віртуалізації пам'яті від виробників процесорів, для мінімізації завантаження процесора і досягнення високої пропускної здатності. PROXMOX VE успадковує потужні функції управління пам'яттю від Linux. Пам'ять віртуальної машини зберігається так само, як пам'ять будь-якого іншого Linux-процесу, і може замінюватися, копіюватися великими сторінками для підвищення продуктивності, узагальнюватися або зберігатися в файлі на диску.

Для збереження даних PROXMOX VE може використовувати будь-який носій, підтримуваний Linux, для зберігання образів віртуальних машин, в тому числі локальні диски з інтерфейсами IDE, SCSI і SATA, Network Attached Storage (NAS), включаючи NFS і SAMBA / CIFS, або SAN з підтримкою iSCSI і Fibre Channel. Для поліпшення пропускної спроможності системи зберігання даних і резервування може використовуватися багато-введення / виведення.

Знову ж таки, оскільки система входить до складу ядра Linux, може використовуватися перевірена і надійна інфраструктура зберігання даних з підтримкою всіх провідних виробників; його набір функцій зберігання перевірений на багатьох виробничих установках. Система підтримує динамічну міграцію, що продемонстровано на рис 6. Цим забезпечується можливість переміщення працюючих віртуальних машин між фізичними вузлами без переривання обслуговування.

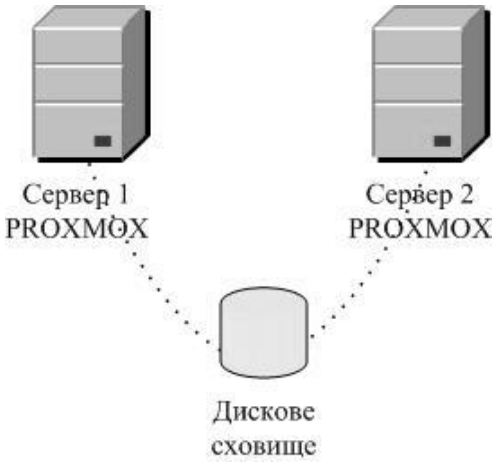


Рис. 6. Динамічна міграція віртуальних машин

Динамічна міграція є прозорою для користувачів: віртуальна машина залишається включеною, мережеві з'єднання - активними, і призначені для користувача додатки продовжують працювати, в той час як віртуальна машина переміщається на новий фізичний сервер.

Велику частину обладнання, що використовується в мережах можна замінити сервісом, які надають оператори та провайдери або орендою виділеного серверу.

Наприклад, орендована віртуальна АТС з параметрами: 10 SIP-абонентів, 10 робочих місць, 1 GSM шлюз коштує в середньому 700 грн/місяць [13]. Процедура з віртуальним сервером зводиться до зміни налаштувань в панелі управління і, при необхідності, перезапуску сервера. Тобто можна почати з мінімальних необхідних вимог і в міру потреби збільшувати використовувані ресурси, масштабуючи роботу. Якщо ресурси більш не потрібні, від них так само легко можна відмовитися.

Фізичний сервер володіє певними параметрами і для їх зміни потрібен час і кошти. Наприклад, для встановлення додаткового модуля оперативної пам'яті потрібно втручання в роботу сервера, чим порушується безперебійність роботи. При оренді сервера використовується 100% його ресурсів - ніяких сусідів по серверному обладнанні не буде.

Таким чином, переваги виділеного серверу наступні: не потрібно витрачати кошти на придбання серверів та обладнання; підключення за лічені хвилини; доступність сервера; мінімальні кошти на оренду віртуального виділеного сервера та багатоканального номеру; розширення можливостей серверу: гнучкості і пропускної здатності; вибір мінімальних затримок для сервера в залежності від розташування абонентів.

Оренда виділеного сервера надає можливість самостійно вибрати конфігурацію і програмне середовище, в якій буде розвиватися АТС. Виділений сервер з мінімальними параметрами коштує в середньому 1000 грн/місяць [14].

Віртуальна машина працює незалежно від інших, розташованих з нею на одній хост-машині. Це означає, що збій в роботі одного сервера не впливає на функціонування сусідів.

Розглянемо конфігурацію налаштування середовища віртуалізації на прикладі Asterisk. Накладні витрати на створення контейнерів LXC для АТС Asterisk, дуже невеликі, і ніщо не заважає запускати їх сотнями або тисячами. Це неможливо при використанні повноцінної віртуалізації. При створенні контейнера LXC для Asterisk, треба визначити основні параметри: ім'я контейнера, кількість ядер процесора, обсяг оперативної пам'яті, образ системи для Asterisk, розмір диска, адресу мережі.

Всі ці параметри, за допомогою POST запиту передаються в відповідний процес, що продемонстровано на рис 7. Процес запускає утиліту, яка створює контейнер, або видає помилку, якщо якісь параметри вказані невірно.

Рис. 7. Схема створення контейнера для Asterisk

Для розробки схеми IP-телефонії використовувалася стандартна схема побудови подібних телефонних систем, в якій застосовано існуючу IP-мережу, що виключає закупівлю додаткового мережевого обладнання. Крім того, для уникнення проблем з масштабуванням проєкту, необхідний перехід з тризначного номерного плану на чотиризначний план. Схему реалізації середовища віртуалізації PROXMOX для віртуальної АТС Asterisk зображено на рис. 8.

Далі, необхідно визначиться з уніфікацією обладнання, яке буде здійснювати роботу всієї мережі. Сервер з потужностями, достатніми для організації підключення всіх користувачів, в разі переходу на оптоволоконний зв'язок. У такому випадку пропаде необхідність встановлювати сервера для віддалених ділянок. Системні вимоги для сервера в такому випадку будуть наступними: процесор Xeon E3-1220, пам’ять 1Gb DDR3 RAM, мережа зі швидкістю 200 Мбіт/с.

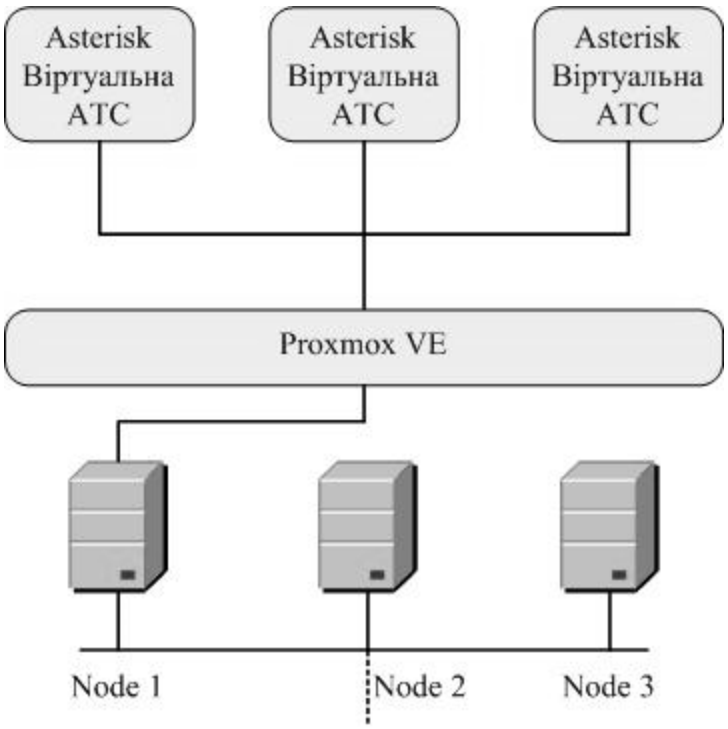


Рис. 8. Модель налаштування середовища віртуалізації

У роботі проведено дослідження, яке з'ясує, наскільки можна провести економію оперативної пам'яті у хост-системі у разі використання контейнерної віртуалізації у порівнянні з гіпервізорною. У якості навантаження на сервер, на якому будуть працювати віртуальні машини, взято процедуру встановлення операційної системи. Ця процедура задіє відразу всі види ресурсів й супроводжується високим процесорним навантаженням, великим споживанням ОП, інтенсивною роботою із зовнішніми пристроями та, що дуже важливо, активною роботою з накопичувачем на магнітних дисках (як правило, це віртуальні накопичувачі, як використовуються файли хост-системи). При цьому підготовлено сервери, встановлено VirtualBox для сервера, на якому використовується гіпервізорная віртуалізація, а для сервера з контейнерною віртуалізацію - програмне забезпечення Docker [15].

Розглянемо дослідження з однією віртуальною машиною та одним контейнером з однією віртуальною машиною. Дослідження проведено у два етапи:

- на першому етапі проаналізовано навантаження на оперативну пам'ять з одним контейнером (табл. 1) та з однією віртуальною машиною (табл. 2).

Таблиця 1

Час, с	0	100	150	200	400	450	700	750
Навантаження на ОП, %	0,2	0,4	1,4	1,5	1,5	3,7	3,7	0,2

Таблиця 2

Час, с	0	100	150	200	400	450	550
Навантаження на ОП, %	0,5	1,7	1,7	1,7	4,3	4,3	0,5

- на другому етапі проаналізовано навантаження на CPU з одним контейнером (табл. 3) та з однією віртуальною машиною (табл. 4).

Таблиця 3

Час, с	0	100	150	200	400	450	700	750
Навантаження на CPU, %	0	1,5	6,5	6,5	8,5	8,5	8	0,5

Таблиця 4

Час, с	0	100	150	200	400	450	550
Навантаження на CPU, %	0,5	7,5	8,2	8,5	8,5	8,5	0,5

Аналіз показує, що звичайна віртуальна машина працює швидше, ніж аналогічна у контейнері, споживаючи при цьому більше обчислювальних ресурсів. Контейнер показав менше споживання ресурсів, але більш тривалу роботу. Однак помітно, що після фази розпакування файлів з образу навантаження зростає приблизно в 2 рази. Це характеризує процес встановлення операційної системи і є основним піком навантаження на ОП. Таким чином, побудова (складання) системи з двійкових файлів вимагає істотно більше ресурсів, ніж підготовка цих файлів.

Що стосується навантаження на CPU, то помітно, що віртуальна машина більш вимоглива, їй потрібно більше обчислювальної потужності. Але в масштабах сервера це не так значно, якщо аналізується одна віртуальна машина.

Розглянемо узагальнене дослідження при запуску десяти віртуальних машин на одному сервері та десяти контейнерів. У табл. 5 показано навантаження на ОП від часу. У табл. 6 показано навантаження на CPU від часу.

Таблиця 5

Час, с	0	250	2000	2500	4000	4500
Навантаження на ОП, %	0	15	15	37	37	1

Таблиця 6

Час, с	0	250	2000	2500	4000	4500
Навантаження на CPU, %	0	50	17	17	20	5

Зі збільшенням кількості одиниць віртуальних машин і контейнерів потреба в ресурсах зростає однаково, тобто залежність витрати ресурсів відносно один одного зберігається. Час виконання всіх операцій також зростає, але з різною інтенсивністю.

Таким чином, контейнерна віртуалізація є більш ефективною в плані витрати пам'яті, але втрачає у швидкодії через додаткові витрати на обчислення адрес. Контейнери, у свою чергу, навпаки, є віртуалізацією на рівні операційної системи. А це вже має на увазі, що є гостьова операційна система, яка використує те саме ядро, що й хостова ОС. Такий підхід дає контейнерам велику перевагу: вони можуть бути меншими і компактнішими за гіпервізорні гостьові середовища, оскільки у них з хостом набагатого більше загальних процесів, ніж у віртуальних машин.

Дослідження показали, що при використанні контейнерів та програмного забезпечення Docker при організації кластерних обчислень не тільки вирішено проблему ізоляції віртуальних машин і мереж одного віддаленого користувача від іншого, але й отримано виграш у швидкості обчислень й витратах ОП.

Висновки

Показано основні вигоди хмарних АТС при високому рівні технологічності та відносній дешевизні в порівнянні з класичними АТС.

На прикладі моделей віртуалізації проведено аналіз методів віртуалізації, які організовано через різні рівні абстракції. Доведено переваги використання віртуалізації в залежності від витрат на придбання й підтримку обладнання, зменшення кількості серверного обладнання, скорочення штату співробітників, простоти в обслуговуванні, резервуванні, а також від налаштування за різними сценаріями.

На прикладі безкоштовного програмного продукту Asterisk, перевага якого в розширеному функціоналі, розглянуто рішення для побудови хмарної АТС. Показано процес запуску створення контейнеру для Asterisk. Надано модель реалізації середовища віртуалізації PROXMOX для віртуальної АТС Asterisk.

Проведено дослідження для оцінки контейнерної та гіпервізорної віртуалізацій. Дослідження показало, що хоча споживання обчислювальних ресурсів збільшується практично однаково зі збільшенням кількості використовуваних контейнерів та віртуальних машин, контейнери споживають менше ресурсів. Тривалість виконання обчислень зростає приблизно однаково, і тут виграють контейнери, тому що відпрацьовують швидше звичайних віртуальних машин. Для проєктування кластерної системи цей критерій є дуже важливим. Оскільки використовувані всередині контейнерів віртуальні машини безпечно ізольовані, то це дає можливість працювати окремо і ніяк не перетинатися в процесі виконання завдань та процесів.

Список літератури:

1. А. Гаврилов Платформы виртуализации. Обзор [Электронный ресурс] // Режим доступа: http://dx.doi.org/10.1109/ICC.2010.5502484.
2. Романов О.І., Нестеренко М.М., Фесьоха Н.О. Аналіз сучасних технологій віртуалізації для побудови інформаційно-телекомунікаційних систем // Збірник наукових праць ВІТІ. 2019. № 1. С. 82-90.
3. Новый плакат - VMware [Электронный ресурс] // Cloud on AWS Logical Design Poster for Workload Mobility. Режим доступа: https://www.vmgu.ru/search/AWS.
4. Івченко Ю. М., Івченко В. Г., Гондар О. М. Впровадження технології віртуалізації для підвищення надійності та безпеки інформаційних систем на залізничному транспорті // Електромагнітна сумісність та безпека на залізничному транспорті. 2014. № 7. С. 82-86.
5. Чепцов В.Ю., Хорошилов А.В. Эмуляция ввода-вывода оборудования с отображением в ОЗУ внутри ядер операционных систем // Труды Института системного программирования РАН. 2018. № 30(3). С. 121-134.
6. Yang Ye etc. S2H: Hypervisor as a setter within Virtualized Network I/O for VM isolation on cloud platform // Computer Networks. 2021. V.201. P. 156-163.
7. Ekane Brice, Ngoc Tu Dinh, Teabe Boris, Hagimont Daniel, Noel De Palma Adaptive network device services in a virtualized environment // Future Generation Computer Systems. 2021. V. 127. P. 14-22.
8. Wessel Sascha, Huber Manuel, Stumpf Frederic, Eckert Claudia Improving mobile device security with operating system-level virtualization // Computers & Security. 2015. V. 52. P. 207-220.
9. PROXMOX VE ADMINISTRATION GUIDE RELEASE [Электронный ресурс] // Proxmox Server Solutions Gmbh. Режим доступа: https://pve.proxmox.com/pve-docs/pve-admin-guide.pdf.
10. Gordeev A. V., Gorelik D. V. Comparative Testing of Container and Hypervisor Virtualizations // Information and Control Systems. 2018. no. 2. P. 60–66.
11. Евстратов В. В. Контейнеризация как современный способ виртуализации // Молодой ученый. 2020. № 49 (339). С. 7-9.
12. Jim Van Meggelen, Russell Bryant и Leif Madsen Asterisk: The Definitive Guide. O'Reilly Media, Inc., Gravenstein Highway North, 2013. - 311 p.
13. ТОП-7 сервисов виртуальных АТС для IP телефонии в Украине [Электронный ресурс] // Режим доступа: https://seoukraine.com.ua/.
14. Конфігуратор виділених серверів [Электронный ресурс] // Режим доступа: https://www.ukraine.com.ua/uk/dedicated/.
15. Jessie Frazelle Docker Containers on the Desktop [Электронный ресурс] // Режим доступа: https://blog.jessfraz.com/post/docker-containers-on-the-desktop/.

Надійшла до редколегії 15.01.2022

Відомості про авторів:

Токар Любов Олександрівна – канд. техн. наук, доцент, Харківський національний університет радіоелектроніки, доцент кафедри інфокомунікаційної інженерії ім. В.В. Поповського (ІКІ); Україна; e-mail: liubov.tokar@nure.ua; ORCID: https://orcid.org/0000-0002-7780-1928

УДК 621.382.232 **DOI:10.30837/rt.2022.1.208.07**

К.С. ЯЦУН

ВПЛИВ СТРУКТУРИ АКТИВНОЇ ОБЛАСТІ РЕЗОНАНСНО-ТУНЕЛЬНОГО ДІОДУ НА КРИТИЧНІ ТОЧКИ ЙОГО ВОЛЬТ-АМПЕРНОЇ ХАРАКТЕРИСТИКИ

Вступ та постановка завдання

Резонансно-тунельні діоди становлять великий інтерес для створення високошвидкісних приладів терагерцового діапазону та цифрових пристроїв з часом перемикання близько 10^{-12} с і менше, за рахунок напівпровідникових нанорозмірних гетеро структур, які мають N-подібну вольт-амперну характеристику (ВАХ) з ділянкою негативного диференціального опору та малою інерційністю процесу тунелювання (тривалість процесу має порядок 10^{-13} с). Практичну реалізацію резонансно-тунельного діоду у 1963 році здійснив Л.В. Йогансен, який запропонував використовувати ефект резонансного тунелювання електронів у багатошарових тонкоплівкових структурах метал-діелектрик для створення електронних інтерферометрів, тонкоплівкових діодів, тріодів тощо [1].

Сучасна передова інформаційна технологія, в основному, пов’язана з електронним представленням та обробкою інформації недорогим, швидкісним, дуже компактним та високонадійним способом, саме тому пошуки та досягнення постійної мініатюризації та інтеграції електроніки є ключем до успіху комп'ютерної індустрії та комп'ютерних програм. Розширена мультимедійна інфраструктура та послуги в майбутньому вимагатимуть подальшого зменшення розміру мікросхеми. Щільність мікросхем, представлена технологією пам’яті, відповідає закону Мура і приблизно подвоюється кожні два роки протягом останніх трьох десятиліть. У той час як зменшення масштабу звичайних транзисторів має винятково швидку еволюцію, революційні концепції пристроїв активно досліджуються, особливо в двох суміжних областях, відомих як наноелектроніка та єдина електроніка [2].

Добре відомо, що коли розмір системи стає порівнянним з довжиною хвилі електрона, домінуючими стають квантові ефекти. Це відбувається, коли транзистори зменшуються, а їх характерні розміри досягають нанометрового діапазону, що призводить до нових явищ і можливих нових пристроїв, заснованих на квантових тунельних механізмах. Щоб наноелектроніка стала реальністю, важливо, щоб нові пристрої та схеми були виготовлені з нанометровою точністю, а також необхідно вміти точно проектувати пристрої та схеми. Це призвело до максимізації дослідницьких зусиль і досягнень у трьох областях: нанофабрикація, квантове моделювання та інновації схем.

Постійні зусилля щодо квантового транспортного моделювання резонансно-тунельного діоду мотивуються необхідністю зрозуміти роботу пристрою та забезпечити первинний тест для розробки теоретичних інструментів для наноелектронних пристроїв. Не дивно, що це сильно відрізняється від традиційного моделювання пристроїв. Більше того, це дає цінні знання про квантові аспекти транспорту електронів у мезоскопічних системах. Досі залишається складним завданням точно передбачити вольт-амперні характеристики наноелектронних пристроїв, таких як РТД.

Серед численних наноелектронних пристроїв, запропонованих і продемонстрованих, РТД є, мабуть, найперспективнішим кандидатом для застосування цифрових схем завдяки своїй характеристиці негативного диференціального опору, простоті конструкції, відносній простоті виготовлення, високій швидкості, гнучкості та універсальності.

Аналіз останніх досліджень і публікацій. За останні два десятиліття дослідженню резонансних тунельних діодів приділяли велику увагу чимало як вітчизняних так і

зарубіжних вчених. Значних досягнень було досягнуто з точки зору фізики пристроїв РТД, моделювання, технології виготовлення, а також розробки схем і застосувань. РТД був широко вивчений, і було написано понад тисячу наукових робіт щодо різних аспектів цього пристрою. Проте, чи знайдуть РТД свій шлях до основної електроніки в майбутньому, залишається незрозумілим. Дослідження тривають і в деяких областях дуже активні.

Так, А.О. Семенов [3] розробив багаточастотний генератор квазіперіодичних коливань за методом Ван дер Поля на основі польової транзисторної структури з від'ємним диференційним опором.

О.В. Осадчук, В.С. Осадчук та Я.О. Осадчук [4] провели дослідження реактивних властивостей тунельно-резонансного діода. Авторами доведено, що резонансно-тунельні діоди можна використовувати як регульовані ємнісні та індуктивні елементи, причому їх добротність можна регулювати за рахунок від'ємного диференційного опору в інтервалах від 100 і більше.

У [5] автором здійснено розробку та продемонстровано застосування формалізованого підходу (на основі модифікованого методу перевалу та формалізму матриці розсіювання), для дослідження динамічних характеристик квантових систем.

Є. В. Малий [6] дослідив властивості дефектів структури у фосфіді галію та їхній вплив на параметри світло діодів. Автором зазначено, що для діодів, опромінених нейтронами, коефіцієнт пошкоджуваності носіїв струму є функцією температури вимірювання і проявляє тенденцію до зростання при охолодженні. Очевидно, що така поведінка k_n зумовлена температурною зміною положення рівня Фермі – зміщення E_F до середини E_g активізує вплив компенсації акцепторними центрами електропровідності nобласті та донорними – p-області.

Із зарубіжних авторів варто відзначити такі роботи як: Huang, Keh-Ching [7], Ortega-Piwonka, Ignacio & Piro, Oreste & Figueiredo, José & Romeira, Bruno & Javaloyes, Julien [8], Halimatus Saadiah, Warsuzarina Mat Jubadi, Nabihah Ahmad and M. Hairol Jabbar [9], Khanna, Vinod [10], Jian Pind Sun, George J. Haddad, Pinaki Mazumder and Joel N. Schulman [11], Feiginov, Michael [12], Bhukya, Revathi & Hampika, Gorla & Guduri, Manisha [13], Awan, Jram Taj [14], Cimbri, Davide & Wasige, E. [15] та інші.

Проте, враховуючи описані наукові набутки, за темою, питання модифікації активної галузі резонансно-тунельного діода залишається відкритим та потребує детального опрацювання.

Постановка завдання. Дослідити вплив структури активної області РТД на критичні точки його вольт-амперної характеристики (струми та напруги піку і долини ВАХ), та її температурну стабільність.

Викладення основного матеріалу дослідження. Основна конфігурація пристрою РТД являє собою структуру квантової ями з подвійним бар'єром нанометрових розмірів, що включає два контакти, як показано на рис. 1, де області I, II і VI, VII є сильно легованими контактами, виготовленими з напівпровідника з відносно малою забороненою зоною, наприклад, GaAs.

Ці шари містять емітер і колектор відповідно. Області III і V є квантовими бар'єрами, виготовленими з напівпровідника з відносно більшою забороненою зоною, наприклад, AlGaAs, і, зокрема, з позитивним зміщенням зони провідності відносно напівпровідника з меншою забороненою зоною. Область IV між двома бар'єрами – це квантова яма, знову зроблена з напівпровідника з меншою забороненою зоною. Іноді його також називають базою, незалежно від того, чи справді існує електричний контакт. Структура показана в термінах залежності енергії електронів від відстані під зміщенням, оскільки цікавить процес транспортування електронів, який, по суті, є рухом електронів у межах певної структури енергетичного діапазону під дією прикладених напруг зміщення. Оскільки характерні розміри структури квантової ями з подвійним бар'єром порівняні з довжинами хвиль електронів, хвильова природа електронів призводить до таких квантових явищ, як

інтерференція, тунелювання, квантування енергії тощо. В результаті в структурах квантової ями з подвійним бар'єром виникають резонансні явища тунелювання, які утворюють основу для роботи РТД.

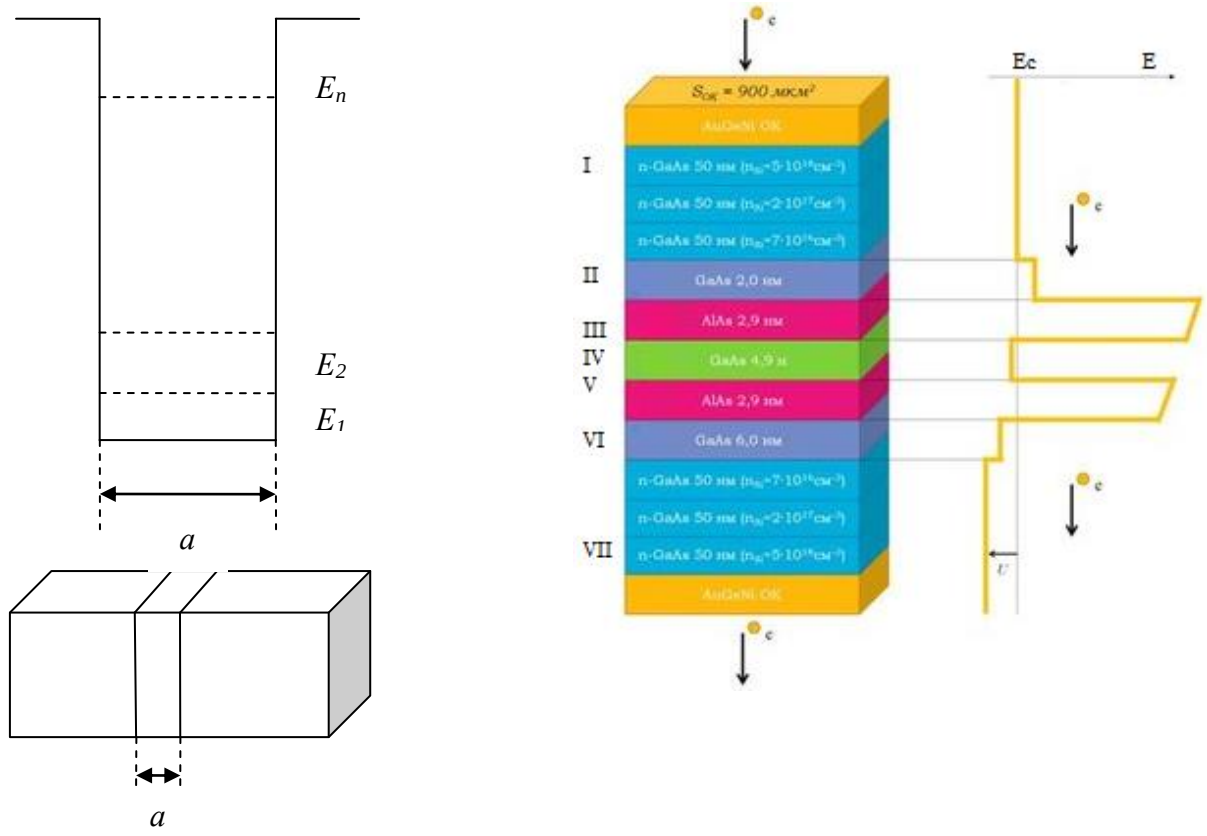


Рис. 1. Конфігурація резонансно-тунельного діода

Основна структура РТД, показана на рис. 1, може мати багато варіацій з точки зору профілю потенціалу (енергетичного), який визначається насамперед конкретною системою матеріалів, що використовуються.

Спектр електронів в області I, керований напругою зміщення, прикладеною до контактів РТД, що падає на структуру квантової ями з подвійним бар'єром, показану на рис. 1. Вважається, що електронний спектр розподілений по енергії відповідно до статистики Фермі–Дірака. Контакти зазвичай сильно леговані, щоб забезпечити низький омічний контакт і високу щільність струму. Використання розподілу Фермі передбачає, що електрони в області I перебувають у тепловій рівновазі через взаємодію між електронами та їх оточенням в області контакту I. Те саме припущення зроблено для області контакту VII.

Багаторазове відображення викликає деструктивні або конструктивні перешкоди залежно від довжини хвилі конкретного електрона. Для електронів із певною довжиною хвилі, що сприяє конструктивній інтерференції, ймовірність передачі, близька до одиниці, може бути знайдена при енергіях, що відповідають цим довжинам хвиль. Перший процес, це процес збігу резонансної енергії з основною. У процесі 2 електрон спочатку розсіюється на енергетичному рівні в шарі накопичення емітера, який є двовимірною потенційною ямою в області II. Потім він може поглинати фонон і послідовно тунелювати через резонансний рівень. Аналогічно, в процесі 3 електрон з початковою енергією може взаємодіяти з вібрацією решітки, випускаючи фонон, а потім тунелювати через E_0. З іншого боку, електрони з достатньо високими енергіями (наприклад, E_4) можуть подолати бар'єри за допомогою термоелектронної емісії, на яку вказує процес 4. Падаючі електрони також мають кінцеву, але малу ймовірність тунелювання через нерезонансні діапазони енергій, що лежать між резонансами.

Фізичні процеси, які беруть участь у роботі РТД, насправді набагато складніші, ніж попередній простий опис, і особливо ускладнені взаємодією електрона з його середовищем. Перш за все, електрони обмінюються частинками та енергією з системою, яка застосовує напругу зміщення, що робить пристрій відкритим для зовнішнього середовища і дуже відрізняється від ізольованої квантової системи. Більше того, електрони в структурі РТД мають взаємодію з вібрацією решітки, домішками нерівності, шорсткості розділу і різнорідності сплаву, а також взаємодії між собою. На хвильовій картині падаюча електронна хвиля розсіюється не тільки профілем потенціалу гетероструктури, але й потенціалами розсіювання, що виникають від цих розсіювачів. Ці процеси можуть суттєво вплинути на властивості пристрою, що робить точну фізичну модель РТД складною системою.

У рамках даного дослідження пропонується розглянути РТД з висотою бар'єра 0,3 – 0,4 еВ.

Щільність струму відповідає виразу:

$$j = \frac{e\times m^*\times k_Б\times T}{2\pi^2\times\hbar^3}\int_0^\infty D(E)\times ln\left[1+exp\left(\frac{E_Ф-E}{k_Б T}\right)\right]dE - \frac{e\times m^*\times k_Б\times T}{2\pi^2\times\hbar^3}\int_0^\infty D(E)\times ln\left[1+ \right.$$
$$\left. +exp\left(\frac{E_Ф-E-eV}{k_Б T}\right)\right]dE, \quad (1)$$

де e – заряд;
m^* – ефективна маса;
$k_Б$ – коефіцієнт Больцмана;
T – температура;
$D(E)$ – коефіцієнт проходження;
E – енергія;
$E_Ф$ – енергія рівня Фермі;
V – напруга, яка подається у структуру;
Енергію рівня Фермі отримаємо з рішення рівняння електронейтральності:

$$\frac{N_д}{1+\beta^{-1}exp\left(\frac{E_Ф-E_д}{k_Б T}\right)} = N_c F_{1/2}\left(\frac{E_Ф}{k_Б T}\right), \quad (2)$$

де β – фактор спінового виродження;
$N_д$ – концентрація донорної домішки;
N_c – ефективна щільність станів у зоні провідності;
$F_{1/2}$ – інтеграл Фермі з індексом $1/2$;
$E_д$ – енергія донорного рівня.

Залежність коефіцієнта проходження знаходимо шляхом вирішення рівняння Шредінгера у одно електронному наближенні без урахування ефектів розсіяння. Нехай двобар'єрна структура розміщена на відстані від 0 до L, тоді хвильова функція виходить з рівняння Шредінгера:

$$\psi'' + \frac{2m^*}{\hbar^2}\big(E - U(x)\big)\psi = 0. \quad (3)$$

Зовнішні функції задаються рівняннями виду:

$$x \le 0, \psi = e^{ikx} + re^{-ikx}; \quad (4)$$

$$x \ge L, \psi = de^{ik(x-L)}, \quad (5)$$

де r – амплітуда відбиття;
d – амплітуда проходження;
k – модуль хвильового вектора.

Граничні умови:

$$\psi(0) = 1 + r, \quad \psi(L) = d, \tag{6}$$

$$\psi'(0) = ik(1 - r), \quad \psi'(L) = ikd. \tag{7}$$

Коефіцієнти відбиття та проходження дорівняють відповідно:

$$R = |r|^2, D = |d|^2. \tag{8}$$

Представимо амплітуду r та d через функції $\psi(0)$ та $\psi(L)$, тоді граничні умови матимуть вигляд:

$$\psi'(0) = ik\psi(0) = 2ik, \tag{9}$$

$$\psi'(L) - ik\psi(L) = 0. \tag{10}$$

Тоді коефіцієнти відбиття та проходження знаходимо як:

$$R = |r|^2 = |\psi(0) - 1|^2, \tag{11}$$

$$D = |d|^2 = |\psi(L)|^2. \tag{12}$$

Якщо припустити, що повна довжина структури дорівнює 1 тоді рівняння Шредінгера приймає вид:

$$\psi'' + \big(\varepsilon - U(x)\big)\psi = 0, \tag{13}$$

де ε – енергія;
$U(x)$ – потенціал.

Якщо здійснити розбиття ділянки від 0 до L на N областей довжиною a. Тоді $L = Na$; а $L = 1$, то $a = {}^{1}/_{N}$.

Для будь-якої точки, що знаходиться в області рівняння Шредінгера у дискретному вигляді має вид:

$$\psi_{n+1} + \psi_{n-1} + \varepsilon_n\psi_n = 0, \tag{14}$$

$$\varepsilon_n = -2 + a^2(\varepsilon - V_n). \tag{15}$$

З першої граничної умови $\psi'(0) = ik\psi(0) = 2ik$ зробимо заміну похідної хвильової функції на її дискретний аналіз:

$$\psi'(0) \approx \frac{\psi_1 - \psi_{-1}}{2a}. \tag{16}$$

Тоді гранична умова та рівняння Шредінгера при $x = 0$ має вид:

$$\psi_1 - \psi_{-1} + 2ika\psi_0 = 4ika, \tag{17}$$

$$\psi_1 - \psi_{-1} + \varepsilon_0\psi_0 = 0. \tag{18}$$

Перш гранична умова дорівнює сумі наведених рівнянь поділеної на 2:

$$\psi_1 + \left(\frac{\varepsilon_0}{2} + ika\right)\psi_0 = 2ika. \tag{19}$$

Для другої граничної умови $x = N$ знаходимо:

$$\psi_{N+1} - \psi_{N-1} - 2ika\psi_N = 0, \tag{20}$$

$$\psi_{N+1} - \psi_{N-1} + \varepsilon_N\psi_N = 0, \tag{21}$$

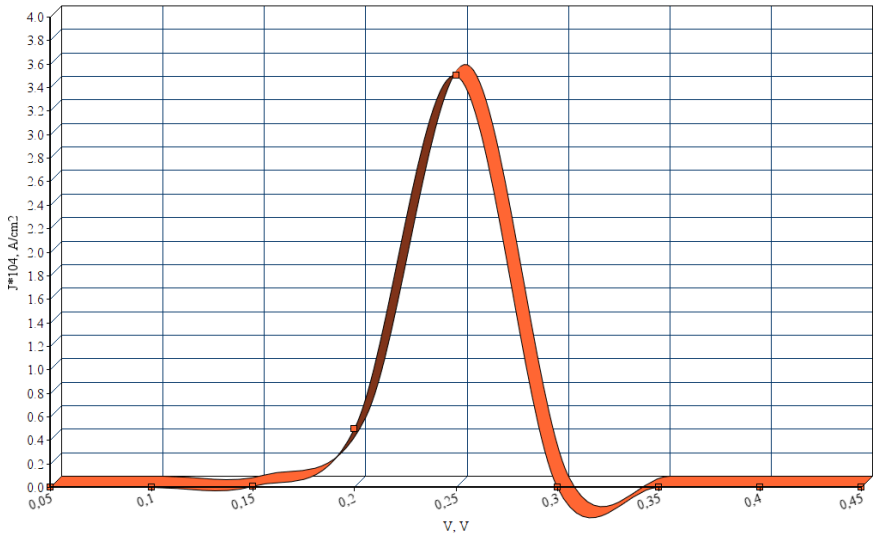
звідки

$$\psi_{N-1} + \left(\frac{\varepsilon_N}{2} + ika\right)\psi_N = 0. \tag{22}$$

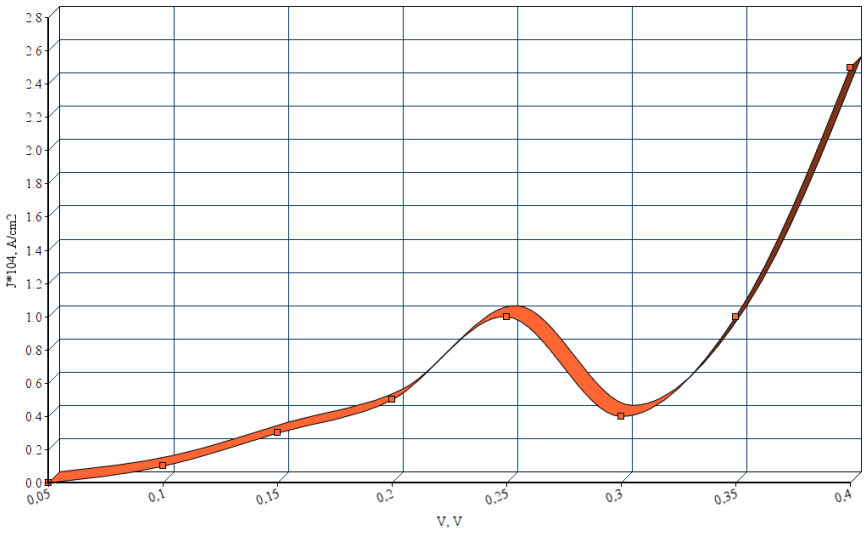
Розрахунок ВАХ резонансно-тунельного діода здійснюється при температурах у 100 та 300 К. На рис. 2 наведено ВАХ резонансно-тунельного діода з висотою бар'єра гетеропереходу 0,3 еВ та товщиною 6 нм. Дані значення обрані для моделювання так як саме на них виникає найбільш широкий та високий пік струму.

З аналізу ВАХ, наведених на рис. 2 випливає, що при температурі 300 К пік щільностей струму є максимальним та досягає до 10^8 А/м^2. Наведені ВАХ отримані без врахування ефектів розсіяння електронів. Однак варто відмітити, що головним впливовим фактором є резонансне тунелювання через другий рівень, для якого пік коефіцієнта проходження значно ширше та вище. Проте у легованому арсеніді галію факт розсіяння електронів може суттєво надавати вплив на значення коефіцієнта проходження та значення струму.

Таким чином, згідно проведеного дослідження, видно, що зменшення висоти піку коефіцієнта проходження у 4,2 рази та збільшення його ширини у 2 рази, є наслідком впливу процесів розсіяння. Даний факт призводить до зниження рівня тунельного струму.



а)



б)

а) температура 100 К
б) температура 300 К

Рис. 2. ВАХ резонансно-тунельного діода

Висновки

У роботі досліджено вплив структури активної області резонансно-тунельного діоду на критичні точки його вольт-амперної характеристики. Доведено той факт, що тунельні ефекти у структурах активної області резонансно-тунельного діода зберігаються при надвисоких температурах, а показники піку щільності струму, такі як положення та форма, змінюються зі зміною конфігурації бар'єру резонансно-тунельного діода.

Список літератури:

1. Иогансен Л.В. О возможности резонансного прохождения электронов в кристаллах через системы барьеров // ЖЭТФ. 1963 Т. 45 № 2 С. 207–213.
2. Ховерко, Ю. М. Мікроелектронні сенсори на основі КНІ-структур з рекристалізованим шаром полікремнію [Текст]: дис... канд. техн. наук: 05.27.01 / Ховерко Юрій Миколайович; Національний ун-т "Львівська політехніка". – Л., 2003. – 168 с.
3. Семенов А. О. Методи і пристрої генерування та формування сигналів з регулярною й хаотичною динамікою для інфокомунікаційних систем. – Кваліфікаційна наукова праця на правах рукопису. Дисертація на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.12.13 «Радіотехнічні пристрої та засоби телекомунікацій» (172 – Телекомунікації та радіотехніка). – Вінницький національний технічний університет, Національний університет "Львівська політехніка" МОН України, Вінниця, 2019. 463 с.
4. Осадчук О. В. Дослідження реактивних властивостей тунельно-резонансного діода / О. В. Осадчук, В. С. Осадчук, Я. О. Осадчук // Вісник Хмельницького національного університету. Технічні науки. – 2020. – № 4(1). – С. 160-167. – Режим доступу: http://nbuv.gov.ua/UJRN/Vchnu_tekh_2020_4(1)__29.
5. Динамічні закономірності резонансних квантових систем [Текст] : дис. ... канд. фіз.-мат. наук : 01.04.02 / Іванов Микита Анатолійович ; Дніпропетр. нац. ун-т. – Дніпропетровськ, 2015. – 115 с. : іл.
6. Малий Є.В. Властивості дефектів структури у фосфіді галію та їхній вплив на параметри світлодіодів. – Кваліфікаційна наукова праця на правах рукопису. Дисертація на здобуття наукового ступеня кандидата фізикоматематичних наук (доктора філософії) за спеціальністю 01.04.07 «Фізика твердого тіла» – Південноукраїнський національний педагогічний університет ім. К.Д. Ушинського, Одеса, 2019. 154 с.
7. Huang, Keh-Ching. (2021). Characterization of resonant tunneling diodes. ETD Collection for Purdue University.
8. Ortega-Piwonka, Ignacio & Piro, Oreste & Figueiredo, José & Romeira, Bruno & Javaloyes, Julien. (2021). Bursting and Excitability in Neuromorphic Resonant Tunneling Diodes. Physical Review Applied. 15. 10.1103/PhysRevApplied.15.034017.
9. Halimatus Saadiah, Warsuzarina Mat Jubadi, Nabihah Ahmad and M. Hairol Jabbar. Resonant Tunneling Diode Design for Oscillator Circuit. International Postgraduate Conference. Physics 2017, P. 1–8.
10. Khanna, Vinod. (2020). Resonant Tunneling Diodes. 10.1201/9781351204675-24.
11. Jian Pind Sun, George J. Haddad, Pinaki Mazumder and Joel N. Schulman. Resonant Tunneling Diodes: Models and Properties. Proceedings of The JEEE, vol. 86, N 4, April 1998, P. 641–661.
12. Feiginov, Michael. (2020). THz resonant-tunnelling diodes. 20. 10.1117/12.2559674.
13. Bhukya, Revathi & Hampika, Gorla & Guduri, Manisha. (2020). Resonant Tunneling Diodes: Working and Applications. 10.1007/978-981-15-5089-8_17.
14. Awan, Jram Taj. Optical and Transport of p-i-n GaAs-AlAs resonant tunneling diode. Jram Taj Awan – Sao Carlos: UFS Car, 2014, P. 85.
15. Cimbri, Davide & Wasige, E.. (2021). Terahertz Communications with Resonant Tunnelling Diodes. 10.1201/9781003001140-3.

Надійшла до редколегії 23.01.2022

Відомості про автора:

Яцун Кирило Сергійович – Харківський національний університет радіоелектроніки, аспірант кафедри мікроелектроніки, електронних приладів та пристроїв (МЕЕПП), факультет електронної та біомедичної інженерії; Україна; e-mail: deadwoldi@gmail.com

SYSTEMS AND METHODS OF INFORMATION PROTECTION
СИСТЕМИ І МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ
СИСТЕМЫ И МЕТОТЫ ЗАЩИТЫ ИНФОРМАЦИИ

UDC 004.056

Scientific approach to probabilistic assessment of information protection against imposing false messages in telecommunication systems / *I.D. Gorbenko, A.A. Zamula* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2022. №208. P. 7 – 15.

To date, in all economically developed countries of the world, multibillion-dollar scientific and exploratory research is being carried out on the problems of building quantum-resistant cryptographic systems. In particular, work is being carried out on the analysis, development and research of models, methods and computational algorithms for post-quantum cryptographic transformations, their possible standardization and implementation. At the same time, it is necessary to have an objective, scientifically based approach for assessing the level of information security, which can be guaranteed when implementing one or another protection mechanism. This paper presents formulated scientific approaches, derived expressions making it possible to evaluate the strength of MAC codes as mechanisms for ensuring the authenticity, integrity, and authenticity of messages. It is shown that it is necessary to use the statistics of joint message distributions for accurate calculation of the MAC codes simulation and collision stability. It is proved that the lower limits for the probabilities of imitation and substitution ignore the statistical properties of authenticators arrays. They are based on the pseudo-randomness model of f(x) function and determine the minimum requirements for the key space size and the MAC values space. The upper bounds for the imitation and substitution probabilities are related to combinatorial properties of the MAC arrays and evaluate the value of collisions in the space of MAC values f(x) and messages for the worst case choice of keys and messages. Collision characteristics of MAC codes are considered. The derived equations make it possible to solve accurately the problem of determining the number of experiments indispensable to create a collision with a certain probability on a set of MAC code values. The MAS stability estimates for one of the types of hash functions are obtained using the derived equations.

Key words: cyber and information security threats; authenticity; MAC code; MAC code attacks; collision; MAC code stability.

Ref: 6 items.

УДК 004.056

Науковий підхід до ймовірнісної оцінки захищеності інформації від нав'язування хибних повідомлень у телекомунікаційних системах / *І.Д. Горбенко, О.А. Замула* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2022. Вип. 208. С. 7 – 15.

На сьогоднішній день в усіх економічно розвинутих країнах світу за проблематикою побудови квантово-стійких криптографічних систем проводяться багатомільярдні науково-пошукові дослідження. Зокрема, проводяться роботи з аналізу, розробки та дослідженню моделей, методів та обчислювальних алгоритмів постквантових криптоперетворень, їх можливої стандартизації та впровадження. При цьому необхідно мати об’єктивній, науково-обґрунтований підхід до оцінки рівня захищеності інформації, який може бути гарантовано при реалізації того чи іншого механізму захисту. У роботі сформульовані наукові підходи, отримані вирази, які дозволяють виконати оцінку стійкості МАС кодів як механізмів забезпечення справжності, цілісності, автентичності повідомлень Показано, що для точного обчислення імітаційної та колізійної стійкості МАС кодів необхідно використовувати статистику спільних розподілів МАС кодів за ключами для дійсних та підроблених повідомлень. Доведено, що нижні межі для ймовірностей імітації та підміни не враховують статистичні властивості масивів автентифікаторів, і ґрунтуються на моделі псевдовипадковості функції f(x) та визначають мінімальні вимоги до розміру ключового простору та простору МАС значень, а верхні межі для ймовірностей імітації та підміни пов'язані з комбінаторними властивостями МАС масивів та оцінюють значення колізій у просторі МАС значень і повідомлень для найгіршого випадку вибору ключів та повідомлень. Розглянуті колізійні властивості МАС кодів. Отримані рівняння, які дозволяють точно розв'язати задачу визначення кількості експериментів (подій), які необхідно виконати для створення колізії з визначеною ймовірністю на безлічі значень МАС коду. Із застосуванням отриманих рівнянь виконані оцінки стійкості МАС для одного з типів хеш-функцій.

Ключові слова: загрози кібер - і інформаційної безпеки; справжність (автентичність); МАС код; атаки на МАС коди; колізія; стійкості МАС кодів.

Бібліогр.: 6 назв.

УДК 004.056

Научный подход к вероятностной оценке защищенности информации от навязывания ложных сообщений в телекоммуникационных системах / *И.Д. Горбенко, А.А. Замула* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2022. Вып. 208. С. 7 – 15.

На сегодняшний день во всех экономически развитых странах мира проводятся многомиллиардные научно-поисковые исследования по проблематике построения квантово-стойких криптографических систем. В частности, проводятся работы по анализу, разработке и исследованию моделей, методов и вычислительных алгоритмов пост квантовых криптопреобразований, их возможной стандартизации и внедрению. При этом необходимо иметь объективный, научно обоснованный подход к оценке уровня защищенности информации, кото-

рый может быть гарантирован при реализации того или иного механизма защиты. В работе сформулированы научные подходы, получены выражения, которые позволяют выполнить оценку стойкости MAC кодов как механизмов обеспечения подлинности, целостности, подлинности сообщений. Показано, что для точного вычисления имитационной и коллизионной устойчивости MAC кодов необходимо использовать статистику совместных распределений сообщений. Доказано, что нижние пределы для вероятностей имитации и подмены не учитывают статистические свойства массивов аутентификаторов, и основываются на модели псевдо случайности функции f(x) и определяют минимальные требования к размеру ключевого пространства и пространства MAC значений, а верхние границы для вероятностей имитации и подмены связаны с комбинаторными свойствами MAC массивов и оценивают значение коллизий в пространстве MAC значений и сообщений для худшего случая выбора ключей и сообщений. Рассмотрены коллизионные характеристики MAC кодов. Получены уравнения, позволяющие точно решить задачу определения количества экспериментов, которые необходимо выполнить для создания коллизии с определенной вероятностью на множестве значений MAC кода. С применением полученных уравнений выполнены оценки устойчивости MAC для одного из типов хэш-функций.

Ключевые слова: угрозы кибер и информационной безопасности; подлинность (аутентичность); MAC код; атаки на MAC коды; коллизия; устойчивости MAC кодов.

Библиогр.: 6 назв.

UDC 621.391.15: 519.7

On correctness of conditions for the CSIDH algorithm implementation on Edwards curves / *A.V. Bessalov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2022. №208. P. 16 – 27.

Incorrect formulation and incorrect solution of the problem of the CSIDH algorithm implementation on Edwards curves E_d was revealed in one of the famous works. The purpose of this paper is to present a detailed critique of such concept with a proof of its inconsistency. Specific properties of three non-isomorphic classes of super singular curves in the generalized Edwards form are considered: full, quadratic, and twisted Edwards curves. Conditions for existence of curves of all 3 classes with $p+1$ order of curves over a prime field F_p are determined. The implementation of the CSIDH algorithm on isogenies of odd prime degrees is based on the use of quadratic twist pairs of elliptic curves. To this end, the CSIDH algorithm can be built both on complete Edwards curves with quadratic twist within this class, and on quadratic and twisted Edwards curves forming pairs of quadratic twist. In contrast to this, the authors of a well-known work are trying to prove theorems that state that there is a solution within one class of E_d curves with a parameter d which is a square. The critical analysis of theorems, lemmas, erroneous statements in this work is carried out. Theorem 2 on quadratic twist in classes of Edwards curves is proved. The CSIDH algorithm modification based on isogenies of quadratic and twisted Edwards curves is presented. To illustrate the correct solution of the problem, an example of Alice and Bob calculations in the secret sharing scheme according to the CSIDH algorithm is considered for $p = 239$.

Key words: curve in generalized Edwards form; complete Edwards curve; twisted Edwards curve; quadratic Edwards curve; curve order; point order; isomorphism; isogeny; w-coordinates; square; non squareю.

3 tab. Ref: 16 items.

УДК 621.391.15: 519.7

О коректності умов імплементації алгоритму CSIDH на кривих Эдвардса / *А.В. Бессалов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2022. Вип. 208. С. 16 – 27.

В одної з відомих робіт виявлені некоректна постановка і невірне рішення задачі імплементації алгоритму CSIDH на кривих Едвардса E_d. Дана розгорнена критика цієї роботи с доведенням неспроможності її концепції. Розглянуті специфічні властивості трьох неізоморфних класів суперсингулярних кривих в узагальненої формі Едвардса: повних, квадратичних та скручених кривих Едвардса. Визначені умови існування кривих усіх 3-х класів з порядком кривих $p+1$ над простим полем F_p. Імплементація алгоритму CSIDH на ізогеніях непарних простих степенів базується на застосуванні пар квадратичного кручення еліптичних кривих. З цією метою алгоритм CSIDH можна будувати як на повних кривих Едвардса з квадратичним крученням всередині цього класу, або на квадратичних і скручених кривих Едвардса, які створюють пари квадратичного кручення. В противагу до цього автори відомої роботи намагаються довести теореми, які стверджують о наявності рішення всередині одного класу кривих E_d з параметром d, який є квадратом. Проведено критичний аналіз теорем, лем, помилкових стверджень в цієї роботі. Доведено теорема 2 про квадратичне кручення в класах кривих Едвардса. Приведено модифікація алгоритму CSIDH, побудованого на ізогеніях квадратичних і скручених кривих Едвардса, Для ілюстрації коректного рішення задачі розглянуто приклад обчислень Аліси і Боба в схемі розподілу секретів згідно алгоритму CSIDH при $p = 239$.

Ключові слова: крива в узагальненій формі Едвардса; повна крива Едвардса; скручена крива Едвардса; квадратична крива Едвардса; порядок кривої; порядок точки; ізоморфізм; лізогенія; w—координати; квадратичний лишок; квадратичний не лишок.

Табл. 3. Бібліогр.: 16 назв.

УДК 621.391.15: 519.7

О корректности условий имплементации алгоритма CSIDH на кривых Эдвардса / *А.В. Бессалов* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2022. Вып. 208. С. 16 – 27.

В одной из известных работ обнаружена некорректная постановка и неверное решение задачи имплементации алгоритма CSIDH на кривых Эдвардса E_d. Дана развернутая критика этой работы с доказательством несостоятельности ее концепции. Рассмотрены специфические свойства трех неизоморфных классов суперсингулярных кривых в обобщенной форме Эдвардса: полных, квадратичных и скрученных кривых Эдвардса. Определены условия существования кривых всех 3-х классов с порядком кривых $p+1$ над простым полем F_p. Имплементация алгоритма CSIDH на изогениях нечетных простых степеней базируется на использовании пар квадратичного кручения эллиптических кривых. С этой целью алгоритм CSIDH можно строить как на полных кривых Эдвардса с квадратичным кручением внутри этого класса, так и на квадратичных и скрученных кривых Эдвардса, образующих пары квадратичного кручения. В противовес этому авторы известной работы пытаются доказать теоремы, утверждающие о наличии решения внутри одного класса кривых E_d с параметром d, который является квадратом. Проведен критический анализ теорем, лемм, ошибочных утверждений в этой работе. Доказана теорема 2 о квадратичном кручении в классах кривых Эдвардса. Приведена модификация алгоритма CSIDH, построенного на изогениях квадратичных и скрученных кривых Эдвардса. Для иллюстрации корректного решения задачи рассмотрен пример вычислений Алисы и Боба в схеме разделения секретов согласно алгоритма CSIDH при $p = 239$.

Ключевые слова: кривая в обобщенной форме Эдвардса; полная кривая Эдвардса; скрученная кривая Эдвардса; квадратичная кривая Эдвардса; порядок кривой; порядок точки; изоморфизм; изогения; w-координаты; квадратичный вычет; квадратичный невычет.

Табл. 3. Библиогр.: 16 назв.

RADIOLOCATION AND RADIONAVIGATION
РАДІОЛОКАЦІЯ І РАДІОНАВІГАЦІЯ
РАДИОЛОКАЦИЯ И РАДИОНАВИГАЦИЯ

UDC 621.396.967.2

Estimation of the relative throughput of requesting airspace surveillance systems / *M.G. Tkach, I.V. Svyd, O.V. Vorgul, S.V. Starokozhev, O.S. Maltsev, A.O. Hlushchenko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2022. № 208. P. 28 – 37.

The paper considers a method for increasing the relative throughput of requesting airspace surveillance radar systems, in which it is proposed to use broadband signals as request and response signals. Thanks to the use of broadband signals, it is possible to reduce significantly the detection range of such response signals with the required quality indicators by means of radio reconnaissance, which practically excludes the possibility for the interested party to use the response signals of an aircraft responder both for long-range detection of air objects and for measuring their coordinates. And, as a result, it makes it possible to exclude unauthorized use of an aircraft responder of requesting radar systems for airspace monitoring by an interested party to suppress the response channel, and, consequently, increase the relative throughput of the considered information systems.

Key words: requesting radar systems; radar systems; airspace surveillance systems; relative bandwidth; aircraft's responder; broadband signals; request signal; response signal; hindrance.

5 fig. Ref: 31 items.

УДК 621.396.967.2

Оцінка відносної пропускної здатності запитальних систем спостереження повітряного простору / *М.Г. Ткач, І.В. Свид, О.В. Воргуль, С.В. Старокожев, О.С. Мальцев, А.О. Глущенко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2022. Вип. 208. С. 28 – 37.

У роботі розглядається метод підвищення відносної пропускної здатності запитальних радіолокаційних систем спостереження повітряного простору, в якому як сигнали запиту та відповіді запропоновано використовувати широкосмугові сигнали. Завдяки використанню широкосмугових сигналів вдається значно знизити дальність виявлення таких сигналів відповіді з необхідними показниками якості засобами радіорозвідки, що практично виключає можливість зацікавленій стороні використовувати сигнали відповіді літакового відповідача як для далекого виявлення повітряних об'єктів, так і для вимірювання їх координат. І, як наслідок, дозволяє виключити несанкціоноване використання літакового відповідача запитальних радіолокаційних систем спостереження повітряного простору зацікавленою стороною для подавлення каналу відповіді, а, отже, дозволяє підвищити відносну пропускну здатність розглядаємих інформаційних систем.

Ключові слова: запитальні системи; радіолокація; радіолокаційна система; система спостереження повітряного простору; відносна пропускна здатність; літаковий відповідач; широкосмугові сигнали; сигнал запиту; сигнал відповіді; завада.

Іл. 5. Бібліогр.: 31 назв.

УДК 621.396.967.2

Оценка относительной пропускной способности запросных систем наблюдения воздушного пространства / *М.Г. Ткач, И.В. Свид, А.В. Воргуль, С.В. Старокожев, А.С. Мальцев, А.А. Глущенко* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2022. Вып. 208. С. 28 – 37.

В работе рассматривается метод повышения относительной пропускной способности запросных радиолокационных систем наблюдения воздушного пространства, в котором в качестве сигналов запроса и ответа предложено использовать широкополосные сигналы. Благодаря использованию широкополосных сигналов удается значительно снизить дальность обнаружения таких ответных сигналов с требуемыми показателями качества средствами радиоразведки, что практически исключает возможность заинтересованной стороне использовать сигналы ответа самолетного ответчика как для дальнего обнаружения воздушных объектов, так и для измерения их координат. И, как следствие, позволяет исключить несанкционированное использование самолетного ответчика запросных радиолокационных систем наблюдения воздушного пространства заинтересованной стороной для подавления канала ответа, а, следовательно, позволяет повысить относительную пропускную способность рассматриваемых информационных систем.

Ключевые слова: запросные системы; радиолокация; радиолокационная система; система наблюдения воздушного пространства; относительная пропускная способность; самолетный ответчик; широкополосные сигналы; сигнал запроса; сигнал ответа; помеха.

Ил. 5. Библиогр.: 31 назв.

UDC 621.396.96, 621.397.48:004.932.2

The use of UAV interceptors to increase the detection range of intruder drones / *V.M. Kartashov, V.A. Kizka, V.A. Tikhonov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2022. №208. P. 38 – 43.

Various threats of terrorist attacks on the social infrastructure arise due to strengthening of terrorist organizations, both in the context of their coming to power in certain countries (Afghanistan), and their association with the drug business, which significantly increases the financing of terrorist structures, allowing them to acquire modern weapons. Unmanned aerial vehicles (UAVs) are cheap, readily available and capable of carrying containers of lethal agents, what make them a common means of terrorist attack. Effective protection of critical industrial facilities from UAV terrorist attacks is an important task for improving systems and means of electronic warfare against terrorism.

This paper considers the possibility of detecting an UAV near a critically important industrial facility using small-sized radar stations (SRS) placed on board of UAV-interceptors. Typically, SRS are placed on board drones for radio mapping of the terrain, operational-tactical and reconnaissance combat missions, and rescue operations. The possibility of using SRS on board interceptor drones to detect intruder drones as an additional channel to a remote radar channel has not been considered anywhere before.

The paper provides a review of existing small-sized radar stations (SRS) that can be used or are used on-board of UAVs, as well as a review of existing UAV-interceptors. It is shown that UAV-interceptors equipped with SRS can be used to fly around the area about a critical industrial facility, by analogy with overflights performed by multicopters around agricultural areas, with recharging in specially equipped places for this at different distances from the control center and from critical industrial facility.

A method is proposed to increase the existing optical and acoustic channel for detecting an intruder drone by an order of magnitude, and the radar channel by 5 km, if not only small-sized radar, but also optoelectronic with the acoustic UAV detection system are installed on the UAV-interceptor with the integrated use of these channels with remote radar UAV detection system.

Key words: unmanned aerial vehicle; detection; small-sized radar station; UAV-interceptor; intruder drone.

1 fig. Ref: 26 items.

УДК 621.396.96, 621.397.48:004.932.2

Використання БПЛА-перехоплювачів для збільшення дальності виявлення дронів-порушників / *В.М. Карташов, В.О. Кізка, В.А. Тихонов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2022. Вип. 208. С. 38 – 43.

Через посилення терористичних організацій як у зв'язку з приходом їх до влади в окремих країнах (Афганістан), так і за рахунок їх об'єднання з наркобізнесом, що суттєво збільшує фінансування терористичних структур, дозволяючи їм набувати сучасної зброї, з'являються різні загрози терористичних атак соціальної інфраструктури. Поширеним засобом терористичної атаки все частіше стають безпілотні літальні апарати (БПЛА), які дешеві, доступні в придбанні і здатні переносити контейнери з вражаючими речовинами. Ефективний захист критично важливих індустріальних об'єктів від терористичних атак БПЛА є важливим завданням удосконалення систем та засобів радіоелектронної боротьби з тероризмом.

Стаття розглядає можливість виявлення БПЛА поблизу критично важливого індустріального об'єкта за допомогою малогабаритних радіолокаційних станцій (МРЛС), розміщених на борту БПЛА-перехоплювачів. Зазвичай МРЛС розміщуються на борту дронів для радіокартографування місцевості, оперативно-тактичних і розвідувальних бойових завдань, рятувальних операцій. Можливість використання МРЛС на борту дронів-

перехоплювачів для виявлення дронів-порушників як додаткового каналу до дистанційного РЛС каналу ніде раніше не розглядалася.

У статті проведено огляд існуючих МРЛС, які можуть використовуватися або використовуються як бортові на БПЛА, а також проведено огляд існуючих БПЛА-перехоплювачів. Показано, що БПЛА-перехоплювачі, оснащені МРЛС, можна використовувати для обльоту місцевості навколо критично важливого промислового об'єкта за аналогією з обльотами, що здійснюються мультикоптерами навколо сільгосп-місцевостей, з підзарядкою в спеціально обладнаних для цього місцях на різній відстані від центру управління та від критично важливого індустріального об'єкта.

Запропоновано спосіб збільшення існуючих оптичного та акустичного каналу виявлення БПЛА-порушника на порядок, а радіолокаційного каналу на 5 км, якщо на БПЛА-перехоплювач встановити не тільки МРЛС, але й оптико-електронну з акустичною системи виявлення БПЛА при комплексному застосуванні цих каналів з дистанційною радіолокаційною системою виявлення БПЛА.

Ключові слова: безпілотний літальний апарат; виявлення; малогабаритна радіолокаційна станція; БПЛА-перехоплювач; дрон-порушник.

Іл. 1. Бібліогр.: 26 назв.

УДК 621.396.96, 621.397.48:004.932.2

Использование БПЛА-перехватчиков для увеличения дальности обнаружения дронов-нарушителей / *В.М. Карташов, В.А. Кизка, В.А. Тихонов* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2022. Вып. 208. С. 38 – 43.

Из-за усиления террористических организаций как в связи с приходом их к власти в отдельных странах (Афганистан), так и за счет их объединения с наркобизнесом, что существенно увеличивает финансирование террористических структур, позволяя им приобретать современное оружие, появляются различные угрозы террористических атак социальной инфраструктуры. Распространенным средством террористической атаки всё чаще становятся беспилотные летательные аппараты (БПЛА), которые дешёвые, легкодоступные в приобретении и способны переносить контейнеры с поражающими веществами. Эффективная защита критически важных объектов от террористических атак БПЛА является важной задачей совершенствования систем и средств радиоэлектронной борьбы с терроризмом.

Статья рассматривает возможность обнаружения БПЛА вблизи критически важного индустриального объекта с помощью малогабаритных радиолокационных станций (МРЛС), размещенных на борту БПЛА-перехватчиков. Обычно МРЛС размещаются на борту дронов для радиокартографирования местности, оперативно-тактических и разведывательных боевых задач, спасательных операций. Возможность использования МРЛС на борту дронов-перехватчиков для обнаружения дронов-нарушителей как дополнительного канала к дистанционному РЛС каналу нигде до этого не рассматривалась.

В статье проведен обзор существующих МРЛС, которые могут использоваться или используются как бортовые на БПЛА, а также проведен обзор существующих БПЛА-перехватчиков. Показано, что БПЛА-перехватчики, оснащенные МРЛС, можно использовать для облета местности вокруг критически важного промышленного объекта по аналогии с облетами, совершаемыми мультикоптерами вокруг сельхоз-местностей, с подзарядкой в специально оборудованных для этого местах на разном расстоянии от центра управления и от критически важного индустриального объекта.

Предложен способ увеличения существующих оптического и акустического канала обнаружения БПЛА-нарушителя на порядок, а радиолокационного канала на 5 км, если на БПЛА-перехватчик установить не только МРЛС, но и оптоэлектронную с акустической системы обнаружения БПЛА при комплексном применении этих каналов с дистанционной радиолокационной системой обнаружения БПЛА.

Ключевые слова: беспилотный летательный аппарат; обнаружение; малогабаритная радиолокационная станция; БПЛА-перехватчик; дрон-нарушитель.

Ил. 1. Библиогр.: 26 назв.

UDC 621.396.967.2

Comparative analysis of noise immunity of the information transmission channel of secondary radar systems / *I.V. Svyd, I.Yu. Vorgul, S.V. Starokozhev, M.G. Tkach, O.S. Maltsev, I.O. Shevtsov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2022. № 208. P. 44 – 54.

This paper presents the conducted assessment of noise immunity of the request signal transmission channel and response channel for flight information of secondary radar systems as part of aircraft responders. The considered system is an open single-channel queuing system with refusing due to the action in the request channel of intentional and unintentional correlated and uncorrelated (intra-system) interference and ground-based receivers that receive, process and decode flight information in the presence of fluctuation and intra-system interference in the receiving channel. The results of assessing the noise immunity of the aircraft responder in the form of the aircraft responder's readiness factor under the action of internal and deliberate interference are given. It is shown that the principle of constructing an aircraft responder and the principle of servicing request signals and transmitting flight information do not allow ensuring acceptable probabilities of obtaining flight data at ground control points.

Key words: secondary radar systems; aircraft responder; single-channel queuing system with refusing; intentional interference; unintentional interference; intra-system interference, noise immunity.

4 fig. Ref: 43 items.

УДК 621.396.967.2

Порівняльний аналіз завадостійкості каналу передачі інформації вторинних радіолокаційних систем / *І.В. Свид, І.Ю. Воргуль, С.В. Старокожев, М.Г. Ткач, О.С. Мальцев, І.О. Шевцов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2022. Вип. 208. С. 44 – 54.

У роботі наведено оцінку завадостійкості каналу передачі сигналів запиту та каналу відповіді польотної інформації вторинних радіолокаційних систем у складі літакових відповідачів. Розглянута система являє собою відкриту одноканальну систему масового обслуговування з відмовами при дії в каналі запиту навмисних і ненавмисних або корельованих і некорельованих (внутрісистемних) завад та наземних приймачів, що здійснюють прийом, обробку та декодування польотної інформації за наявності в каналі прийому флуктуаційних та внутрісистемних завад. Наведено результати оцінки завадостійкості літакового відповідача як коефіцієнта готовності літакового відповідача при дії внутрісистемних і навмисних завад. Показано, що принцип побудови літакового відповідача та принцип обслуговування сигналів запиту та передачі польотної інформації не дозволяє забезпечити допустимі ймовірності отримання польотних даних на наземних пунктах управління.

Ключові слова: вторинні радіолокаційні системи; літаковий відповідач; одноканальна система масового обслуговування з відмовами; навмисні завади; ненавмисні завади; внутрісистемні завади; завадостійкість.

Іл. 4. Бібліогр.: 43 назв.

УДК 621.396.967.2

Сравнительный анализ помехоустойчивости канала передачи информации вторичных радиолокационных систем / *И.В. Свид, И.Ю. Воргуль, С.В. Старокожев, М.Г. Ткач, А.С. Мальцев, И.А. Шевцов* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2022. Вып. 208. С. 44 – 54.

В работе проведена оценка помехоустойчивости канала передачи сигналов запроса и канала ответа полетной информации вторичных радиолокационных систем в составе самолетных ответчиков. Рассматриваемая система представляет собой открытую одноканальную систему массового обслуживания с отказами при действии в канале запроса преднамеренных и непреднамеренных или коррелированных и некоррелированных (внутрисистемных) помех и наземных приемников, осуществляющих прием, обработку и декодирование полетной информации при наличии в канале прима флуктуационных и внутрисистемных помех. Приведены результаты оценки помехоустойчивости самолетного ответчика в виде коэффициента готовности самолетного ответчика при действии внутрисистемных и преднамеренных помех. Показано, что принцип построения самолетного ответчика и принцип обслуживания сигналов запроса и передачи полетной информации не позволяю обеспечить допустимые вероятности получения полетных данных на наземных пунктах управления.

Ключевые слова: вторичные радиолокационные системы; самолетный ответчик; одноканальная система массового обслуживания с отказами; преднамеренные помехи; непреднамеренные помехи; внутрисистемные помехи; помехоустойчивость.

Ил. 4. Библиогр.: 43 назв.

TELECOMMUNICATIONS MEAS
ЗАСОБИ ТЕЛЕКОМУНІКАЦІЙ
СРЕДСТВА ТЕЛЕКОММУНИКАЦИЙ

UDC 621.396.004

Features of building virtual PBX / *L.O. Tokar* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2022. №208. P. 55 – 64.

The article considers the features of organizing highly efficient telephone communication using cloud-based PBXs.

The advantages of solutions based on IP-telephony compared to classical automatic telephone exchanges are treated. It is shown that the use of a virtual PBX as a separate configuration of a dedicated server will provide a flexible system of settings.

The virtualization model is considered. The analysis of virtualization methods is carried out and it is noted that the result of their development is the emergence of multi-core processors, an increase in the throughput of computer interfaces, an increase in the capacity and speed of data storage systems. It is shown that each of these methods differs in hardware emulation methods and finds its place depending on the application.

A solution using the Asterisk software product is considered for organizing the IP-telephony. The configuration of the virtualization environment setting is discussed. It is proposed to use a reliable PROXMOX VE infrastructure, which is an open source virtualization system and support for live migration.

Studies have been carried out to determine the performance parameters of virtualization technologies, namely, hypervisor and container ones. It is noted that the main peak of the load on the OP is the assembly of the system from binary files, which requires significantly more resources (the load increases by about 2 times) than the preparation of these files. During the CPU load analysis, the virtual machine was found to be very demanding. It has been proven that

virtual machines with hypervisor virtualization technology consume more server hardware resources than virtual machines with container virtualization technology.

Key words: virtualization; containerization; cloud PBX; hypervisor; hardware emulation; Asterisk.

6 tab. 8 fig. Ref: 15 items.

УДК 621.396.004

Особливості побудови віртуальних АТС / *Л.О. Токар* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2022. Вип. 208. С. 55 – 64.

У статті розглянуто особливості організації високоефективного телефонного зв'язку за допомогою хмарних АТС.

Розглянуто переваги рішень на основі IP-телефонії у порівнянні з класичними АТС. Показано, що використання віртуальної АТС не як додаткового сервісу, а як окремої конфігурації виділеного сервера дасть можливість отримати гнучку та доступну систему для налаштувань.

Розглянуто модель віртуалізації. Проведено аналіз методів віртуалізації та відмічено, що результатом їх розвитку є поява багатоядерних процесорів, зріст пропускної здатності інтерфейсів комп'ютерів, а також збільшення ємності та швидкодії систем зберігання даних. Показано, що кожен з цих методів відрізняється способами емуляції апаратних засобів та знаходить своє місце в залежності від області застосування.

Для організації IP-телефонії розглянуто рішення з використанням програмного продукту Asterisk. Розглянуто конфігурацію налаштування середовища віртуалізації. Запропоновано використати надійну інфраструктуру PROXMOX VE, яка є системою віртуалізації з відкритим вихідним кодом і підтримує динамічну міграцію.

Проведено дослідження для визначення параметрів продуктивності двох технологій віртуалізації - гіпервізорної та контейнерної. Зазначено, що основним піком навантаження на ОП є складання системи з двійкових файлів, що та вимагає істотно більше ресурсів (навантаження зростає приблизно в 2 рази), ніж підготовка цих файлів. У ході аналізу навантаження на CPU виявлено більшу вимогливість віртуальної машини. Доведено, що віртуальні машини, що використовують технологію гіпервізорної віртуалізації, споживають більше апаратних ресурсів сервера, ніж контейнери, працюючі на технології контейнерної віртуалізації.

Ключові слова: віртуалізація; контейнеризація; хмарна АТС; гіпервізор; емуляція обладнання; Asterisk.

Табл. 6. Іл.8. Бібліогр.: 15 назв.

УДК 621.396.004

Особенности построения виртуальных АТС / *Л.А. Токарь* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2022. Вып. 208. С. 55 – 64.

В статье рассмотрены особенности организации высокоэффективной телефонной связи с помощью облачных АТС.

Рассмотрены преимущества решений на основе IP-телефонии по сравнению с классическими АТС. Показано, что использование виртуальной АТС не в качестве дополнительного сервиса, а в качестве отдельной конфигурации выделенного сервера, позволит получить гибкую систему настроек.

Рассмотрена модель виртуализации. Проведен анализ методов виртуализации и отмечено, что результатом их развития является появление многоядерных процессоров, рост пропускной способности интерфейсов компьютеров, увеличение емкости и быстродействия систем хранения данных. Показано, что каждый из этих методов отличается способами эмуляции аппаратных средств и находит свое место в зависимости от области применения.

Для организации IP-телефонии рассматрено решение с использованием программного продукта Asterisk. Рассмотрена конфигурация настройки среды виртуализации. Предложено использовать надежную инфраструктуру PROXMOX VE, являющуюся системой виртуализации с открытым исходным кодом и поддержкой динамической миграции.

Проведены исследования для определения параметров производительности технологий виртуализации – гипервизорной и контейнерной. Отмечено, что основным пиком нагрузки на ОП является сборка системы из двоичных файлов, что требует существенно больше ресурсов (нагрузка возрастает примерно в 2 раза), чем подготовка этих файлов. В ходе анализа нагрузки на CPU обнаружена большая требовательность виртуальной машины. Доказано, что виртуальные машины с технологией гипервизорной виртуализации потребляют больше аппаратных ресурсов сервера, чем виртуальные машины с технологией контейнерной виртуализации.

Ключевые слова: виртуализация; контейнеризация; облачная АТС; гипервизор; эмуляция оборудования; Asterisk.

Табл. 6. Ил.8. Библиогр.: 15 назв.

PHYSICS OF DEVICES, ELEMENTS AND SYSTEMS
ФІЗИКА ПРИЛАДІВ, ЕЛЕМЕНТІВ І СИСТЕМ
ФИЗИКА ПРИБОРОВ, ЭЛЕМЕНТОВ И СИСТЕМ

UDC 621.382.232

Influence of the active region structure of the resonant tunneling diode on the critical points of its current-voltage characteristic / *K.S. Yatsun* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2022. №208. P. 65 – 71.

The article proposes a study of the effect of the structure of the active region of a resonant tunneling diode on the critical points of its current-voltage characteristic. The basic configuration of a resonant tunneling diode, which is a structure of a quantum well with a nanometer-sized double barrier including two contacts, and a region with strongly doped contacts made of a semiconductor with a relatively small band gap, is disclosed and illustrated. It is emphasized that since the characteristic dimensions of the structure of the quantum well with a double barrier are comparable to the wavelengths of electrons, the wave nature of electrons leads to such quantum phenomena as interference, tunneling, energy quantization, etc. the double barrier causes resonant tunneling phenomena, which form the basis for the operation of the resonant-tunneling diode. It is emphasized that repeated reflection causes destructive or constructive interference depending on the wavelength of a particular electron. For electrons with a certain wavelength that promotes constructive interference, a transfer probability close to unity can be found at energies corresponding to these wavelengths. The modification of the active region of the resonant tunnel diode with a barrier height of 0.3 - 0.4 eV is mathematically substantiated. The dependence of the transmission coefficient is found by solving the Schrödinger equation in one electron approximation without taking into account the scattering effects. The calculation of the volt-ampere characteristic of the resonant-tunnel diode was performed at temperatures of 100 and 300 K. The given volt-ampere characteristics were obtained without taking into account the effects of electron scattering. However, it should be noted that the main influencing factor is the resonant tunneling through the second level, for which the peak of the transmission coefficient is much wider and higher. However, in gallium doped arsenide, the fact of electron scattering can significantly affect the value of the transmission coefficient and the value of current. It is established that an increase in the width of quantum wells leads to a significant decrease in the densities of peak currents and valley currents, and an increase in the width of potential barriers leads to a slight decrease in the current density of the first peak and current densities of the second peak and valley.

Key words: resonant-tunnel diode; volt-ampere characteristic; barrier; tunneling; quantum well; structure; energy; wave.

2 fig. Ref: 15 items.

УДК 621.382.232

Вплив структури активної області резонансно-тунельного діоду на критичні точки його вольт-амперної характеристики / *К.С. Яцун* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2022. Вип. 208. С. 65 – 71.

У статті запропоновано дослідження впливу структури активної області резонансно-тунельного діоду на критичні точки його вольт-амперної характеристики. Розкрито та проілюстровано основну конфігурацію резонансно-тунельного діода, яка являє собою структуру квантової ями з подвійним бар'єром нанометрових розмірів, що включає два контакти, та області з сильно легованими контактами, виготовленими з напівпровідника з відносно малою забороненою зоною. Наголошено, що оскільки характерні розміри структури квантової ями з подвійним бар'єром порівняні з довжинами хвиль електронів, хвильова природа електронів призводить до таких квантових явищ, як інтерференція, тунелювання, квантування енергії тощо та зазначається, що в результаті зазначеного явища в структурах квантової ями з подвійним бар'єром виникають резонансні явища тунелювання, які утворюють основу для роботи резонансно-тунельного діода. Підкреслено, що багаторазове відображення викликає деструктивні або конструктивні перешкоди залежно від довжини хвилі конкретного електрона. Для електронів із певною довжиною хвилі, що сприяє конструктивній інтерференції, ймовірність передачі, близька до одиниці, може бути знайдена при енергіях, що відповідають цим довжинам хвиль. Математично обґрунтовано модифікацію активної області резонансно-тунельного діода з висотою бар’єра 0,3 – 0,4 еВ. Залежність коефіцієнта проходження знаходимо шляхом вирішення рівняння Шредінгера у одно електронному наближенні без урахування ефектів розсіяння. Розрахунок вольт-амперної характеристики резонансно-тунельного діода здійснено при температурах у 100 та 300 К. Наведені вольт-амперні характеристики отримані без врахування ефектів розсіяння електронів. Однак варто відмітити, що головним впливовим фактором є резонансне тунелювання через другий рівень, для якого пік коефіцієнта проходження значно ширше та вище. Проте у легованому арсеніді галію факт розсіяння електронів може суттєво надавати вплив на значення коефіцієнта проходження та значення струму. Встановлено, що збільшення ширини квантових ям призводить до істотного зменшення щільностей пікових струмів і струмів долини, а збільшення ширини потенційних бар'єрів призводить до незначного зменшення щільності струму першого піку, а також збільшення щільностей струмів другого піку і долини.

Ключові слова: резонансно-тунельний діод; вольт-амперна характеристика; бар’єр; тунелювання; квантова яма; структура; енергія; хвиля.

Іл. 2. Бібліогр.: 15 назв.

УДК 621.382.232

Влияние структуры активной области резонансно-туннельного диода на критические точки его вольт-амперной характеристики / *К.С. Яцун* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2022. Вып. 208. С. 65 – 71.

В статье предложено исследование влияния структуры активной области резонансно-туннельного диода на критические точки его вольт-амперной характеристики. Раскрыта и проиллюстрирована основная конфигурация резонансно-туннельного диода, которая представляет из себя структуру квантовой ямы с двойным барьером нанометровых размеров, которая включает в себя два контакта, и области с сильно легированными контактами, изготовленных из полупроводника с относительно малой запрещенной зоной. Отмечено, что поскольку

характерные размеры структуры квантовой ямы с двойным барьером соизмеримы с длинами волн электронов, волновая природа электронов приводит к таким квантовым явлениям, как интерференция, туннелирование, квантование энергии и т.п. и отмечается, что в результате обозначенного явления в структурах квантовой ямы с двойным барьером возникают резонансные явления туннелирования, которые создают основу для работы резонансно-туннельного диода. Отмечено, что многоразовое отображение вызывает деструктивные или конструктивные помехи в зависимости от длины волны конкретного электрона. Для электронов с определенной длиной волны, которая способствует конструктивной интерференции, вероятность передачи, близкая к единице, может быть обнаружена при энергиях, которые отвечают этим волновым длинам. Математически обосновано модификацию активной области резонансно-туннельного диода с высотой барьера 0,3 – 0,4 В. Зависимость коэффициента прохождение получено путем решения уравнения Шредингера в одно электронном приближении без учета эффектов рассеивания. Расчет вольт-амперной характеристики резонансно-туннельного диода выполнен при температурах 100 и 300 К. Приведенные вольт-амперные характеристики получены без учета эффектов рассеивание электронов. Однако стоит отметить, что главным влияющим фактором является резонансное туннелирование через второй уровень, для которого пик коэффициента прохождения значительно выше и шире. Тем не менее в легированном арсениде галия факт рассеивания электронов может существенно влиять на значение коэффициента прохождения и значение тока. Установлено, что увеличение ширины квантовых ям приводит к существенному уменьшению плотностей токов пика и токов долины, а увеличение ширины потенциальных барьеров приводит к незначительному уменьшению плотности тока первого пика, а также увеличению плотности тока второго пика и долины.

Ключевые слова: резонансно-туннельный диод; вольт-амперная характеристика; барьер; туннелирование; квантовая яма; структура; энергия; волна.

Ил. 2. Библиогр.: 15 назв.

COLLECTION OF SCIENTIFIC PAPERS
RADIOTEKHNIKA
Issue 208
In English, Ukrainian and Russian

ЗБІРНИК НАУКОВИХ ПРАЦЬ
РАДІОТЕХНІКА
Випуск 208
Англійською, українською, та російською мовами

СБОРНИК НАУЧНЫХ ТРУДОВ
РАДИОТЕХНИКА
Выпуск 208
На английском, украинском и русском языках

Коректор Л.І. Сащенко

Підп. до друку 30.03.2022. Формат 60x90/8. Папір офсет. Гарнітура Таймс. Друк. ризограф.
Ум. друк. арк**.** 10,4. Обл.-вид. арк. 9,36. Тираж 300 прим. Зам. № 478. 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.