МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ
УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ

РАДІОТЕХНІКА

Всеукраїнський міжвідомчий науково-технічний збірник

Засновано в 1965 р.

В И П У С К 2 0 7

Харків
Харківський національний
університет радіоелектроніки
2021

УДК 621.3

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

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

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

Сайт: rt.nure.ua

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

За зміст статті відповідальні автори.

Відповідальні за випуск: *І.Д. Горбенко, д-р техн. наук, проф.*, *І.В. Свид, канд. техн. наук, доц.*
Технічний секретар *О.С. Полякова.*

Рекомендовано Вченою радою Харківського національного університету радіоелектроніки, протокол №11/15 від 24.12.2021.

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

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

ЗМІСТ

CONTENT

МЕТОДИ ПЕРСПЕКТИВНИХ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ
МЕТОДЫ ПЕРСПЕКТИВНЫХ КРИПТОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ
METHODS OF PROMISING CRYPTOGRAPHIC TRANSFORMATIONS

УДК 004.056.55 **DOI:10.30837/rt.2021.4.207.01**

І.Д. ГОРБЕНКО, д-р техн. наук, О.Г. КАЧКО, канд. техн. наук, О.В. ПОТІЙ, д-р техн. наук,
Ю.І. ГОРБЕНКО, канд. техн. наук, В.А. ПОНОМАР, канд. техн. наук,
М.В. ЄСІНА, канд. техн. наук, І.В. СТЕЛЬНИК, С.О. КАНДІЙ, К.О.КУЗНЕЦОВА

ОБҐРУНТУВАННЯ ТА ПРОПОЗИЦІЇ ЩОДО ВИБОРУ, УДОСКОНАЛЕННЯ ТА СТАНДАРТИЗАЦІЇ МЕХАНІЗМУ ПОСТКВАНТОВОГО ЕЛЕКТРОННОГО ПІДПИСУ НА НАЦІОНАЛЬНОМУ ТА МІЖНАРОДНОМУ РІВНЯХ

Вступ

Наразі, та очевидно в перспективі, для криптографічного захисту інформації (КЗІ) застосовуються та будуть застосовуватись математичні методи, механізми та алгоритми стандартизованих асиметричних криптоперетворень типу електронний підпис (ЕП). Він є основною та суттєвою складовою забезпечення кібербезпеки у сенсі якісного надання таких послуг з безпеки інформації як цілісність, неспростовність та автентичність інформації та даних, що обробляються [1 – 4]. Але є реально обґрунтовані підозри, що у постквантовий період існуючі стандарти ЕП будуть зламуватись та компрометуватись з використанням класичних та квантових криптоаналітичних систем з відповідним математичним, програмним та апаратно-програмним забезпеченням [5 – 13].

Аналіз підтвердив, що уже практично розроблені, виготовлені та застосовуються квантові комп'ютери. Стан створення та можливості застосування квантових комп'ютерів для вирішення задач криптоаналізу можна оцінити наступним чином [1 – 13].

Згідно з [9 – 11] IBM розробила та представила квантовий 127-кубітний процесор Eagle. Він прийшов на зміну 65-кубітному квантовому процесору Hummingbird, що відповідає дорожній карті квантових технологій від IBM [10].

Є відомості [10, 12] про наміри IBM представити 433-кубітний процесор Osprey в 2022 р., а 1121-кубітний процесор Condor – в 2023 р. Вказане відповідає дорожній карті, наведеній в [10]. В [10] також зазначено, що відмінність Eagle від попередніх процесорів полягає в тому, що він потребує, завдяки застосуванню мультиплексування зчитування, на кубіт регістрі значно меншої кількості електроніки для контролю та зчитування. Також IBM повідомляє про наміри щодо побудови на основі покращених чіпів нової інтегрованої квантової обчислювальної системи IBM Quantum System Two замість вже існуючої системи IBM Quantum System One.

Компанія D-Wave [13], що відома своїми розробками в сфері побудови псевдоквантових (гібридних) комп'ютерів з великою загальною кількістю кубітів (понад 2000 кубітів на початку та понад 5000 кубітів сьогодні), повідомила про наміри представити машину із загальною кількістю кубітів понад 7000 приблизно в 2023 – 2024 рр. та про наміри щодо розробки власних комп'ютерів для провідникових квантових машин гейтового типу (розробкою яких наразі займаються IBM, Google та інші).

На наш погляд, цим даним можна довіряти, але зрозуміло, що фактичний стан розроблення та застосування потужних квантових комп'ютерів та їх математичного і програмного забезпечень є, очевидно, строго конфіденційним та надійно захищається, а розголошуються тільки явно відомі дані про квантові комп'ютери та їх можливості застосування в криптології. Дані, що наведені вище, певною мірою нами перевірені практично [8].

Вирішення вказаної проблеми кібербезпеки та безпеки інформації у цілому в перехідний та постквантовий періоди може бути здійснено на основі розроблення, прийняття та застосування як на міжнародному, так і національному рівнях, в тому числі стандартизованих постквантових ЕП. Вказане може досягатись суттєвим обґрунтуванням, розробкою пропозицій щодо застосування нових математичних методів та механізмів криптоперетворень типу ЕП [1 – 4, 23 – 28] на основі існуючих альтернатив та відповідних моделей безпеки [14 – 19].

Таким чином, зважаючи на можливості та перспективи зламу існуючих асиметричних криптосистем типу ЕП, Національний інститут стандартів і технологій (NIST) США закінчив та прийняв рішення у вигляді проєкту стандарту NIST 8309 щодо 2-го раунду конкурсу на перспективні стандарти асиметричних криптоперетворень [4, 24 – 28]. Визначені фіналісти типу ЕП 2-го етапу конкурсу ґрунтуються на методах Crystals-Dilithium [24, 25, 30 – 33], Falcon [26] та Rainbow [28]. Визначено також три альтернативні кандидати на міжнародний постквантовий стандарт ЕП – GeMSS, Picnic та SPHINCS+ [4], які потребують більш детальних досліджень, скоріше всього на 4-му етапі конкурсу.

Попередній аналіз показав, що в Україні є розуміння існування загроз кібербезпеці та безпеці інформації у випадку застосування у перехідний та постквантовий періоди існуючих стандартизованих ЕП. Розроблено та прийнято національний стандарт «Алгоритми асиметричного шифрування та інкапсуляції ключів» (ДСТУ 8961-2019), що побудований на основі застосування криптоперетворень на алгебраїчних решітках. Особливістю цього стандарту є суттєве підвищення криптографічної стійкості асиметричного шифрування та інкапсуляції ключів у перехідний та постквантовий період проти усіх відомих класичних, квантових, спеціальних атак та атак на основі помилок [17 – 19]. Тому, по суті, наразі одним із основних проблемних питань щодо забезпечення необхідних рівнів безпеки в перехідний та постквантовий періоди є також розробка та прийняття постквантових стандартів ЕП.

Метою цієї статті є обґрунтування, порівняння альтернатив та розробка пропозицій щодо вибору та стандартизації постквантових стандартів ЕП на міжнародному та національному рівнях з урахування результатів 2-го та 3-го раундів конкурсу NIST США [4] та національних досліджень [6 – 8, 24, 27].

1. Аналіз альтернатив та вибір методу (схеми) розробки та прийняття постквантового стандарту ЕП на національному та міжнародному рівнях

Аналіз показав [4, 20 – 28], що серед постквантових механізмів (схем) ЕП суттєві переваги надані проєктам ЕП Crystals-Dilithium [23, 30, 31], Falcon [26] та Rainbow [28]. Вони рекомендовані для подальшого дослідження та стандартизації в процесі 3-го етапу конкурсу та, по суті, є фіналістами конкурсу NIST США. Причому кращими визначено як математичні основи, так і алгоритми ЕП Crystals-Dilithium [6, 11 – 13]. ЕП Falcon досліджувався на 2-му раунді як один із трьох проєктів стандартів ЕП. Основним та домінуючим підходом до проєктування механізму ЕП Falcon є використання парадигми «геш і підпис» [26]. Його перевагою є доказова стійкість в межах моделі квантового випадкового оракула. Але його аналізу присвячено значно менше робіт, ніж, наприклад, щодо Crystals-Dilithium та Rainbow.

У [26, 27] представлено удосконалений варіант схеми ЕП Falcon. Вказана удосконалена реалізація варіанту ЕП Falcon забезпечує постійний час виконання операцій перетворень. Вона може реалізуватись без використання апаратного забезпечення, хоча при його використанні може досягатись вища продуктивність. В новій реалізації необхідний менший обсяг оперативної пам’яті, вона більш ефективна як у великих системах (x86 з ядрами Skylake, POWER8 тощо), так і на малих мікроконтролерах (ARM Cortex M4) [26].

Основними властивостями ЕП Falcon є наступні [26, 27].

1. В ЕП Falcon для криптоперетворень використовується вибірка Гауса, розроблена Престом, Рікоссетом та Россі. Така вибірка використовує вибірку з відхиленнями з ретельно налаштованими параметрами таким чином, що спостереження за швидкістю відхилення не дає ніякої статистично корисної інформації щодо особистих ключів при усіх параметрах безпеки.

2. Проблемним було використання плаваючої точки, що приводило до появи неконстантних операцій, наприклад множення поліномів. Щоб уникнути будь-яких неконстантних операцій під час ЕП, їх було оптимізовано. Зокрема, ділення та квадратні корені використовуються лише при генерації ключів і не можуть викрити навіть незначної інформації про особистий ключ.

3. Весь доступ до пам'яті засобів реалізації здійснюється за несекретними адресами. Причому шаблон доступу до пам'яті не залежить від будь-якої секретної інформації, як для генерування ключів, так і для вироблення ЕП.

4. В реалізації ЕП Falcon не потрібна підтримка операцій з плаваючою точкою. Хоча така реалізація може використовувати апаратне забезпечення з плаваючою точкою, коли вона доступна. Вона включає код емуляції з плаваючою точкою, який забезпечує використання лише операції з цілими числами. Такий код емуляції характеризується повністю постійним часом виконання перетворень для всіх значень, які можуть з'являтися, і переноситься на всі платформи, що мають, наприклад, компілятор C99 і звичайні типи цілочисельних значень фіксованої ширини (uint32_t, uint64_t).

5. Нова реалізація Falcon є більш швидкою та ефективна при роботі з RAM. Так, коли підтримуються операційні коди AVX2, то така реалізація може їх використовувати в Falcon-512 на Intel Core i7-6567U на частоті 3,3 ГГц [26]. При цьому, якщо використовується одне ядро, то за секунду можна генерувати приблизно 7700 ЕП. Також можна реалізувати варіант зі зменшеним обсягом RAM. За цієї умови ЕП може бути обчислений для Falcon-512 у межах менше, ніж 40 кБ оперативної пам’яті. Це досягається для тимчасових значень та незначного використання простору стека, при цьому досягається приблизно 3800 підписів в секунду.

6. З використанням процесорів ARM Cortex M4 для підвищення продуктивності були додані спеціальні вбудовані процедури збірки; варіант із зменшеним використанням оперативної пам’яті. При його застосуванні можна виконати ЕП «Сокіл» та Falcon-512 приблизно за 21,2 мільйона тактів. Але це досягається при застосуванні «розширеного особистого ключа». Безпосередньо розширений ключ обчислюється зі звичайного особистого ключа приблизно за 16,2 млн. тактів і використовує 57,3 кБ оперативної пам’яті.

7. Удосконалена реалізація ЕП «Сокіл» та ЕП Falcon має відкритий код (ліцензія MIT щодо Falcon) та доступна на веб-сайті: https://FALCON-sign.info.

Разом з тим, в удосконаленій версії враховано основні відмінності версії 2.0 Falcon специфікації від версії 1.0 специфікації? Вони полягають у наступному [26].

1) Видалено набір параметрів II – III рівня, що спричинило видалення n=768 та $\varphi=x^n-x^{n/2}+1$. Детально версію 1.1 специфікації, а також еталонну реалізацію наведено в [27].

2) Наведено опис режиму відновлення ключів, який робить Falcon ще більш конкурентоспроможним з точки зору компактності.

Зроблено кілька інших доповнень, які по суті складаються з уточнення та деталізації кількох моментів.

Крім того, під час розроблення обох версій ЕП Falcon, були прийняті обмеження щодо рівнів безпеки, максимально 256 біт проти класичного та 128 біт – проти квантового криптоаналізу [4, 26, 27]. Такі обмеження залишились для проєкту ЕП Falcon також на 3-му етапі міжнародного конкурсу NIST США. Ці обмеження, на наш погляд, пов’язані зі складністю обчислення загальносистемних параметрів, а також із суттєвим впливом їх збільшення параметрів на швидкодію ЕП. Тобто, для безпечного використання ЕП Falcon повинні бути знайдені набори загальносистемних параметрів, за яких забезпечується стійкість до всіх відомих та потенційних атак, тобто класичних, квантових, на основі помилок та спеціальних атак.

В процесі формування вимог до ЕП NIST у рамках конкурсу був зацікавлений тільки в наборах загальносистемних параметрів до 256 біт класичної безпеки включно. Проте, на нашу думку, на перспективу доцільним є забезпечення не менше 384 і 512 біт безпеки проти класичного криптоаналізу та не менше 192 та 256 біт безпеки проти квантового криптоаналізу [29]. Але, як показали дослідження, як з точки зору теорії, так і практики, генерація загальносистемних параметрів для використання 384 і 512 біт безпеки проти класичного криптоаналізу та 192 і 256 біт безпеки проти квантового криптоаналізу є важливою задачею.

Пропозиції щодо розв’язку такої проблеми у вигляді проєкту Національного стандарту у наступному [27, 29].

Розроблення проєкту стандарту має за мету визначення криптографічних алгоритмів ЕП на алгебраїчних решітках для забезпечення послуг цілісності, справжності, доступності та неспростовності інформації та ресурсів, які служать основою надання електронних довірчих послуг під час взаємодії двох або більше суб'єктів, які довіряють надавачу електронних довірчих послуг. Стандарт призначено для використання під час розробки систем, комплексів та засобів криптографічного захисту інформації для надання користувачам послуг цілісності, справжності та неспростовності підписувача в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, в тому числі для захисту від спеціальних атак, а також у постквантовий період.

Основною перевагою проєкту стандарту є доказова стійкість в межах моделі квантового випадкового оракула. Іншими перевагами ЕП «Сокіл » є те, що він забезпечує, у порівнянні з усіма іншими алгоритмами ЕП, мінімальну суму розміру відкритого ключа та розміру підпису, а також ефективні алгоритми підписання та перевірки ЕП, хоча генерація ключів в них відбувається повільніше. Також ЕП «Сокіл» без проблем може вводиться в існуючі протоколи та додатки та забезпечує прийнятну загальну продуктивність. Під час застосування ЕП «Сокіл» є можливість реалізувати його за технологією обробки з відновленням повідомлень.

В алгоритмі асиметричного ЕП «Сокіл» використовують асиметричну пару ключів – особистий (секретний) ключ та відкритий ключ. Для ЕП інформації (даних) використовують особистий (секретний) ключ підписувача, а для перевірки ЕП використовують відкритий ключ перевірки ЕП. На основі перевірки ЕП інформації (даних) отримувачем (перевірником) встановлюється та приймається рішення щодо її цілісності, справжності та неспростовності підписувача тощо.

Прирозробленні стандарту мають бути враховані вимоги щодо забезпечення криптографічної стійкості проти спеціальних атак на основі витоку по технічних каналах, а також потенційних класичних та квантових атак, в тому числі у перехідний та постквантовий періоди. Стандарт розроблено з урахуванням досвіду створення та застосування національних стандартів ДСТУ 7564:2014, ДСТУ 7624:2014, ДСТУ 8845:2019 та ДСТУ 8961:2019.

Стандарт у залежності від рівнів криптографічної стійкості проти класичних та квантових атак, атак сторонніми каналами та на основі помилок, які необхідно забезпечити, можна застосовувати в трьох режимах роботи:

– 128 біт захисту від класичних атак та 64 біт захисту від квантових атак, захист від спеціальних атак сторонніми каналами та на основі помилок (запас стійкості відповідає ДСТУ 7624:2014 (128), AES (128)) (1 режим);

– 256 біт захисту від класичних атак та 128 біт захисту від квантових атак, захист від спеціальних атак сторонніми каналами та на основі помилок (запас стійкості відповідає ДСТУ 7624:2014 (256), AES (256)) (2 режим);

– 512 біт захисту від класичних атак та 256 біт захисту від квантових атак, захист від спеціальних атак сторонніми каналами та на основі помилок (запас стійкості відповідає ДСТУ 7624:2014 (512)) (4 режим).

В кожному із режимів роботи необхідно використовувати криптографічні перетворення та відповідні функції гешування з необхідними розмірами параметрів та ключів.

Важливим є те, що в кожному з вказаних режимів роботи, за рахунок застосування ЕП, для надання послуг цілісності, справжності, доступності та неспростовності використовують алгоритми криптографічних перетворень з відкритими ключами на основі алгебраїчних NTRU решітках з заданою вибіркою, що дозволяє у залежності від вимог, отримати різні рівні безпеки та техніко-економічні і техніко-експлуатаційні характеристики (показники). В цій статті наводяться відповідні результати досліджень з використанням комплексної методики [14 – 16]. Їх аналіз показує, що розроблення та впровадження проєкту національного стандарту «Інформаційні технології. Криптографічний захист інформації. Алгоритми електронного підпису на алгебраїчних NTRU решітках з заданою вибіркою» є актуальною та надзвичайно важливою науково-технічною задачею, вирішення якої спрямоване на забезпечення належного виконання вимог Положення про порядок здійснення криптографічного захисту інформації в Україні, затвердженого Указом Президента України від 22.05.98 № 505, а також тісно пов'язане із виконанням завдань та основних положень Концепції національної безпеки

України, законів України «Про основні засади забезпечення кібербезпеки України» [32], «Про електронні довірчі послуги», «Про захист інформації в інформаційно-телекомунікаційних системах» та інших нормативно-правових актів із захисту національного інформаційного простору України.

Перевагами проєкту стандарту «Сокіл» є доказова стійкість, так як він в межах моделі квантового випадкового оракула. При його використанні будуть забезпечуватись, у порівнянні з усіма іншими алгоритмами ЕП постквантового періоду, мінімальна сума розміру відкритого ключа та розміру підпису, а також ефективні алгоритми підписання та перевірки ЕП, хоча генерація ключів в них відбувається повільніше. Проєкт стандарту ЕП «Сокіл» без проблем може застосовуватись в існуючих протоколах та додатках, забезпечуючи при цьому прийнятну загальну продуктивність. Також ЕП «Сокіл» може ефективно застосовуватись за технологією обробки інформації з відновленням повідомлень.

Наведені результати досліджень дозволили прийняти рішення про перспективність та можливість застосування математичного методу (схеми) Falcon [26] для створення проєкту постквантового національного стандарту ЕП «Сокіл» [27].

2. Сутність математичних методів (схем) (механізмів) ЕП Falcon та «Сокіл»

Проєкти ЕП Falcon [26] та «Сокіл»[27] – це засновані на алгебраїчній решітці механізми ЕП, що використовують парадигму «геш і підпис». Їх стійкість ґрунтується на складності проблеми SIS (коротке ціле рішення) над решітками NTRU, а докази безпеки є як у класичній випадковій моделі оракула (ROM), так і у квантовій моделі оракула QROM. Інтегрально стосовно схеми необхідно відмітити наступне [26, 27]. Необхідно також погодитись, що однією з основних переваг схеми Falcon є те, що вона забезпечує, у порівнянні з усіма іншими схемами ЕП, що були представлені до 2-го раунду конкурсу NIST США та досліджуються на 3-му етапі, мінімальну суму розміру відкритого ключа та розміру ЕП. Також, схема ЕП Falcon забезпечує постійний час виконання операцій перетворень, що дозволяє забезпечити захист і від спеціальних атак. ЕП Falcon та «Сокіл» ефективні при підписанні та перевірці ЕП, хоча генерація ключів в них виконується, у порівнянні, наприклад, з Crystals-Dilithium, повільніше [23, 30, 31]. Також ЕП Falcon [4, 26] та «Сокіл» [27] можуть без особливих проблем вводитися в існуючі протоколи та додатки та забезпечувати загальну продуктивність, що вимагається. Але, ЕП Falcon, при його застосуванні для реалізації ЕП «Сокіл», є складнішим для впровадження, ніж Crystals-Dilithium. Так, він вимагає використання деревоподібних структур даних, операцій з плаваючою комою та випадкової вибірки, по суті, для викривлення коефіцієнтів поліномів, з використанням дискретних гаусових розподілів. Крім того, щодо схеми ЕП на першому етапі її реалізації у детермінованій процедурі ЕП [26] спостерігався потенційний витік (підозри) інформації про особистий ключ.

Генеалогія механізму ЕП Falcon може бути подана у вигляді генеалогічного дерева, що наведене на рис. 1. Безпосередньо схема (метод) та його математична основа є результатом багаторічної праці криптологів та математиків [26]. Значне число досліджень та розробок поступово привели до нинішньої технології ЕП Falcon.

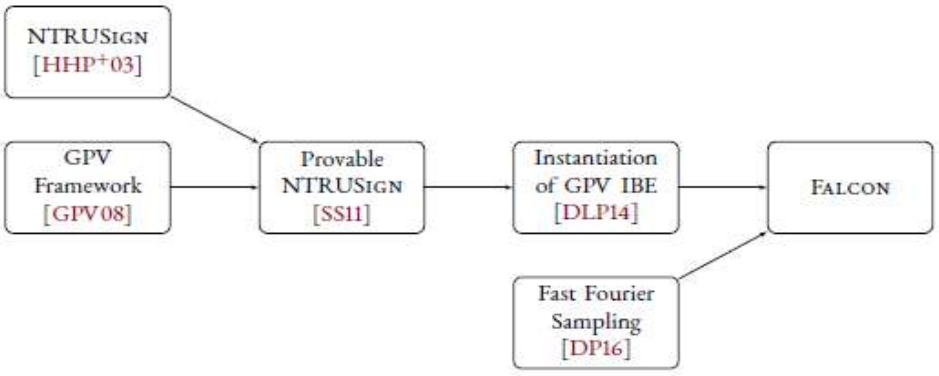


Рис. 1. Генеалогічне дерево Falcon

У 2008 р. Gentry, Peikert і Vaikuntanathan [34, 35] запропонували метод, який дозволив суттєво зменшив вразливість процедури ЕП NTRU. Більше того, зробив це доказово стійким способом. Результатом застосування вказаного способу стала основна платформа (GPV-платформа) побудови захищених ЕП на основі концепції «геш та підпис». Ця платформа будується на основі використання двох специфічних інгредієнтів:

1) Класу криптографічних решіток у вигляді NTRU решіток.
2) Нової методики підвищення безпеки, яка була названа «швидкою вибіркою Фур'є».

Подальший розвиток схеми наведено в [26], де було запропоновано поєднати платформу GPV з решітками NTRU. Результат такого поєднання привів до доказово стійкого NTRUSign. У цілому, коротко, схему підпису на основі схеми Falcon можна подати у такому вигляді:

Falcon = платформа GPV + решітки NTRU + швидка вибірка Фур'є.

Таким чином, схема Falcon ґрунтується на решітках, що уже були випробувані часом в NTRU асиметричному криптоперетворенні. Усі операції в такій конкретній NTRU решітці виконуються над поліномами $\mathbb{Z}[X]$ по модулю $\phi = X^n + 1$, де n – степінь двійки ($n = 512$ для Falcon-512, 1024 – для Falcon-1024 та додатково 2048 – для «Сокіл»). В схемах Falcon та «Сокіл» відкриті ключі, особисті ключі та підписи подаються також у вигляді поліномів, коефіцієнти яких цілі числа, тобто в вигляді $\mathbb{Z}[X]$. Але все ж таки певні проміжні значення перетворень є поліномами, коефіцієнти яких не є цілими числами.

Особистий ключ складається з чотирьох поліномів f, g, F і G, які задовольняють (вирішують) рівняння NTRU виду [26, 27]:

$$fG - gF = q \bmod \phi, \tag{1}$$

де $q = 12289 = 3 \times 2^{12} + 1$ – просте ціле число, що вибрано у такому вигляді для забезпечення використання при множенні поліномів, швидкого NTT множення. Причому коефіцієнти елементів особистого ключа є обмеженими по значенням (малі) цілі числа, їх величину рекомендується змінювати в межах від -127 до +127 [25, 26].

Відкритий ключ подається у вигляді поліному $h = \mathbb{Z}[X]$, коефіцієнти якого можуть змінюватись в інтервалі від 0 до q-1, тобто приймають значення, у порівнянні з особистим ключем та поліномом, що є ЕП, у найбільшому інтервалі – від 0 до 12289, причому

$$fh = g \bmod \phi \bmod q \tag{2}$$

або

$$h = (g / f) \bmod \phi \bmod q. \tag{3}$$

В схемі Falcon значення ЕП також подається у вигляді поліному, але коефіцієнти поліному ЕП рекомендується змінювати в інтервалі від -1080 до +1080 [26, 25].

Таким чином, коефіцієнти полінома особистого ключа рекомендується змінювати в інтервалі від -127 до +127, безпосередньо значення ЕП в інтервалі -1080 до +1080, а значення відкритого ключа у найбільшому інтервалі – від 0 до 1228, а також в менших інтервалах зі вказаними обмеженнями. По суті, застосування у поліномах названих сутностей трьох модулів дозволяє у цілому збільшити ентропію криптографічного перетворення схеми Falcon.

Необхідно також відмітити, що особистий ключ – поліном $f \in \mathbb{Z}[X] \bmod(\phi)$ можна подати [26] у вигляді матриці розміром $n \times n$, кожен *i*-й рядок якої складається з коефіцієнтів

$$f_i = x^i \bmod(\phi(x)). \tag{4}$$

Додавання та множення таких матриць є однозначним додаванню та множенню відповідних поліномів, взятих по модулю $\phi(x)$.

Аналіз показав, що особистий ключ насправді є коротким базисом для решітки $2n \times 2n$ та може бути поданим у матричному вигляді [26]:

$$B = \begin{bmatrix} g & -f \\ G & -F \end{bmatrix}. \quad (5)$$

Також відкритий ключ ж може бути поданий у вигляді основи для тієї ж самої алгебраїчної решітки, але зі збільшеними векторами:

$$p = \begin{bmatrix} -h & I_n \\ qI_n & O_n \end{bmatrix}, \quad (6)$$

де I_n і O_n – одинична і нульова матриці з $n \times n$ розміром відповідно.

Безпосередньо ЕП повідомлення M виконується у такій послідовності:

1) Підписувач, що має доступ до особистого ключа, під час ЕП кожен раз генерує нове випадкове значення (сіль) *r* відповідної довжини.

2) Здійснюється конкатенація та наступне гешування при ЕП кожного нового значення r та повідомлення *M*, що підписується, яке перетворюється в поліном $c \in \left[X\right]/(\phi(x))$ з коефіцієнтами в діапазоні від 0 до $q-1$.

3) Підписувач, використовуючи свій особистий ключ чи знання про свій особистий ключ, обчислює два поліноми s_1 та s_2, але такі, щоби вони задовольняли рівнянню:

$$s_1 + s_2 h = c (\mathrm{mod}\, \phi \,\mathrm{mod}\, q). \quad (7)$$

Безпосередньо ЕП повідомлення *M* є поліномом s_2 та випадкове чи псевдовипадкове *r* значення, що визначає ентропію перетворення типу ЕП.

При перевірці ЕП повідомлення *M*, спочатку обчислюється геш-значення конкатенації значення r та повідомлення *M*, які отримані перевірником, потім воно перетворюється в поліном *c* з коефіцієнтами в діапазоні від 0 до $q-1$. Далі, використовуючи обчислене значення *c*, *в*ідкритий ключ *h* та значення ЕП s_2, обчислюємо

$$s_1 = c - s_2 h \,\mathrm{mod}\, \phi \,\mathrm{mod}\, q. \quad (8)$$

3) Наостанок перевіряється, що складений вектор поліномів (s_1, s_2) розмірності $2n$ дійсно має достатньо низьку (необхідну) норму.

Перевірку ЕП можна виконати повністю за допомогою обчислень над цілими числами по модулю q, а оскільки $2n$ ділить значення $q-1=12288$, то для прискорення множення при перевірці можна використати швидке NTT множення (перетворення). За рахунок цього підвищується швидкодія перевірки ЕП та більш ефективно може використовуватись оперативна пам'ять засобу перевірки.

3. Алгоритми обчислення ключів, основні положення вироблення та перевірки ЕП

3.1. Алгоритм обчислення ключів

В цьому параграфі наводиться системно зібраний алгоритм із доступних джерел та подається з єдиних системних позицій алгоритм генерування ключів для проєктів стандартів ЕП Falcon та «Сокіл» [26, 27].

Етапи обчислення асиметричної пари ключа – особистої та відкритої частин.

Особистий ключ складається з поліномів *f, g, F, G*.

Відкритий ключ складається з поліному *h*.

Далі наведено етапи виконання алгоритму обчислення ключів.

3.1.1. Обчислення компонентів особистого ключа (поліноми *f, g*)

1) Обчислення відкритого ключа (полінома $h=g/f(\mathrm{mod}\ q, \mathrm{mod}\ x^n+1)$);

2) Обчислення компонентів особистого ключа (поліноми *F*, *G*, що повинні бути розв'язком *NTRU* рівняння

$$f*G - g*F = q\ (mod\ x^n+1) \quad (9)$$

Алгоритм обчислення поліномів *f, g*.

Коефіцієнти поліномів *f, g* повинні бути випадковими, знаходитись в інтервалі [-($2^{SK\_0\_BITS}$-1, ($2^{SK\_0\_BITS}$-1], задовольняти розподілу Гауса для $\sigma = 1.17\sqrt{\frac{q}{2n}}$, μ =0, що забезпечує властивості для полінома *h*, як для випадкового полінома [26, 25].

Сума коефіцієнтів для поліному (*f*) та поліному (*g*) повинна бути непарною.

Квадратична норма вектору [*f, g*] не повинна перевищувати *max_norma* = 1.17^2q.

Квадратична норма вектору [*f*', *g*'], ортогонального до вектору [*f, g*], не повинна перевищувати *max_norma* = 1.17^2q.

3.1.2. Алгоритм обчислення відкритого ключа (поліном *h*)

Формула для обчислення:

$$h=g/f\ (mod\ q,\ mod\ x^n+1). \qquad (10)$$

Поліном *f* повинен мати інверсію, що забезпечує можливість обчислення поліному *h*.

3.1.3. Алгоритм обчислення особистого ключа – поліномів *F, G*

Поліноми *F, G* повинні задовольняти NTRU рівнянню (9)

Загальний алгоритм обчислення поліномів *F, G*:

1. Для поліномів *f, g* виконати покроковий перехід від поля x^n+1 до полів $x^{n/2}+1$, $x^{n/4}+1$, … x^1+1. В результаті отримаємо поліноми:

$f^{(n/2)}$ – поліном *f* для поля $x^{n/2}+1$, який має *n*/2 коефіцієнтів;

$g^{(n/2)}$ – поліном *g* для поля $x^{n/2}+1$, який має *n*/2 коефіцієнтів;

$f^{(n/4)}$ – поліном *f* для поля $x^{n/4}+1$, який має *n*/4 коефіцієнтів;

$g^{(n/4)}$ – поліном *g* для поля $x^{n/4}+1$, який має *n*/4 коефіцієнтів;

…

$f^{(1)}$ – поліном *f* для поля *x*+1, який має один коефіцієнт;

$g^{(1)}$ – поліном *g* для поля *x*+1, який має один коефіцієнт;

Виконується $log_2 n$ кроків, всі кроки виконуються ідентично.

2. Вирішити діафантове рівняння $f^{(1)}*G'^{(1)} - g^{(1)}*F'^{(1)} = 1$ відносно невідомих $F'^{(1)}$, $G'^{(1)}$; (умова існування рішення в цілих числах – $GCD\ (f^{(1)}, g^{(1)}) = 1$).

3. Обчислити $F^{(1)} = q * F'^{(1)}$; $G^{(1)} = q * G'^{(1)}$; $F^{(1)}$, $G^{(1)}$ – рішення рівняння $f^{(1)}*G^{(1)} - g^{(1)}*F^{(1)} = q$, поліноми $F^{(1)}$, $G^{(1)}$ мають по одному коефіцієнту.

4. Для пари поліномів $F^{(1)}$ $G^{(1)}$, виконати покроковий перехід від поля x^1+1 до полів x^2+1, x^4+1, …, x^n+1. В результаті отримаємо поліноми:

$F^{(2)}$ – поліном, який має 2 коефіцієнта;

$G^{(2)}$ – поліном, який має 2 коефіцієнта;

$F^{(4)}$ – поліном, який має 4 коефіцієнта;

$G^{(4)}$ – поліном, який має 4 коефіцієнта;

…

$F^{(n)}$ – поліном, який має *n* коефіцієнтів;

$G^{(n)}$ – поліном, який має *n* коефіцієнтів;

Якщо усі коефіцієнти $F^{(n)}$, $G^{(n)}$ задовольняють вимогам щодо допустимих розмірів, то приймається рішення $F^{(n)}=F$, $G^{(n)}=G$. Якщо ні, то процес починається з обчислення складових особистого ключа *f, g* повторно.

Виконується $log_2 n$ кроків, всі кроки виконуються ідентично.

3.1.4. Перетворення переходу від поля x^t+1 до поля $x^{t/2}+1$

Вхід: поліном *a* з коефіцієнтами $a_0, a_1, \ldots, a_{t-1}$;

Вихід: поліном a з коефіцієнтами $b_0, b_1, \ldots, b_{t/2-1}$;

Для фіксованого *t* необхідно виконати кроки 1–3.

1. Формування двох поліномів *e*, *o*, перший з коефіцієнтами з парними номерами, другий з непарними вхідного полінома *a*:

$e_j = a_{2j}$ (j =0, 1, $t/2 - 1$);

$o_j = a_{2j+1}$ (j =0, 1, $t/2 - 1$);

2. Обчислення поліномів *e*2, *o*2:

$e2 = e^2 \ mod \ x^{t/2}+1$;

$o2 = o^2 \ mod \ x^{t/2}+1$;

3. Обчислення коефіцієнту поліному b_0:

$b_0 = e2_0 + o2_{t/2-1}$

4 Обчислення решти коефіцієнтів з індексами 1, 2, $t/2–1$

$b_j = e2_j – o2_{j-1}$

При виконанні кроків 2–4 застосовують довгі числа.

Перехід від поля x^t+1 до поля $x^{2t}+1$

Включає:

- обчислення поліномів F для поля $x^{2t}+1$;
- обчислення поліномів G для поля $x^{2t}+1$.

Для обчислення поліному $F'^{(2t)}$ для поля $x^{2t}+1$ застосовують поліном $F^{(t)}$ для поля x^t+1 та поліном $g^{(2t)}$ для поля $x^{2t}+1$, який отримано на етапі переходу від поля $2t$ до t.

Для формування поліному $G'^{(2t)}$ для поля $x^{2t}+1$ застосовують поліном $G^{(t)}$ для поля x^t+1 та поліном $f^{(2t)}$ для поля $x^{2t}+1$, який отримано на етапі переходу від поля $2t$ до t

Для перетворення застосовують однакові операції:

Вхід:

- поліном $A^{(t)}$ з коефіцієнтами $A^{(t)}_0, A^{(t)}_1, \ldots, A^{(t)}_{t-1}$;
- поліном $b^{(2t)}$ з коефіцієнтами $b^{(2t)}_0, b^{(2t)}_1, \ldots, b^{(2t)}_{2t-1}$.

Вихід:

- поліном $C^{(2t)}$ з коефіцієнтами $C^{(t)}_0, C^{(t)}_1, \ldots, C^{(t)}_{2t-1}$.

3.1.5. Прикінцеве отримання складових ключа – поліномів *F, G*

Для отримання коефіцієнтів поліному C необхідно виконати кроки 1–3.

1. Формування поліному u для поля $x^{2t}+1$: $u_{2j}=A^{(t)}_j$; $u_{2j+1}=0$, (j = 0, 1, …t-1);
2. Формування поліному v для поля $x^{2t}+1$: $v_{2j}= b^{(2t)}_{2j}$; $v_{2j+1}= -b^{(2t)}_{2j+1}$, ($j$ = 0, 1, …t-1);
3. Обчислення поліному C для поля $x^{2t}+1$: $C = u * v \ mod \ x^{2t}+1$

Пункти 1 – 3 необхідно виконати для обчислення поліномів $F'^{(2t)}$, $G'^{(2t)}$.

4. Редукція поліномів $F'^{(2t)}$, $G'^{(2t)}$.

Обчислюють значення цілого коефіцієнту k:

$$k = \left\lfloor \left(\mathrm{F}'^{(2t)} f^{*(2t)} + \mathrm{G}'^{(2t)} g^{*(2t)}\right) / \left(f^{(2t)} f^{*(2t)} + g^{(2t)} g^{*(2t)}\right) \right\rfloor.$$

Обчислюють нові значення $F'^{(2t)}$, $G'^{(2t)}$

$$(F'^{(2t)}, G'^{(2t)}) = (F'^{(2t)} - k * f^{(2t)}, G'^{(2t)} - k * g^{(2t)}).$$

Редукція продовжується до тих пір, поки $k \neq 0$.

5. В якості поточних значень $f^{(2t)}$, $g^{(2t)}$ приймаються обчислені значення $F'^{(2t)}$, $G'^{(2t)}$

$$f^{(2t)}=F'^{(2t)}; \ g^{(2t)}=G'^{(2t)};$$

Після обчислення поліномів для поля x^2+1, x^4+1, … x^n+1 отримані значення – поліноми F, G, що разом із особистими (секретними) складовими f та g і є особистим (секретним) ключем. Відмітимо також, що наведений вище метод розв'язку порівняння (1) може бути оптимізований по критерію складності і це потребує окремого розгляду.

3.2. Алгоритм вироблення ЕП

Вироблення ЕП виконується в два етапи: розгортання особистого ключа (однократно) та вироблення електронного підпису на сеансі зв'язку.

Алгоритм вироблення ЕП здійснюється виконанням таких складових етапу:

- розгортання особистого ключа, в процесі якого на його основі формується базис решітки у *FFT* форматі та обчислюється дерево для базису решітки;

- алгоритм обчислення компонентів ЕП, в процесі виконання якого виконується генерація псевдовипадкового поліному r по модулю q (сеансового ключа для ЕП), обчислюються безпосередньо компоненти електронного підпису s_1 та s_2 поліноми та відповідно розподілу Гауса застосовується функція вибірки та відбракування (sampler).

3.2.1. Алгоритм розгортання особистого ключа

Параметри:

n – визначає степінь полінома:

$\sigma 2$ – визначає дисперсію для розподілу Гауса.

Вхід:

- складові особистого ключа – поліноми f, g, F, G.

Вихід:

- базис решітки у вигляді матриці B, побудований згідно з особистим ключем;
- дерево для решітки, яке застосовується при обчисленні компонентів ЕП.

Формування на основі особистого ключа базису решітки.

Базис решітки у вигляді матриці B:

$$B = \begin{bmatrix} g & -f \\ G & -F \end{bmatrix}.$$

Визначник цієї матриці дорівнює $f*G - g*F = q$, де f, g, F, G – є відповідні поліноми.

Для забезпечення швидких обчислень базис може задаватися в *FFT* форматі, тобто у вигляді

$$\hat{B} = \begin{bmatrix} B_{0,0} & B_{0,1} \\ B_{1,0} & B_{1,1} \end{bmatrix} = \begin{bmatrix} FFT(g) & -FFT(f) \\ FFT(G) & -FFT(F) \end{bmatrix}.$$

Формування матриці Грама.

Матриця Грама $\hat{G} = \hat{B} * B^*$, де B^* матриця є результатом транспонування матриці $\hat{B}$, та заміни комплексних даних на комплексно зв'язані дані:

$$\hat{G} = \begin{bmatrix} G_{0,0} & G_{0,1} \\ G_{1,0} & G_{1,1} \end{bmatrix} = \hat{B} * B^* = \begin{bmatrix} B_{0,0} & B_{0,1} \\ B_{1,0} & B_{1,1} \end{bmatrix} * \begin{bmatrix} B_{0,0}{}^* & B_{1,0}{}^* \\ B_{0,1}{}^* & B_{1,1}{}^* \end{bmatrix}.$$

Так як $G_{0,1} = G_{1,0}$, тому в подальшому будуть застосовуватись $G_{0,0}, G_{0,1}, G_{1,1}$

3.2.2. Формування дерева швидких обчислень для базису решітки

Компоненти ЕП залежать від особистого ключа та повідомлення, яке підписується. Усі обчислення, які необхідні для особистого ключа, можна виконати заздалегідь та оформити у вигляді двійкового дерева, яке має $\log_2 n$ рівнів.

Для побудови кожного наступного рівня $logn = log_2 n, log_2 n\text{-}1, \ldots, 2$ виконуються операції:

Матриця G для рівня $logn$ подається у вигляді добутку:

$$G=L*D*L^*,$$

де компоненти матриці G – поліноми порядку 2^{logn}; L – нижня трикутна матриця з одиничними діагональними елементами, при цьому $L_{0,0} = L_{1,1} = 1$; $L_{0,1} = 0$; $L_{1,0}$ належить обчисленню; D – діагональна матриця, тобто $D_{0,1} = D_{1,0} = 0$; елементи діагоналі $D_{0,0}, D_{1,0}$ належать обчисленню.

Показано, що таке подання існує та воно єдине.

Значення $L_{1,0}$ розглядається як вузол дерева наступного рівня.

Значення $D_{0,0}$ та $D_{1,1}$ застосовуються для побудови вузлів дерева кожного наступного рівня ($D_{0,0}$, $D_{1,1}$ – поліноми для поля x^t+1).

$D_{0,0}$ перетворюється в 2 поліноми порядку 2^{logn-1} (позначимо їх *left*1, *right*1) з урахуванням *FFT* представлення кожного поліному.

$D_{1,1}$ перетворюється в 2 поліноми порядку 2^{logn-1}(позначимо їх *left2*, *right*2) з урахуванням *FFT* представлення кожного поліному.

Значення *left*1, *right*1, *left*1 застосовуються в якості елементів матриці G для побудови лівого піддерева, тобто $G_{0,0} = left1, G_{0,1} = right1, G_{1,1} = left1$.

Значення *left*2, *right*2, *left*2 застосовуються в якості елементів матриці G для побудови правого піддерева, тобто $G_{0,0} = left2, G_{0,1} = right2, G_{1,1} = left2$.

Для першого рівня *logn*=1 значення елементу обчислюється за формулою: $\frac{\sqrt{G_{0,0}[0]}}{\sigma 2}$ ($G_{0,0}[0]$ – значення нульового (єдиного) коефіцієнту поліному $G_{0,0}$, σ2 – параметр).

Далі для обчислення ЕП застосовується особистий ключ key з полями *key*.*B*00, *key*.*B*01, *key*.*B*10, *key*.*B*11, *key*.*tree*.

3.2.3. Алгоритм обчислення компонентів електронного підпису

Спочатку обчислюється геш для випадкового (псевдовипадкового) рядка октетів *nonce* та повідомлення *m* для підпису, отриманий рядок перетворюється в поліном *r* з коефіцієнтами по модулю *q*. Далі обчислюються поліноми s_1 та s_2, такі що

$$s_1+s_2*h=r\ (mod\ q\ mod\ \varphi), \tag{11}$$

де *h* – відкритий ключ.

Для обчислення s_1 та s_2 застосовують розгорнутий особистий ключ та поліном *c*. При обчисленні додається випадковий шум, для створення якого застосовують генератор псевдовипадкових даних. Для ініціалізації цього генератору застосовують випадкову послідовність октетів, в подальшому позначену як *seed*.

Значення s_1 може бути обчислено з формули (11) при відомих s_2, *h*, *c*, тому в якості ЕП застосовують значення *nonce* та s_2.

Параметри та вхідні дані.

Вхідними параметрами являються довжини випадкових компонентів та гешу*:*

SEED_OCTETS – довжина *seed*;

NONCE_OCTETS – довжина *nonce*;

HASH_OCTETS – довжина hash.

Вхідними даними для обчислення компонентів ЕП є:

- базис на основі особистого ключа у вигляді матриці *B*;
- дерево *tree* для базису на основі особистого ключа;
- вхідне повідомлення *m* завдовжки *mlen*.

Вихід:

- компоненти підпису (*nonce*, s_2).

В алгоритмі вироблення компонентів ЕП застосовується функція *gen_r* для обчислення псевдовипадкового поліному *r* з коефіцієнтами за модулем *q*, та функція *sign_tree* для безпосереднього обчислення s_1, s_2 (визначені нижче).

Обчислення компонентів електронного підпису.

1. Генерація *seed* завдовжки *SEED_OCTETS* (випадкові або псевдовипадкові).

2. Генерація *nonce* завдовжки *NONCE_OCTETS* (випадкові або псевдовипадкові).

3. Ініціалізація генератору псевдовипадкових даних (*ctx*1) на основі геш-значення *H=Hash*(*nonce*||*m*). Конкретна реалізація залежить від генератору псевдовипадкових послідовностей, що застосовується.

4. Обчислення поліному *r* з застосуванням функції *r* = *gen_r* (*ctx*1).

5. Ініціалізація генератору псевдовипадкових даних (*ctx*2) для створення ЕП з застосуванням *seed*. Конкретна реалізація залежить від генератору псевдовипадкових послідовностей, що застосовується.

6. Обчислення s_1, s_2 (функція *sign_tree*)

s_1, s_2 = sign_tree (*ctx*2, *r*, *key*)

Генерація псевдовипадкового поліному *r* по модулю *q*. Функція *gen_r*.

Параметри:

n – визначає степінь полінома;

q – просте число.

Передобчислена константа:

$c = \lfloor 65536 \,/\, q \rfloor * q$.

Вхід:

ctx – контекст для генератору псевдовипадкових чисел.

Вихід:

r – псевдовипадковий поліном.

Для усіх коефіцієнтів поліному:

1. Генерація псевдовипадкових байтів (2 байта): *low*, *high*.
2. Обчислення цілого числа *temp* = *high* * 256 + *low*.
3. *if temp* < *c then*

поточний коефіцієнт полінома = *temp mod q*

else

перехід на крок 1

end if

Обчислення s_1, s_2. Функція *sign_tree*.

Параметри:

n – визначає степінь поліному;

β – граничне значення квадратичної норми для ЕП.

В функції *sign_tree* для вибірки значень застосовується функція *sampling_fft,* яка визначена нижче.

Вхід:

ctx – контекст генератору псевдовипадкових чисел;

r – псевдовипадковий поліном;

key – особистий ключ після завантаження, який містить матрицю $\hat{B}$ та дерево.

Для прискорення операцій над поліномами застосовують *FFT* формат.

Вихід:

s_1, s_2 – компоненти ЕП.

Алгоритм.

1.1 Формування псевдовипадкових даних завдовжки 64 байта за допомогою генератору з заданий контекстом (*ctx*).

1.2 Ініціалізація генератору сформованими даними (ctx2).

1.3 Обчислення вектору *t* з компонентами *t*0, *t*1, такого, що $t * \hat{B} = r$, тобто

$$\hat{B}^{-1}=\begin{bmatrix} FFT(g) & -FFT(f) \\ FFT(G) & -FFT(F) \end{bmatrix}^{-1} = \frac{1}{q}\begin{bmatrix} -FFT(F) & FFT(f) \\ -FFT(G) & FFT(g) \end{bmatrix};$$

$$\begin{bmatrix} FFT(t0) \\ FFT(t1) \end{bmatrix} = [FFT(r) \quad 0] * \frac{1}{q}\begin{bmatrix} -FFT(F) & FFT(f) \\ -FFT(G) & FFT(g) \end{bmatrix} == \frac{1}{q}\begin{bmatrix} FFT(r) * FFT(-F) \\ FFT(r) * FFT(f) \end{bmatrix};$$

$$FFT(t0) = \frac{1}{q}\, FFT(r) * FFT(-F);\; FFT(t1) = \frac{1}{q}\, FFT(r) * FFT(f).$$

4. Обчислення вектору $\begin{bmatrix} FFT(tx) \\ FFT(ty) \end{bmatrix}$ за допомогою функції *sampling_fft* (додавання випадкового шуму)

$$\begin{bmatrix} FFT(tx) \\ FFT(ty) \end{bmatrix} = sampling\_fft\ (ctx, tree, FFT(\text{t0}), FFT\ (\text{t1})).$$

5. Обчислення вектору $[FFT(t0') \quad FFT(t1')]$ з урахування шума, який внесла функція *sampling_fft*

$$[FFT(t0') \quad FFT(t1')] = \begin{bmatrix} FFT(tx) \\ FFT(ty) \end{bmatrix} * \hat{B}.$$

6. Відновлення вектору [*t*0', *t*1'] (зворотне перетворення з *FFT* формату)

$$t0' = FFT^{-1}(FFT(t0')); \qquad t1' = FFT^{-1}(FFT(t1')).$$

7. Обчислення вектору *s* (s_1, s_2): $s_1 = r - t0'$; $s_2 = 0 - t1'$.

8. Якщо квадратична норма (s_1, s_2) не перевищує β^2 (малі поліноми), закінчити, інакше перейти на крок 4.

Функція вибірки (*sampling_fft*).

Параметри:

n – степінь поліному.

Функція рекурсивна, виконується для поліномів степені *n*, *n*/2, *n*/4, …, 1, тобто загальна кількість кроків $log_2 n+1$.

Спочатку визначаються дії для усіх кроків крім останнього, а потім для останнього кроку.

Вхід:

logn – номер рівня, приймає значення $log_2 n$, $log_2 n - 1, \ldots, 0$.

ctx – контекст генератору псевдовипадкових чисел;

*t*0, *t*1 – поліноми в *FFT* форматі;

tree – гілка дерева, яка визначена поточним рівнем.

Вихід:

*t*x, *t*y – поліноми.

Для усіх рівнів крім останнього виконуються кроки 1–7.

1. Визначається степінь полінома для поточного рівня $t=2^{logn}$.

2. Поліном *t*1 степені *t* перетворюється в два поліноми *t*10 та *t*11 степені *t*/2 з урахуванням *FFT* формату. Значення *t*10, *t*11 застосовуються в якості вхідних даних для наступного рівня функції *sampling_fft*, тобто для поліномів степені *t*/2. Позначимо результат роботи функції *sampling_fft* для *t*10, *t*11 як *ty*10 та *ty*11.

3. Поліноми *ty*10 та *ty*11 порядку *t*/2 об'єднуються в один поліном порядку *t* з урахуванням *FFT* формату. Позначимо отриманий результат *ty*.

4. Коригування *t*0 з урахуванням зміни *t*1 та відповідного листа дерева для приватного ключа: *t*0' = *t*0 + (*t*1 – *t*y) * *tree*.

5. Поліном *t*0' степені *t* перетворюється в два поліноми *t*00 та *t*01 з урахуванням *FFT* формату. Значення *t*00, *t*01 – застосовуються в якості вхідних даних для наступного рівня функції *sampling_fft*, тобто для поліномів степені *t*/2. Позначимо результат роботи функції *sampling_fft* для *t*00, *t*01 як *tx*00 та *tx*01.

6. Поліноми *tx*00 та *tx*01 порядку *t*/2 об'єднуються в один поліном порядку *t* з урахуванням *FFT* формату. Позначимо отриманий результат *tx*.

7. Значення *tx*, *ty* – результат роботи функції для рівня *logn*.

Для останнього кроку (*logn* = 0, *t* = 1, поліноми *t*0, *t*1 та відповідний лист дерева містять по одному елементу) застосовується функція *sampler* (вибірка та відбракування).

1. σ := *tree* Відповідний лист дерева.

2. *tx* := *sampler*(*ctx*, *t*0, σ); Вибірка наступного елементу

3. *ty* := *sampler*(*ctx*, *t*1, σ); Вибірка наступного елементу

Значення *tx*, *ty* – результат роботи функції для рівня logn

Функція вибірки та відбраківки (sampler)

Дозволяє виконати вибірку згідно розподілу Гауса $D_{\mu,\sigma}$ для заданих μ (μ = *t*0 або μ = *t*1) та σ, яке обчислене при формуванні дерева для секретного базису.

Параметри:

σ_{min} – мінімальне значення для відхилення;

σ_{max} – максимальне значення для відхилення.

Вхід:

ctx – контекст генератору псевдовипадкових чисел;

μ – математичне очікування;

σ – середнє квадратичне відхилення.

Вихід:

z – значення, яке задовольняє розподілу Гауса.

1. Для значення μ виділяється ціла частина (*i*μ), яка не перевищує задане значення (функція floor) та дробова *d*μ (μ = *i*μ + *d*μ, *d*μ≥ 0).

2. Для *d*μ генерується випадкове *z*0, яке задовольняє розподілу Гауса для значення σ_{max}.

3. Перевіряється, можливість застосування *z*0 з урахуванням поточного значення σ. Якщо значення *z*0 треба відхилити, алгоритм повертається на крок 2.

4. Повертається значення z = *i*μ + *z*0.

3.3. Алгоритм перевірки електронного підпису

Параметри:

n – визначає степінь полінома;

q – просте число;

NONCE_OCTETS – розмір *nonce* (байтів);

β^2 – константа, яка обмежує значення норми для підпису.

Вхід:

повідомлення *m* завдовжки *mlen*;

nonce завдовжки NONCE_OCTETS;

s_2 – компонент електронного підпису;

h – відкритий ключ.

Вихід:

OK – електронний підпис правильний;

ERROR – електронний підпис не правильний.

Алгоритм перевірки ЕП зводиться до ініціалізації на основі геш-значення *H* генератору псевдовипадкових даних, обчислення поліному *r*, обчислення s_1 та перевірка, що квадратична норма s_1, s_2 не перевищує β^2.

1. Ініціалізація генератору псевдовипадкових даних (*ctx*1) на основі геш значення *H*=*Hash*(*nonce*||*m*). Конкретна реалізація залежить від генератору псевдовипадкових послідовностей, що застосовується.

2. Обчислення поліному *r* з застосуванням функції *r* = *gen_r* (*ctx*1).

3. Обчислення $s_1=(r-s_2*h) \bmod q \bmod \varphi$.

4. Перевірка, що квадратична норма s_1, s_2 не перевищує β^2 $(\sum_{i=0}^{n-1}(s1_i{}^2 + s2_i{}^2) < \beta^2)$. Якщо умова виконується, то повертає *OK*, інакше *ERROR*.

4. Аналіз потенційних атак на ЕП Falcon та «Сокіл»

На основі обґрунтованих та вибраних моделей порушника, загроз та моделі безпеки [14 – 19], основними атаками, стосовно яких повинно бути здійснено захист, є такі:

- атаки на ЕП Falcon та «Сокіл» на основі функції гешування H;
- атаки на відновлення особистого ключа з відкритого ключа ЕП Falcon та «Сокіл»;
- атаки на основі підробки ЕП Falcon та «Сокіл».

Нижче розглядаються та аналізуються вказані атаки на предмет їх складності.

4.1. Атаки на ЕП Falcon та «Сокіл» на основі функції гешування H

Перетворення GPV [34], яке застосовується в схемах ЕП Falcon та «Сокіл», вимагає щоб функція гешування H була захищена від колізій. Це означає, що розмір початкової ентропії (солі) в бітах повинен бути не меншим за 2λ, де λ – рівень безпеки, що вимагається. Але, враховуючи те, що згідно з вимогами NIST [2, 4] кількість запитів на вироблення ЕП (signature

queries) повинно бути не більшим за $q_s = 2^{64}$, а ми приймаємо також таке обмеження, тому реальне значення солі повинне бути не менше ніж

$$\lambda + \log_2(q_s). \tag{12}$$

Для 5 – 7 рівнів безпеки це дає значення, що наведені в табл. 1 [29].

Таблиця 1

Розмір (ентропія) початкового значення *r* невизначеності (солі) в бітах

Безпека	Розмір *r*	Розмір *r* з врахуванням вимог NIST
256	512	320
384	768	448
512	1024	576

Аналіз показав, що основними атаками щодо ЕП Falcon та ЕП «Сокіл» є атаки на відновлення особистого (закритого) ключа з відкритого ключа та атаки на підробку ЕП. Розглянемо ці атаки детальніше.

4.2. Атаки на відновлення особистого ключа з відкритого ключа щодо ЕП «Сокіл»

Атаки на відновлення особистого (секретного) ключа з відкритого ключа можуть зводиться до вирішення проблеми NTRU [34, 35]. У ряді схем, стійкість яких ґрунтуються на проблемі NTRU, поліноми *f, g* мають коефіцієнти з множини значень {0, 1, -1}. Це робить можливим реалізувати різні комбінаторні атаки. Наприклад, для ДСТУ 8961:2019 «Скеля» найефективнішою атакою є гібридна атака, яка знаходить частину вектора комбінаторними шляхами. Для схем ЕП Falcon та «Сокіл» такі атаки неможливі, оскільки поліноми *f, g* змінюються (точніше, семплуються) згідно з нормальним розподілом з заданими параметрами. За даного перетворення простір можливих значень поліномів збільшується настільки, що застосування комбінаторних методів стає неефективним. Залишається прямий шлях відновлення особистого ключа з відкритого засобом редукції базису решітки. При цьому, чим менші значення має норма найменшого вектора (*f, g*), тим більша криптостійкість системи. В криптосистемі Falcon поліноми генеруються над полем

$$\square_q [X] / (\phi(x)), \deg(\phi) = n \tag{13}$$

з математичним очікуванням рівним 0. Перетворення спираються на результати роботи [26], у якій детально досліджувалися можливості застосування алгоритмів семплування нормально розподілених величин. В [26] було показано, що алгоритм семплування Клейна може давати вектори розміру $\approx \sqrt{\frac{qe}{2}}$, що є дуже близьким до теоретичного мінімуму $\sqrt{q}$. Відповідно, щоб отримати такий розмір, кожний коефіцієнт отримується з розподілу з середньоквадратичним відхиленням [29]

$$\sigma' = \sqrt{\frac{qe}{2}} * \frac{1}{\sqrt{2n}}. \tag{14}$$

Найменший вектор може бути знайдений, якщо його проєкція на простір, що натягнутий на перші B векторів $b_1^*, b_2^*, ..., b_B^*$ буде менша за b_{2n-B}^*. Згідно з [26, 29] ця проєкція може бути оцінена як

$$\sqrt{\gamma_B} * \det(\Lambda_{[b_1^*,...,b_B^*]}) \approx \sqrt{\frac{3}{4}} * \sigma' \sqrt{B} = \sqrt{\frac{3}{4}} * \sqrt{\frac{qe}{2}} * \frac{1}{\sqrt{2n}} * \sqrt{B}. \tag{15}$$

Водночас, b_{2n-B}^* може бути оцінений як [29]

$$\left\|b_{2n-B}^{*}\right\| \approx GH(B)^{\frac{2n+1-2(2n-B)}{2(B-1)}} \det(\Lambda)^{\frac{1}{2n}} = GH(B)^{\frac{2B-2n+1}{2B-2}} \sqrt{q} = \left(\frac{B}{2\pi e}\right)^{\frac{2B-2n+1}{2B-2}} \sqrt{q}\,. \qquad (16)$$

Таким чином, маємо умову щоб

$$\left(\frac{B}{2\pi e}\right)^{\frac{2B-2n+1}{2B-2}} \sqrt{q} < \sqrt{\frac{3eB}{8n}} * \sqrt{q}\,. \qquad (17)$$

Далі, завдяки вибору $\sigma' = \sqrt{\frac{qe}{2}} * \frac{1}{\sqrt{2n}}$ з обох сторін рівняння маємо множник $\sqrt{q}$, який можна скоротити. Тому умова захисту від атак на відновлення особистого ключа з відкритого шляхом редукції виглядає наступним чином:

$$\left(\frac{B}{2\pi e}\right)^{\frac{2B-2n+1}{2B-2}} < \sqrt{\frac{3eB}{8n}}\,. \qquad (18)$$

4.3. Атаки на підробку ЕП «Сокіл»

Атаки на безпосередньо підробку ЕП можуть бути найбільш загрозливими. Тому іншим вектором атаки є атака підробки ЕП. При реалізації такої атаки потрібно знайти достатньо короткий вектор *s*. Відповідно, це можливо зробити, редукувавши базис так, щоб виконувалася умова [25, 26]

$$\left\|b_{1}^{*}\right\| < \beta\,. \qquad (19)$$

Причому оцінити $\left\|b_{1}^{*}\right\|$ можливо таким же чином, що і у попередньому випадку, тобто у такій послідовності:

$$\left\|b_{1}^{*}\right\| \approx GH(B)^{\frac{2n+1-2}{2(B-1)}} \det(\Lambda)^{\frac{1}{2n}} = GH(B)^{\frac{2n-1}{2B-2}} \sqrt{q} = \left(\frac{B}{2\pi e}\right)^{\frac{2n-1}{2B-2}} \sqrt{q}\,. \qquad (20)$$

Отримуємо, що умовою захисту від атак на підробку підпису є

$$\left(\frac{B}{2\pi e}\right)^{\frac{2n-1}{2B-2}} \sqrt{q} < \beta\,. \qquad (21)$$

Для практичного прийняття рішення необхідно визначитись щодо того, як обирати параметр β. Розробники ЕП Falcon пропонують використовувати значення $\sigma = 1.55\sqrt{q}$ для полінома $\phi = x^n + 1$ і $\sigma = 1.32 * 2^{1/4} * \sqrt{q}$ для полінома $\phi = x^n - x^{n/2} - 1$. Параметр β для полінома $\phi = x^n + 1$ обчислюється як

$$\beta = 1.2 * \sigma\sqrt{2nq}\,. \qquad (22)$$

Для полінома $x^n - x^{n/2} - 1$ β обчислюється таким чином:

$$\beta^2 = \frac{(1.2 * \sigma * 2n\sqrt{q})^2}{n}\,. \qquad (23)$$

Формули відрізняються тому, що для полінома $x^n - x^{n/2} - 1$ замість L2 норми обчислення виконуються за допомогою embedding norm під час генерації ключів та підпису.

Якщо підставити значення β у рівняння для оцінки захищеності від атак на підробку підпису, то також обидві сторони будуть пропорційні значенню $\sqrt{q}$. Таким чином, середньоквадратичні відхилення при семплуванні поліномів з нормального розподілу підібрані таким чином, щоб від q складність атаки не залежала. Проте на параметр q існує безліч інших обмежень, які впливають на його вибір.

Параметр q обирається згідно наступних міркувань [6, 8]:

- для захисту від алгебраїчних атак q має бути простим числом;
- якщо q буде занадто малим (порядку $q \approx n$), то будуть можливі BKW атаки;
- якщо q буде занадто великим ($q \approx n^{2.83}$), то будуть можливі атаки на підполе;
- якщо використовується поле $x^n + 1$, то для реалізації ефективного множення повинне виконуватися рівняння $q \equiv 1 \bmod 2n$;
- якщо використовується поле $x^n - x^{n/2} - 1$, то для реалізації ефективного множення повинне виконуватися рівняння $q \equiv 1 \bmod 3n$.

П р и м і т к а : Стійкість найкращого алгоритму пошуку найменшого вектору оцінюється як 2^0.292B, де B – розмір блоку при редукції. Якщо при криптоаналізі застосовувати алгоритм Гровера, то нижня оцінка класичної стійкості в 256 біт складає 2^0.265B квантової стійкості (при класичній стійкості в 256 біт). Тому, для ЕП на решітках квантова стійкість при класичній стійкості 256 біт набагато більше, ніж 128 біт.

5. Результати порівняння перспективних механізмів ЕП, що засновані на перетвореннях на алгебраїчних решітках

Оцінка та порівняння міжнародних та національних проєктів постквантових стандартів ЕП.

В табл. 2 наведено характеристики обраних для порівняння алгоритмів (значення швидкості криптоперетворень та генерації ключів наведено в тактах). В порівнянні брали участь проєкти стандартів «Вершина» та «Сокіл», а також алгоритм Dilithium, який за попередніми дослідженнями мав кращі результати серед постквантових алгоритмів підпису, що засновані на перетвореннях на алгебраїчних решітках. Стійкість алгоритмів «Вершини» 128 біт відповідає 3-му рівню стійкості NIST, 256 – 5-му, тому пропорційно для виконання порівняння згідно шкали оцінок попарного порівняння параметрам 384 був наданий 7-й рівень, а 512 – 9-й.

Таблиця 2

Характеристики алгоритмів ЕП, що засновані на перетвореннях на алгебраїчних решітках

Алгоритми	$I_{ст.}$	$l_{в.к.}$	$l_{о.к.}$	$l_{рез.}$	$T_{пр.}$	$T_{зв.}$	$T_{гк.}$
Dilithium_round3_sec2	2	1 312	3 504	2 420	259 172	118 412	124 031
Dilithium_round3_sec3	3	1 952	3 856	3 293	428 587	179 424	256 403
Dilithium_round3_sec5	5	2 592	5 792	4595	538 986	279 936	298 050
Вершина_1_128 («Вершина»)	3	1 472	3 488	2 693	133 340	109 818	90 328
Вершина_1_256 («Вершина»)	5	2 624	5 792	5 345	259 103	233 712	229 669
Вершина_1_384 («Вершина»)	7	4 528	9 088	6762	411 040	398 029	317 324
Вершина_1_512 («Вершина»)	9	5 824	11 008	10708	643 744	620 989	485 471
Вершина_2_128 («Сокіл»)	3	897	4097	666	655 672	139 620	33 696 000
Вершина_2_256 («Сокіл»)	5	1 793	8193	1 280	1 338 825	285 714	107 055 000
Вершина_2_512 («Сокіл»)	9	3 585	5121	2 515	2 600 053	265 416	28 493 603 229

В табл. 3 наведено результати досліджень – відносна перевага алгоритмів ЕП, що отримана методом попарних порівнянь за кожною з характеристик.

На рис. 2 відображено гістограму загальної відносної переваги алгоритмів ЕП з урахуванням вагових коефіцієнтів характеристик.

Як видно, найбільшу перевагу має алгоритм «Вершина» з параметрами стійкості 128 біт, для більш стійких параметрів перевага вже у алгоритм «Сокіл».

В подальшому порівнювалися алгоритми, що показали кращі результати в попередньому етапі – SPHINCS+_s, «Вершина» та «Сокіл» (через те, що для різних рівнів стійкості перевага у різних алгоритмів), а також Rainbow (оптимізована реалізація зі стандартними параметрами).

Таблиця 3

Відносна перевага алгоритмів ЕП, отримана методом попарних порівнянь, за кожною з характеристик

Алгоритми	$I_{ст.}$	$l_{в.к.}$	$l_{о.к.}$	$l_{рез.}$	$T_{пр.}$	$T_{зв.}$	$T_{гк.}$
Dilithium_round3_sec2	0,0198	0,1770	0,1816	0,1131	0,1583	0,1857	0,2090
Dilithium_round3_sec3	0,0299	0,0965	0,1475	0,0606	0,0849	0,0984	0,1082
Dilithium_round3_sec5	0,0697	0,0655	0,0768	0,0507	0,0666	0,0506	0,0915
Вершина_1_128 («Вершина»)	0,0299	0,1395	0,1816	0,0800	0,3006	0,2195	0,2696
Вершина_1_256 («Вершина»)	0,0697	0,0655	0,0768	0,0339	0,1583	0,0716	0,1388
Вершина_1_384 («Вершина»)	0,1453	0,0327	0,0407	0,0261	0,0975	0,0348	0,0797
Вершина_1_512 («Вершина»)	0,2681	0,0233	0,0296	0,0173	0,0479	0,0218	0,0608
Вершина_2_128 («Сокіл»)	0,0299	0,2487	0,1212	0,3211	0,0479	0,1466	0,0192
Вершина_2_256 («Сокіл»)	0,0697	0,1108	0,0467	0,1989	0,0238	0,1130	0,0146
Вершина_2_512 («Сокіл»)	0,2681	0,0406	0,0973	0,0984	0,0143	0,0581	0,0086

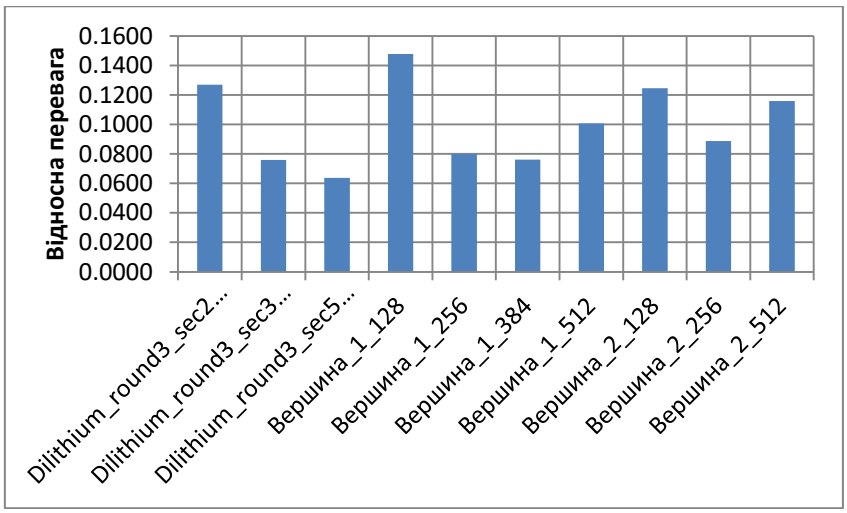


Рис. 2. Переваги алгоритмів ЕП

В табл. 4 наведено результати досліджень – відносна перевага алгоритмів ЕП, що отримана методом попарних порівнянь за кожною з характеристик.

Таблиця 4

Відносна перевага алгоритмів ЕП, отримана методом попарних порівнянь, за кожною з характеристик

Алгоритми	$I_{ст.}$	$l_{в.к.}$	$l_{о.к.}$	$l_{рез.}$	$T_{пр.}$	$T_{зв.}$	$T_{гк.}$
SPHINCS+_128s	0,0155	0,2658	0,2675	0,0189	0,0090	0,0117	0,0164
SPHINCS+_192s	0,0331	0,2289	0,2304	0,0107	0,0090	0,0102	0,0139
SPHINCS+_256s	0,0794	0,1953	0,1984	0,0082	0,0090	0,0079	0,0101
Вершина_1_128 («Вершина»)	0,0331	0,0599	0,0664	0,0385	0,2036	0,1525	0,2908
Вершина_1_256 («Вершина»)	0,0794	0,0416	0,0433	0,0240	0,1340	0,0713	0,2232
Вершина_1_512 («Вершина»)	0,2596	0,0279	0,0274	0,0142	0,0619	0,0305	0,1712
RAINBOW_I_round3_avx	0,0155	0,0117	0,0120	0,2924	0,2864	0,2913	0,0960
RAINBOW_III_round3_avx	0,0331	0,0082	0,0082	0,2043	0,1148	0,1229	0,0500
RAINBOW_VI_round3_avx	0,0794	0,0064	0,0064	0,1746	0,0494	0,0438	0,0263
Вершина_2_128 («Сокіл»)	0,0331	0,0770	0,0578	0,1007	0,0619	0,1095	0,0622
Вершина_2_256 («Сокіл»)	0,0794	0,0495	0,0337	0,0683	0,0363	0,0898	0,0341
Вершина_2_512 («Сокіл»)	0,2596	0,0279	0,0486	0,0451	0,0247	0,0586	0,0057

На рис. 3 відображено гістограму загальної відносної переваги алгоритмів ЕП з урахуванням вагових коефіцієнтів характеристик.

Серед алгоритмів усіх алгоритмів кращий результат у RAINBOW_I_round3_avx (за рахунок малої довжини підпису та великої швидкодії). Але при використанні параметрів, що гарантують більшу стійкість, цей алгоритм вже на останньому місці. Якщо ж брати всі можливі параметри алгоритмів, то на першому місці «Вершина» (який в порівнянні з алгори-

тмами, що засновані на інших математичних апаратах по сукупності оцінок обійшов «Сокіл».

Тобто, якщо необхідний мінімально задовільний рівень захисту, то кращі результати у Rainbow, а в якості універсального алгоритму краще «Вершина». До того ж для «Вершини» не були представлені параметри для рівнів 1-2 NIST. Тобто, якщо б були представлені параметри для даних рівнів, то можливо такі параметри обійшли б і Rainbow.

Кращий результат у алгоритму «Вершина», друге місце у алгоритму Dilithium, а третє у «Сокіл». Але серед параметрів максимальної стійкості 512 біт вже перевага у «Сокіл».

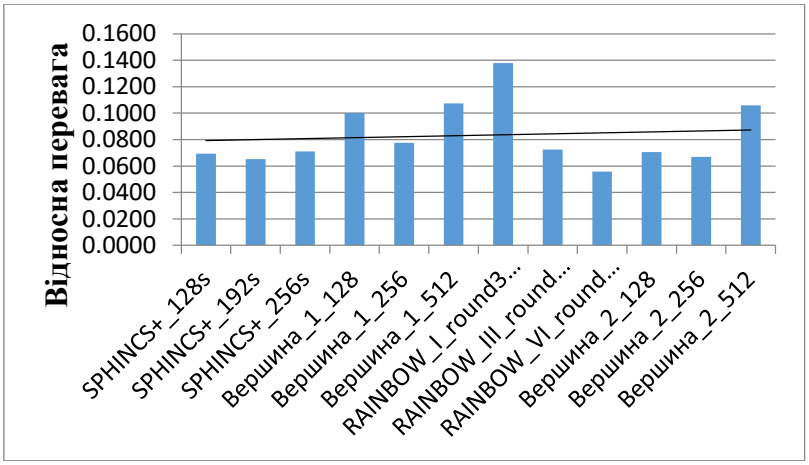


Рис. 3. Переваги алгоритмів ЕП

При порівнянні методом ранжування з'ясувалося, що кращий результат мають алгоритми, які побудовані на основі перетворень в решеті числового поля (рис. 4).

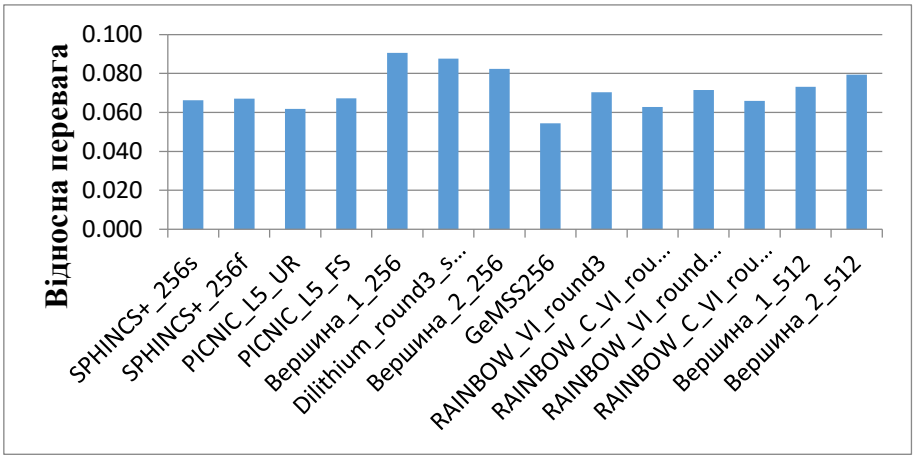


Рис. 4. Переваги алгоритмів ЕП, високого рівня захисту

Висновки

1. Механізми ЕП на решітках є основними претендентами на перемогу в конкурсі NIST PQC. Тому, їх подальший детальний аналіз та порівняння щодо основних характеристик стійкості є першочерговою задачею. Схема Falcon, як фіналіст 2-го етапу, потребує особливої уваги, оскільки має нетипову конструкцію, що використовує арифметику з плаваючою крапкою.

2. На практиці застосовано методику порівняння перспективних постквантових криптоалгоритмів ЕП. Порівнювалися алгоритми, що пройшли до 3-го етапу NIST, а також алгоритми проєктів стандарту «Вершина» та «Сокіл». При порівнянні використовувалися два методи порівняння для отримання більш точної оцінки в залежності від вимог до алгоритмів ЕП.

3. Кращі показники у алгоритмів «Вершина» та «Сокіл» («Сокіл» на даному етапі програє «Вершині» через свою низьку швидкодію, якщо його реалізація буде більш оптимізова-

на, то вже «Сокіл» буде на першому місці), в якості альтернативи можна розглядати алгоритм Rainbow. Крім того «compressed» варіант параметрів Rainbow дозволяє розглядати даний алгоритм в якості повноцінної альтернативи, навіть для систем з обмеженням до розмірів ключів. Але найменші розміри ключів у алгоритму SPHINCS+_s, який досить сильно програє по швидкодії.

4. Криптостійкість ЕП «Сокіл» як ЕП Falcon залежить від двох добре вивчених – NTRU- та SIS-проблем. Завдяки використанню семплування особистих ключів, застосуванням нормального розподілу, гібридні атаки для зламу недоцільні, а NTRU-атаки можуть зводиться до прямої атаки редукцією решітки. Також SIS-проблема, в свою чергу, може вирішуватись за допомогою редукції решітки.

5. Завдяки використанню циклотомічних поліномів розробники проєкту Falcon досягли гарної швидкодії вироблення та перевірки ЕП з використанням бінарних та тернарних дерев. Проте недоліком такого підходу є недостатня гнучкість при генерації загальносистемних параметрів. Криптостійкість здебільшого залежить від параметра n, який має або бути ступенем двійки, або невеликим кратним до ступеня двійки. Можливі значення параметра лежать у невеликій множині, що сильно обмежує вибір параметрів.

6. Криптостійкість ЕП «Сокіл» як і ЕП Falcon сильно залежить від того, наскільки малі вектори можливо семплувати з нормального розподілу. Розробники Falcon детально вивчили відомі алгоритми та обрали алгоритм Клейна, оскільки він у порівнянні з іншими алгоритмами дає найменші вектори. У подальшому дослідження та розробка нових алгоритмів семплування можуть дати можливість зменшити розміри ЕП та підвищити швидкодію. Для підвищення стійкості в ній при криптоперетвореннях використовується вибірка Гауса, що розроблена Престом, Рікоссетом та Россі. Причому, вибірка з відхиленням ретельно налаштована з параметрами таким чином, що спостереження за швидкістю відхилення не дає при усіх параметрах безпеки жодної статистично корисної інформації щодо особистих ключів.

7. Оцінки криптостійкості отримані при зведенні відповідних решіток для розміру блоку B, як 0,265B та 0,292B. Такий підхід вважається класичним і використовувався як авторами ЕП Dilithium, так і авторами ЕП Falcon.

8. Для отримання оцінок щодо складності задач криптоаналізу SIS та NTRU було використано зведення проблеми до редукції решіток. Причому через недостатню гнучкість механізму ЕП «Сокіл», як і для ЕП Falcon, при параметрах 384 біт класичної та 192 біт квантової стійкості. В подальшому такий режим був знятий, і як наслідок поліном $x^n–x^{n/2}–1$ в реалізації ЕП «Сокіл» попередньо не використовується. Але необхідно провести аналіз можливостей реалізації і цього варіанту побудови ЕП.

9. До основного проблемного питання щодо недоліку ЕП Falcon необхідно віднести використання арифметики з плаваючою крапкою. Разом з використанням деревоподібних структур це ускладнює аналіз схеми до атак сторонніми каналами. Іншою проблемою є складність реалізації на малоресурсних пристроях.

10. Обмеження щодо ЕП Falcon на 3-му етапі міжнародного конкурсу NIST США, на наш погляд, пов’язані зі складністю обчислення загальносистемних параметрів, а також із суттєвим впливом їх збільшення на швидкодію ЕП. Тобто, для безпечного використання ЕП Falcon повинні бути знайдені набори загальносистемних параметрів, за яких забезпечується стійкість до всіх відомих та потенційних атак, тобто класичних, квантових, на основі помилок та спеціальних атак.

11. На перспективу доцільним є забезпечення не менше 384 і 512 біт безпеки проти класичного криптоаналізу та не менше 192 і 256 біт безпеки проти квантового криптоаналізу. Але, як показали дослідження, як з точки зору теорії, так і практики, генерація загальносистемних параметрів для використання 384 і 512 біт безпеки проти класичного криптоаналізу та 192 і 256 біт безпеки проти квантового криптоаналізу, є важливою задачею.

Список літератури:

1. Neal Koblitz, Alfred J. Menezes A Riddle Wrapped in an Enigma. [Електронний ресурс]. Режим доступу: https://eprint.iacr.org/2015/1018.pdf.

2. Lily Chen Report on Post-Quatum Cryptography. NISTIR 8105 (DRAFT) / Lili Chen, Stephen Jordan, Yi-Kai-Liu, Dustin Moody, Rene Peralta, Ray Perlner, Daniel Smith-Tone. Режим доступу: http://csrc.nist.gov/publications/drafts/nistir-8105/nistir_8105_draft.pdf.

3. NIST IR 8240 Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process. Режим доступу: https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8240.pdf.

4. NIST IR 8309 Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process. Режим доступу: https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8309.pdf.

5. Квантовые компьютеры. [Електронний ресурс]. Режим доступу: http://www.nkj.ru/archive/articles/5309/.

6. Горбенко Ю. І. Аналіз можливостей квантових комп'ютерів та квантових обчислень для криптоаналізу сучасних криптосистем / Ю. І. Горбенко, Р. С. Ганзя // Східно-європейський журнал передових технологій. 2014. № 1/9 (67). С. 8–15.

7. Горбенко І. Д. Постквантова криптографія та механізми її реалізації / І. Д. Горбенко, О. О. Кузнецов, О. В. Потій, Ю. І. Горбенко, Р. С., Ганзя, В. А. Пономар // Радіотехніка. 2017. Вып. 186. С. 32–52.

8. Каптьол Є. Ю. Аналіз можливостей та особливості програмування задач криптології на квантовому компютері / Є. Ю. Каптьол, І.Д. Горбенко // Радіотехніка. 2020. Вип. 202. С. 37-48.

9. IBM Quantum breaks the 100-qubit processor barrier. IBM Research Blog. [Електронний ресурс]. Режим доступу: https://research.ibm.com/blog/127-qubit-quantum-processor-eagle.

10. IBM's roadmap for scaling quantum technology. IBM Research Blog. [Електронний ресурс]. Режим доступу: https://research.ibm.com/blog/ibm-quantum-roadmap.

11. First quantum computer to pack 100 qubits enters crowded race. [Електронний ресурс]. Режим доступу: https://www.nature.com/articles/d41586-021-03476-5.

12. IBM claims advance in quantum computing. BBC News. Paul Rincon. [Електронний ресурс]. Режим доступу: https://www.bbc.com/news/science-environment-59320073.

13. D-Wave plans to build a gate-model quantum computer. TechCrunch. Frederic Lardinois. [Електронний ресурс]. Режим доступу: https://techcrunch.com/2021/10/05/d-wave-plans-to-build-a-gate-model-quantum-computer/

14. Горбенко Ю. І. Модель порушника систем електронних цифрових підписів в умовах квантового криптоаналізу / Ю. І. Горбенко, О. В. Шевцов, Т. Ю. Кузнецова // Радіотехніка. 2016. Вип. 186. С. 53-69.

15. Горбенко Ю. І. Моделі загроз щодо асиметричних криптоперетворень перспективного електронного підпису / Ю. І. Горбенко, М. В. Єсіна, В. В. Онопрієнко, Г. А. Малєєва // Радіотехніка. 2020. Вип. 202. С. 72-78.

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

17. EUF-CMA and SUF-CMA. [Електронний ресурс]. Режим доступу: https://blog.cryptographyengineering.com/euf-cma-and-suf-cma.

18. Yesina M. Comparative Analysis of Key Encapsulation Mechanisms / Maryna Yesina, Mikolaj Karpinski, Volodymyr Ponomar, Yurij Gorbenko, Tomasz Gancarczyk, Uliana Iatsykovska // Proceedings of the 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS). September 18-21, 2019, Metz, France. Vol. P. 7-12.

19. Єсіна М. В. Моделі безпеки постквантових криптографічних примітивів // Міжнар. наук. симпозіум "Питання оптимізації обчислень (ПОО-XLVI)", 2019 р. Математичне на комп'ютерне моделювання. Сер.: Технічні науки. Вип. 19. С. 49-55.

20. Наказ «Про встановлення вимог з безпеки та захисту інформації до кваліфікованих надавачів електронних довірчих послуг та їхніх відокремлених пунктів реєстрації», №269 від 14.05.2020 р. Режим доступу: https://zakon.rada.gov.ua/laws/show/z0668-20#Text.

21. ДСТУ 4145-2002 «Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння». Режим доступу: https://dbn.co.ua/load/normativy/dstu/4145/5-1-0-1798.

22. ДСТУ ISO/IEC 14888-3:2019 «Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Ч. 3. Механізми, що ґрунтуються на дискретному логарифмі». Режим доступу: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=83556.

23. Dilithium 3. ЕП Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, Peter Schwabe, Gregor Seiler and Damien Stehlé Crystals-Dilithium: Algorithm Specifications and Supporting Documentation. Режим доступу: https://pq-crystals.org/dilithium/data/dilithium-specification.pdf.

24. Олексійчук А. М. Обґрунтування перспективного постквантового національного стандарту електронного підпису на основі решіток / А. М. Олексійчук, В. А. Кулібаба, М. В. Єсіна, С. О. Кандій, Є. В. Острянська, І. Д. Горбенко // Радіотехніка. 2020. Вип. 200 С. 5–14.

25. Ducas L. et al. Crystals-Dilithium: digital signatures from module lattices. Режим доступу: https://cryptojedi.org/papers/dilithium-20170617.pdf.

26. Falcon: Fast-Fourier Lattice-based Compact Signatures over NTRU Specification v1.2 – 01/10/2020. Pierre-Alain Fouque Jeffrey Hoffstein Paul Kirchner. [Електронний ресурс]. Режим доступу: https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions.

27. Горбенко І. Д. Основні положення та результати порівняння властивостей електронних підписів постквантового періоду на алгебраїчних решітках / І. Д. Горбенко, О. Г. Качко, О. В. Потій, А. М. Олексійчук, Ю. І. Горбенко, М. В. Єсіна, І. В. Стельник, В. А. Пономар // Радіотехніка. 2021. Вип. 205 С. 5-21.

28. Rainbow Signature. Режим доступу: https://www.pqcrainbow.org/.

29. Горбенко І. Д. Генерація загальносистемних параметрів для криптосистеми Falcon для 256, 384, 512 біт безпеки / І. Д. Горбенко, С. О. Кандій, М. В. Єсіна, Є. В. Острянська // Радіотехніка. 2020. Вип. 202. С. 57-63.

30. Горбенко І. Д. Методи обчислення системних параметрів для електронного підпису «Crystals-Dilithium» 128, 256, 384 та 512 біт рівнів безпеки / І. Д. Горбенко, А. М. Олексійчук, О. Г. Качко, Ю. І. Горбенко, М. В. Єсіна, С. О. Кандій // Радіотехніка. 2020. Вип. 202 С. 5-27.

31. Горбенко Ю. І. Аналіз стійкості постквантового електронного підпису Dilithium до атак на помилки / Ю. І. Горбенко, О. С. Дроздова // Радіотехніка. 2020. Вип. 202 С. 49-56.

32. Закон України «Про основні засади забезпечення кібербезпеки України» (Відомості Верховної Ради (ВВР), 2017, № 45, ст. 403). Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

33. Горбенко І. Д. Прикладна криптологія : монографія ; вид. 2-ге / І. Д. Горбенко, Ю. І. Горбенко // Харків : Форт, 2012. 868 с.

34. Craig Gentry Trapdoors for hard lattices and new cryptographic constructions / Craig Gentry, Chris Peikert, Vinod Vaikuntanathan // Richard E. Ladner and Cynthia Dwork, editors, 40th ACM STOC, p. 197–206, Victoria, BC, Canada, May 17–20, 2008. ACM Press.

35. Léo Ducas Learning a zonotope and more: Cryptanalysis of NTRUSign countermeasures / Léo Ducas, Phong Q. Nguyen // Wang and Sako, p. 433–450.

Надійшла до редколегії 11.10.2021

Відомості про авторів:

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

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

Потій Олександр Володимирович – д-р техн. наук., професор, заступник Голови Державної служби спеціального зв'язку та захисту інформації; Україна; e-mail: potav@ua.fm; ORCID: https://orcid.org/0000-0002-2366-0541

Горбенко Юрій Іванович – канд. техн. наук, АТ «Інститут інформаційних технологій», перший заступник головного конструктора; Україна; e-mail: gorbenkou@iit.kharkov.ua; ORCID: https://orcid.org/0000-0003-0073-9107

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

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

Стельник Ігор Валерійович – Адміністрація Державної служби спеціального зв'язку та захисту інформації України; директор Департаменту.

Кандій Сергій Олегович – АТ «Інститут інформаційних технологій», технік-конструктор; Україна; e-mail: sergeykandy@gmail.com

Кузнецова Катерина Олександрівна – Харківський національний університет імені В.Н. Каразіна; студентка; Україна; e-mail: kate7smith12@gmail.com

УДК 004.056.5 **DOI:10.30837/rt.2021.4.207.02**

A.A. KOBOZEVA, Sc.D., A.V. SOKOLOV, PhD.

THE THEORETICAL FOUNDATIONS FOR CONSTRUCTING EFFECTIVE CODEWORDS FOR THE CODE-CONTROLLED INFORMATION EMBEDDING STEGANOGRAPHIC METHOD

1. Introduction and statement of the problem

Steganographic subsystem is the important element of modern complex information security systems, the purpose of which is not only to ensure the impossibility of information reading by intruders, but also to hide the very fact of the presence of secret information.

The modern direction of development of cyberspace involves a significant increase in the amount of graphical information in traffic, which leads to an expansion of the scope of steganographic methods application and an increase in their significance in complex information security systems [1]. This circumstance has led to increased attention of modern researchers to steganography and the emergence of a significant number of new steganographic methods operating both in the spatial (temporal) domain and in the domain of various transformations of the original container: DCT [2 – 5], wavelet transforms [6 – 9], singular value decomposition of the corresponding content matrix [10 – 13], Walsh-Hadamard transform [14 – 17].

The use of steganographic methods in modern cyberspace is associated with possible intentional and unintentional attacks against an embedded message, which may include such common effects as: lossy compression, noise, blur, filtering, etc., which can lead to damage of additional information carried by the image considered in this paper as a container. Considering the enormous volumes of transmitted, stored, and processed digital information, a compression attack is the most common today. These circumstances necessitate the development of steganographic methods that would ensure not only the reliability of the perception of the resulting steganographic message, but also resistance to possible attacks against the embedded message.

Modern researchers in the field of steganography agree [18, 19] that considering the computational complexity and features of machine arithmetic, the most rational is the use of the spatial domain of a digital image (DI) for the embedding and extraction of additional information. However, the task of the development of steganographic method corresponding to the necessary requirements for the steganographic message, in particular, ensuring its reliability of perception, insensitivity to disturbing influences, etc., causes significant difficulties in the spatial domain. The existing sufficient conditions for ensuring the above requirements are usually considered in the transform domains of the DI (frequency, singular/spectral value decomposition domain of the corresponding matrix, etc.), which, under such conditions, places the spatial domain in a deliberately “losing” position, in particular, in the development of robust against disturbing influences steganographic methods.

Some modern papers postulate the fact that it is possible to provide resistance to attacks against an embedded message, in particular to lossy compression, exclusively in the DI transform domain, which is clearly not true [20] and is confirmed by the code-controlled information embedding steganographic method recently proposed by the authors in [21]. The mentioned method provides both reliability of perception and perturbation insensitivity of the steganographic message using the spatial domain for steganographic transformation more efficiently than methods that make use of the DI transform domains for steganographic transformation.

As it is known, the efficiency of methods which are based on the code structures directly depends on the properties of the codes used in them. The code-controlled information embedding steganographic method developed in [21] is based on the use of codewords based on the rows of the Walsh-Hadamard matrix (first-order Reed-Muller code) to control the embedding of additional information, the optimality of which has not been researched properly to this point. This circumstance

determines the task of developing a theoretical basis for the construction of effective codewords for their application in the code-controlled information embedding steganographic method.

The *purpose* of this paper is a theoretical substantiation of a method for improving the properties of codewords used in the spatial domain of the container in order to reduce the sensitivity to disturbing influences of the steganographic message generated with their help.

2. The code-controlled information embedding steganographic method

One of the main transforms that is used in processing (in particular, compression) of images and videos is the DCT, defined by the following relation

$$S = C_N X C_N^T, \tag{1}$$

where X is a fragment of the original image of size $N \times N$, C_N is the $N \times N$ DCT matrix, the elements $C(i, j)$, $i, j = 0,1,..., N-1$ of which are calculated in accordance with the following formula

$$C(i, j) = \begin{cases} \dfrac{1}{\sqrt{N}}, & \text{when } i = 0; \\ \sqrt{\dfrac{2}{N}} \cos\left(\dfrac{(2j+1) \cdot i \cdot \pi}{2N} \right), & \text{when } i > 0. \end{cases} \tag{2}$$

Significant attention in the development of modern steganographic methods for DI is given to the two-dimensional Walsh-Hadamard transform [22], which is specified using the following relation

$$W = H'_N X H'^T_N, \tag{3}$$

where X is a matrix of size $N \times N$, $H'_N = \dfrac{1}{\sqrt{N}} H_N$, and the Hadamard matrix H_N of order N is given using the Sylvester construction

$$H_{2^k} = \begin{bmatrix} H_{2^{k-1}} & H_{2^{k-1}} \\ H_{2^{k-1}} & -H_{2^{k-1}} \end{bmatrix}, \; H_1 = 1. \tag{4}$$

In [21], the relationship between the two-dimensional and one-dimensional Walsh-Hadamard transform was established (up to a coefficient $1/N$)

$$\tilde{W} = \tilde{X} H_{N_2}, \tag{5}$$

where the operator $\tilde{A}$ denotes the representation of the matrix A of order $N \times N$ as a row vector of length N^2 by sequential concatenation of the rows of the original matrix A.

The established relationship between the two-dimensional and one-dimensional Walsh-Hadamard transform makes it possible to simplify and make more demonstrative the mathematical transformations used to develop steganographic methods operating directly in the Walsh-Hadamard transform domain or using this domain for their functioning.

The further development of the direction of using the spatial domain of the DI container for the embedding of the additional information, the prospects of which are indicated in [19], is the method for code control of the embedding of additional information, proposed in [21]. The main idea of this method is based on the application of the linearity property of the Walsh-Hadamard transform.

Formally, the steganographic transformation of a container with matrix X, regardless of the domain of embedding of the additional information (spatial, frequency, singular value

decomposition of the matrix, etc.), can be represented as: $M = X + \Delta X$, where M is the matrix of steganographic message, ΔX is the matrix of container perturbation as a result of the steganographic transformation. In other words, steganographic transformation can be represented as an additive embedding of additional information in the spatial domain [18]. Due to this, without limiting the generality of the foregoing, we further consider that the embedding of the additional information is performed as a summation of the initial matrix of the container image X and the matrix corresponding to bits of additional information D , i.e., the following relation takes place

$$M = X + D . \tag{6}$$

In the general case, the matrix D is the result of a preliminary coding of the additional information bits obtained at the output of the precoder in the steganographic system. For the method proposed in [21], D according to a certain rule is assigned to each bit of the additional information.

In the Walsh-Hadamard transform domain, action of (6) is equivalent to summing the transformants of the original container image and the preliminary encoded additional information

$$\tilde{M}H_{N^2} = (\tilde{X} + \tilde{D})H_{N^2} = \tilde{X}H_{N^2} + \tilde{D}H_{N^2} . \tag{7}$$

In other words, by performing the preliminary coding of the additional information in the form of a matrix D , it is possible to perform a targeted impact on one or another transformant of the Walsh-Hadamard transform in order to give to the steganographic message the specified properties determined by the Walsh-Hadamard transformant to which the impact is directed. For example, when information is embedded in such a way that the transformants corresponding to low and medium frequencies are perturbed, it is possible to obtain steganographic messages that are resistant to attacks against the embedded message. The specified is the basis for the code-controlled information embedding method.

The use of code-controlled information embedding in combination with codewords over the alphabet $\{+1,-1\}$ made it possible to obtain a steganographic method [21], which is superior in efficiency to known analogs that are resistant to attacks against an embedded message. However, the number of errors that occur when decoding additional information from a steganographic message subjected to a compression attack with low quality factors $QF < 40$ is more than 5,5 %, which may be unacceptable in some practical applications. In this paper, we propose a further improvement of the method proposed in [21] by researching the characteristics of the codewords used in it.

3. Codewords energy and selectivity

The operation of the code-controlled information embedding method implies the use as a matrix D of size $\mu \times \mu$, which is the result of encoding of the additional information bit, with help of such codewords that would selectively modify those frequency components of the container block that are least affected by attacks against an embedded message (in the case of lossy compression attacks, noisy or blurring, we are talking about components corresponding to low and medium frequencies).

At the same time, the perturbing effect that the attack has on the embedded message, as well as the embedding of the additional information itself, can be represented as an additive perturbation matrix, thus, for the case of the attacked steganographic message, expression (6) takes the form

$$M' = X + D + \varepsilon , \tag{8}$$

where ε is the matrix of the error introduced by the attack, M' is the matrix of the perturbed steganographic message.

It is clear that if the element of the error matrix ε is opposite to the element of the matrix D and will be equal to it or exceed it in amplitude, an error will occur on the decoder side when decoding the specified element of the codeword. Let's denote the probability of such an event as p_e .

To reduce the negative effect from the impact of possible disturbances and increase the resistance of the code-controlled steganographic method, we can increase the energy of the applied codewords, which we define as follows

$$E = \sum_{i=1}^{\mu} \sum_{j=1}^{\mu} t_{i,j}^2 , \tag{9}$$

where $t_{i,j}$ are the elements of the applied codeword.

To construct specific codewords in [21], using a direct correspondence between the Walsh-Hadamard transformants and the DCT transformants, the Walsh-Hadamard transformants were selected corresponding to the low-frequency and mid-frequency components of the DI block

DCT	Size	Walsh-Hadamard transform
$(1,1);\ (1,2);\ (2,1);$ $(3,1);\ (2,2);\ (1,3)...$	4×4	$(1,1);\ (1,3);\ (3,1);\ (4,1);\ (3,3);\ (1,4)...$
	8×8	$(1,1);\ (1,5);\ (5,1);\ (7,1);\ (5,5);\ (1,7)...$
	16×16	$(1,1);\ (1,9);\ (9,1);\ (13,1);\ (9,9);\ (1,13)...$

. (10)

Based on the data (10), it was proposed to use the matrix representation of the rows of the Walsh-Hadamard matrix of order N^2 as codewords. For example, to effect the DCT transformant (1,2) in 4×4-blocks, the matrix representation of the third row of the Walsh-Hadamard matrix of the order $N=16$ is used as a codeword, which, for clarity, we present together with its transformants of the Walsh-Hadamard transform (3), as well as the transformants of the DCT (1)

$$T^{+}_{b,4,(1,2)} = \begin{bmatrix} 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 \end{bmatrix},\ W^{+}_{b,4,(1,2)} = \begin{bmatrix} 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, C^{+}_{b,4,(1,2)} = \begin{bmatrix} 0 & 3.7 & 0 & -1.53 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \tag{11}$$

where the index $b,4,(1,2)$ denotes: *b* is the binary nature of the codeword, 4 is the order of the matrix of the codeword, (1,2) is the transformant of the DCT, on which the given codeword has the greatest impact.

In view of the fact that the codeword $T^{+}_{b,4,(1,2)}$ consists exclusively of elements belonging to the set $\{\pm1\}$, its energy, in accordance with (9), is equal to $E=16$.

An analysis of expression (11) shows that the codeword $T^{+}_{b,4,(1,2)}$ has an exclusive effect on the transformant (1,3) of the Walsh-Hadamard transform $W^{+}_{b,4,(1,2)}$. However, the relationship established in [21] between Walsh-Hadamard transformants and DCT transformants is not one-to-one; the point is that a given Walsh-Hadamard transformant is related to a certain DCT transformant "mainly". This circumstance leads to the fact that in the DCT transformants of the codeword there is an impact not only on the desired transformant (1,2), but also on the transformant (1,4). In other words, while providing a selective effect on the Walsh-Hadamard transformant (1,3), the codeword $T^{+}_{b,4,(1,2)}$ is not selective in terms of the effect on the DCT (1,2) transformant, while a significant part of its energy is spent on changing the DCT transformant (1,4), which is higher frequency, and therefore more susceptible to attacks against the embedded message. From the point of view of steganography, this can be considered as the distribution of the embedded additional information ($T^{+}_{b,4,(1,2)}$ or $T^{-}_{b,4,(1,2)}$ is the result of preliminary coding of additional information), over the frequency components of the DCT (1,2) and (1,4), or otherwise, as a representation of the additional information in

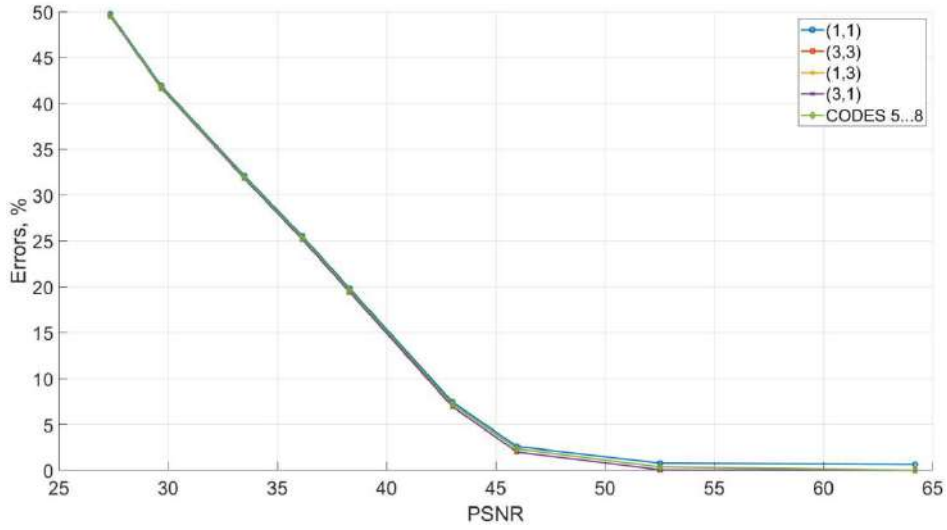
the frequency domain in the form of perturbations of the corresponding frequency coefficients. At a formal level, the additional information decoding will be the more efficient the less these frequency coefficient perturbations change as a result of an attack against an embedded message, in particular, a lossy compression attack. At the same time, that "part of the additional information", the formal representation of which is the perturbation of the DCT coefficient (1,2), is "more protected" from lossy compression attack than the part, the representation of which is the perturbation of the mid-frequency coefficient (1,4). In this regard, an urgent task for the block size 4×4 is to ensure the reduction (minimization) of the perturbation of the DCT coefficient (1,4) as a result of the embedding of an additional information to increase the efficiency of its decoding under conditions of attacks against an embedded message. Similar problems arise for blocks of other sizes.

To quantify the selectivity of the impact of a codeword on the frequency components of a steganographic message, we propose to determine the selectivity coefficient κ as follows

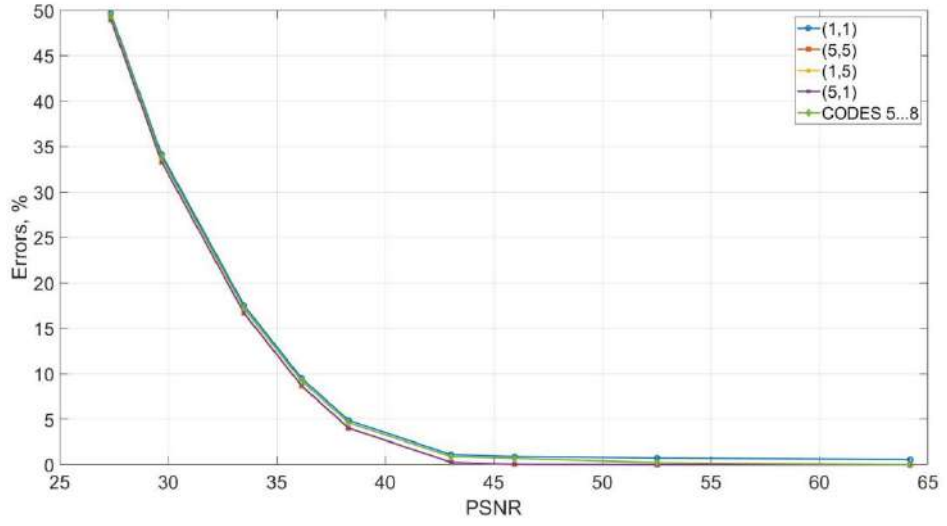
$$\kappa = \frac{\left|c_{n,m}\right|}{\sum_{i=0}^{\mu-1}\sum_{j=0}^{\mu-1}\left|c_{i,j}\right|}. \qquad (10)$$

It directly follows from definition (10) that for a fixed codeword size, with an increase in the selectivity coefficient κ, the expected "effect" from using a particular codeword will increase (in particular, the resistance of the steganographic transformation to attacks against the embedded message for the corresponding codewords will increase) with increasing of $\left|c_{n,m}\right|$ and decrease of $\sum_{i=0}^{\mu-1}\sum_{j=0}^{\mu-1}\left|c_{i,j}\right|$.

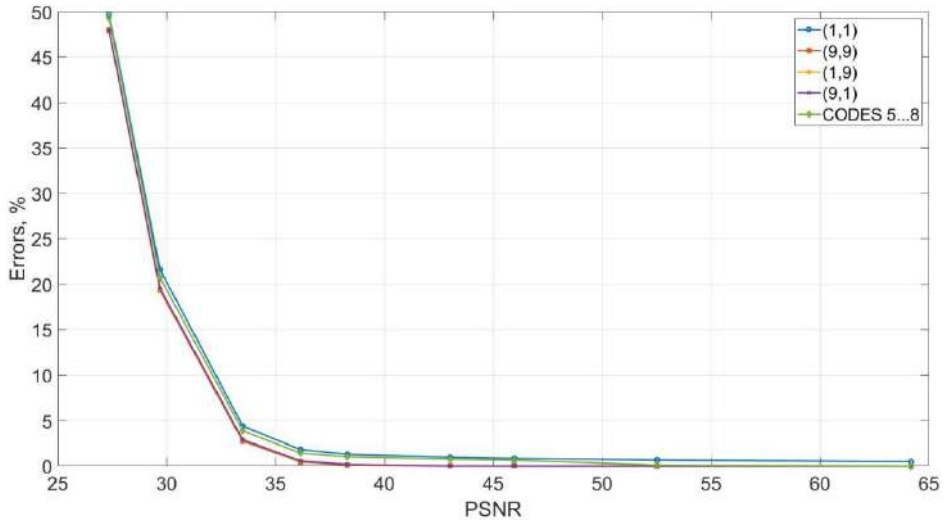
The result of "scattering" the impact of the codeword will increase with the growth of its size. Indeed, as μ increases, the step of changing of the argument of the cosines used in the DCT will decrease. This will cause the increasing in codeword energy, which affects mainly low frequencies (by codeword construction), to be redistributed to more close low frequencies that differ slightly from each other, and this difference decreases with increasing in μ. In this case, the DCT coefficient (n,m) corresponds to different (low) frequencies in blocks of different sizes, as follows from formula (2). Let's call this the "close neighbor" effect. The "close neighbor" effect will lead to a decrease in the value of the selectivity coefficient κ with increasing in μ, determined in accordance with (10) (Table 1), where only the impact on a given frequency coefficient (n,m) is put at the forefront. The increase in total impact on low-frequency "close neighbors" of (n,m) will be strictly shown below. Thus, a decrease in κ with growth in μ in the general case does not reflect a decrease in the resistance of the steganographic transformation to an attack against the embedded message, an illustration of which is Fig. 1, where the resistance of a stenographic message to an attack by Gaussian noise increases with a decrease in κ (increase in μ). Graphs (Fig. 1) were obtained using an experiment to determine the resistance of the code-controlled information embedding steganographic method to a noise attack using 500 images in TIFF format from the NRCS database [23].



a



b



c

Fig.1. Dependence of the number of errors during the extraction of the additional information under the conditions of imposition of Gaussian noise on the steganographic message from the value of the PSNR when using codewords with $\mu \times \mu$-matrices: *a* – $\mu = 4$; *b* – $\mu = 8$; *c* – $\mu = 16$

Table 1

DCT Transformant	Codeword, $\mu = 4$	κ	Codeword, $\mu = 8$	κ	Codeword, $\mu = 16$	κ
(1,1)	$T^{+}_{b,4,(1,1)}$	1	$T^{+}_{b,8,(1,1)}$	1	$T^{+}_{b,16,(1,1)}$	1
(1,2)	$T^{+}_{b,4,(1,2)}$	0.7071	$T^{+}_{b,8,(1,2)}$	0.5603	$T^{+}_{b,16,(1,2)}$	0.4675
(2,1)	$T^{+}_{b,4,(2,1)}$	0.7071	$T^{+}_{b,8,(2,1)}$	0.5603	$T^{+}_{b,16,(2,1)}$	0.4675
(3,1)	$T^{+}_{b,4,(3,1)}$	1	$T^{+}_{b,8,(3,1)}$	0.7071	$T^{+}_{b,16,(3,1)}$	0.5603
(2,2)	$T^{+}_{b,4,(2,2)}$	0.5	$T^{+}_{b,8,(2,2)}$	0.314	$T^{+}_{b,16,(2,2)}$	0.2186
(1,3)	$T^{+}_{b,4,(1,3)}$	1	$T^{+}_{b,8,(1,3)}$	0.7071	$T^{+}_{b,16,(1,3)}$	0.5603

As it can be seen from Table 1, when the codeword size is $\mu = 4$, the codewords $T^{+}_{b,4,(3,1)}$ and $T^{+}_{b,4,(1,3)}$ have the value of the selectivity coefficient equal to $\kappa = 1$ (which means the absolute selectivity). Let us consider in more detail the nature of the existence of absolute selectivity for some codewords. Let codewords $T^{+}_{□,4,(2,1)}$ and $T^{+}_{□,4,(3,1)}$ to be given over a ring of real numbers that have a selectivity coefficient $\kappa = 1$. These codewords can be constructed by solving the following matrix equations

$$CT^{+}_{□,4,(2,1)}C^{T} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ \alpha & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \quad CT^{+}_{□,4,(3,1)}C^{T} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \alpha & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}. \tag{11}$$

Solving these matrix equations using the property of the relationship between two-dimensional and one-dimensional DCT [21], we obtain the following codewords

$$\begin{gathered} T^{+}_{□,4,(2,1)} = \alpha \begin{bmatrix} 0.32665 & 0.32665 & 0.32665 & 0.32665 \\ 0.1353 & 0.1353 & 0.1353 & 0.1353 \\ -0.1353 & -0.1353 & -0.1353 & -0.1353 \\ -0.32665 & -0.32665 & -0.32665 & -0.32665 \end{bmatrix}; \\ T^{+}_{□,4,(3,1)} = \alpha \begin{bmatrix} 0.25 & 0.25 & 0.25 & 0.25 \\ -0.25 & -0.25 & -0.25 & -0.25 \\ -0.25 & -0.25 & -0.25 & -0.25 \\ 0.25 & 0.25 & 0.25 & 0.25 \end{bmatrix}. \end{gathered} \tag{12}$$

In the case of the codeword $T^{+}_{□,4,(3,1)}$, taking the value $\alpha = \sqrt{E}$ (where the energy of the codeword $T^{+}_{b,4,(3,1)}$ is equal to $E = 16$), we get exactly the codeword $T^{+}_{b,4,(3,1)}$, while the specified is not true for the codeword $T^{+}_{□,4,(2,1)}$. In order to map the codeword $T^{+}_{□,4,(2,1)}$ on the binary alphabet $\{\pm 1\}$, we must first take the value $\alpha = \sqrt{E}$, and then round the elements of the resulting matrix to the nearest integer. It is clear that the operation of rounding to the nearest integer will lead to damage of the original structure of the codeword and, accordingly, to the "scattering" of its energy over the other frequency components.

In Table 2 we list the possible codewords for $\mu = \{4,8,16\}$ that have an exclusive effect on one or another DCT transformant, which are characterized by absolute selectivity.

Table 2

Size 4×4	Size 8×8	Size 16×16
$T_{b,4,(1,1)}$, $T_{b,4,(1,3)}$, $T_{b,4,(3,1)}$, $T_{b,4,(3,3)}$	$T_{b,8,(1,1)}$, $T_{b,8,(1,5)}$, $T_{b,8,(5,1)}$, $T_{b,8,(5,5)}$	$T_{b,16,(1,1)}$, $T_{b,16,(1,9)}$, $T_{b,16,(9,1)}$, $T_{b,16,(9,9)}$

Among the DCT coefficients, the DC coefficient is guaranteed not to be affected by the "close neighbor" effect, since it is always determined by the zero frequency, its properties do not depend on the size of the codeword, which is confirmed by Table 1 (for $T^{+}_{b,n,(1,1)}$ the selectivity coefficient has a maximum value and does not change with change in μ). In addition, based on the results of research presented, for example, in [24], it can be argued that the DC coefficients are highly resistant to external influences, which can even exceed the AC coefficients, i.e. are preferred for the organization of steganographic transformation. Taking this into account, we will show that the resistance of the steganographic transformation organized using $T^{+}_{b,\mu,(1,1)}$, will increase with increase in the value of μ.

The matrix $T^{+}_{b,\mu,(1,1)}$ is symmetric, so it is possible to construct a spectral expansion for it in the form of outer products [25]

$$T^{+}_{b,\mu,(1,1)} = \sum_{i=1}^{\mu} \lambda_i u_i u_i^T , \tag{13}$$

where λ_i are real eigenvalues of $T^{+}_{b,\mu,(1,1)}$, and u_i are orthonormal lexicographically positive eigenvectors, $i = \overline{1,\mu}$. Since for $\forall\mu$: $\operatorname{rank}\left(T^{+}_{b,\mu,(1,1)}\right)=1$, relation (13) can be refined

$$T^{+}_{b,\mu,(1,1)} = \lambda_1 u_1 u_1^T , \tag{14}$$

where λ_1 is the only non-zero eigenvalue of $T^{+}_{b,\mu,(1,1)}$. Based on the Frobenius theorem [26], considering the indecomposability and non-negativity of the matrix $T^{+}_{b,\mu,(1,1)}$: $\lambda_1 > 0$. Using the formulas for calculating the energy E of $T^{+}_{b,\mu,(1,1)}$ through the eigenvalues of the matrix, as well as through its elements $T^{+}_{b,\mu,(1,1)}(i,j)$, $i,j=\overline{1,\mu}$, we have [18]

$$E = \sum_{i,j=1}^{\mu} \left(T^{+}_{b,\mu,(1,1)}(i,j)\right)^2 = \mu^2 = \sum_{i=1}^{\mu} \lambda_i^2 = \lambda_1^2 , \tag{15}$$

where

$$\lambda_1 = \mu . \tag{16}$$

Then by direct calculations from (14) we obtain that $u_1 = \left(\frac{1}{\sqrt{\mu}}, \frac{1}{\sqrt{\mu}}, ..., \frac{1}{\sqrt{\mu}}\right)^T$, which is the *n*-optimal vector of the space R^{μ} [18], denoted below as n^O, and the expression (14) itself is transformed to the form

$$T^{+}_{b,\mu,(1,1)} = \mu\left(\frac{1}{\sqrt{\mu}}, \frac{1}{\sqrt{\mu}}, ..., \frac{1}{\sqrt{\mu}}\right)^T \left(\frac{1}{\sqrt{\mu}}, \frac{1}{\sqrt{\mu}}, ..., \frac{1}{\sqrt{\mu}}\right) = \mu n^O \left(n^O\right)^T . \tag{17}$$

For the $\mu\times\mu$-block F of the DI matrix, a normal singular value decomposition is possible, which in the representation of outer products has the form [25]

$$F = \sum_{i=1}^{\mu} \sigma_i u_i v_i^T , \tag{18}$$

where σ_i are singular numbers F, $\sigma_1 \geq \sigma_2 \geq ... \geq \sigma_\mu \geq 0$, u_i, v_i are respectively left and right orthonormal singular vectors, u_i are lexicographically positive, $i = \overline{1, \mu}$. It is shown in [18] that for the original DI: $u_1 \approx v_1 \approx n^O$.

If F is a block of the matrix of the DI-container, then the stenographic transformation using the codeword $T^+_{b,\mu,(1,1)}$ in accordance with (6) will have the form

$$\begin{aligned} F + T^+_{b,\mu,(1,1)} &= \sum_{i=1}^{\mu} \sigma_i u_i v_i^T + \mu n^O \left(n^O\right)^T = \sigma_1 n^O \left(n^O\right)^T + \sum_{i=2}^{\mu} \sigma_i u_i v_i^T + \mu n^O \left(n^O\right)^T = \\ &= \left(\sigma_1 + \mu\right) n^O \left(n^O\right)^T + \sum_{i=2}^{\mu} \sigma_i u_i v_i^T . \end{aligned} \tag{19}$$

Thus, formally, steganographic transformation (6) for $D = T^+_{b,\mu,(1,1)}$ can be represented as a perturbation of the maximum singular value of the container block by a value equal to the size of the block (codeword). It is known [18] that the first singular triple F corresponds in DI mainly to the low-frequency component. If we look at the steganographic transformation (19) in the spatial domain $F + T^+_{b,\mu,(1,1)}$, then here the perturbation of each pixel is the same, equal to ± 1 and does not depend on the block size, but if we analyze the result of the steganographic transformation in accordance with the right side, then the obvious conclusion is that with growth of μ increases the perturbation of the low-frequency component. It is known that for the fundamental possibility of decoding the additional information, the perturbation that the container undergoes during the steganographic transformation must be greater than the perturbation that the steganographic message undergoes as a result of the attack. In this regard, it is obvious that with growth of μ, the ability of a steganographic message to resist a stronger attack increases, while *PSNR* does not change.

All the codewords presented in Table 1 have a unit rank, and even without being symmetric matrices, they can be represented in a form similar to (14), but using a singular value decomposition in the form of outer products

$$T^+_{b,\mu,(k,m)} = \sigma_1 u_1 v_1^T , \tag{20}$$

where $\sigma_1 > 0$ is the only nonzero singular value of $T^+_{b,\mu,(k,m)}$, u_1, v_1 are the left and right singular vector respectively corresponding to σ_1. Thus, any codeword, including $T^+_{b,\mu,(1,1)}$, is determined by the only singular triple corresponding to the maximum singular value, i.e. are focused mainly on low frequencies, which formally demonstrates the achievement of the goal of their construction. With an increase of μ, the first singular triple, taking into account the effect of a “close neighbor”, will correspond to an increasing number of close low frequencies (with the exception of $T^+_{b,\mu,(1,1)}$ considered above), and although the selectivity (10) will decrease, the total contribution of the low-frequency DCT coefficients will increase, considering the properties of the first singular triple. In this case, with increasing of μ, the perturbation and the number of perturbed low-frequency coefficients will increase, considering the “close neighbor” effect (at the same time, for definiteness and uniformity for any μ, we will consider the DCT coefficients belonging to the upper left triangle of the DCT matrix (Fig. 2) to be low-frequency, including the one to which the codeword is initially directed, as a result of steganographic transformation (6), thereby providing an increase in resistance to attacks against the embedded message.

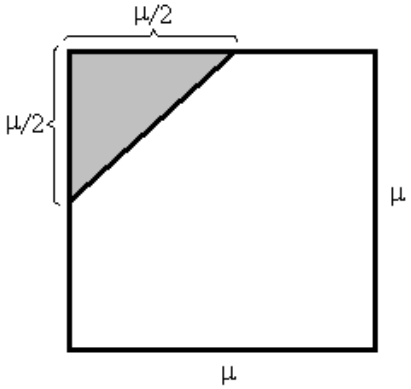


Fig. 2. Matrix of DCT $T^{+}_{b,\mu,(1,1)}$ coefficients with a selected area of coefficients considered as low-frequency

Table 3 illustrates the above, where data are presented on the values of the coefficient η which represents the ratio of the sum of absolute values of low-frequency DCT coefficients to the sum of absolute values of all other DCT coefficients for codewords used in the code-controlled information embedding steganographic method [21].

Table 3

DCT Transformant	Codeword, $\mu = 4$	η	Codeword, $\mu = 8$	η	Codeword, $\mu = 16$	η
(1,2)	$T^{+}_{b,4,(1,2)}$	2.4142	$T^{+}_{b,8,(1,2)}$	3.1165	$T^{+}_{b,16,(1,2)}$	3.8739
(2,1)	$T^{+}_{b,4,(2,1)}$	2.4142	$T^{+}_{b,8,(2,1)}$	3.1165	$T^{+}_{b,16,(2,1)}$	3.8739
(3,1)	$T^{+}_{b,4,(3,1)}$	-	$T^{+}_{b,8,(3,1)}$	2.4142	$T^{+}_{b,16,(3,1)}$	3.1165
(2,2)	$T^{+}_{b,4,(2,2)}$	-	$T^{+}_{b,8,(2,2)}$	0.4576	$T^{+}_{b,16,(2,2)}$	0.9305
(1,3)	$T^{+}_{b,4,(1,3)}$	-	$T^{+}_{b,8,(1,3)}$	2.4142	$T^{+}_{b,16,(1,3)}$	3.1165

Analysis of the data presented in Table 3 confirms that as the size of the codewords μ increases, the concentration of their energy in the low-frequency components increases, which leads to an increase in the resistance of the code-controlled steganographic method to attacks against the embedded message.

This is fully consistent with the coding theory [27], according to which

$$p_{e\,decode} \le 1 - p_{correct} - p_{corrected} = 1 - \sum_{i=1}^{t} C_n^i p_e^t (1 - p_e)^{N-1}, \qquad (21)$$

where $p_{e\,decode}$ is the probability of a decoding error, $p_{correct}$ is the probability of correctly receiving a codeword, $p_{corrected}$ is the probability of successfully correcting an error in a codeword, $t = \frac{d-1}{2}$ is the number of errors that can be guaranteed to be corrected by the code, d is the code distance of the correction code used, and $N = \mu^2$ is the length of the codewords of the code used.

In view of the fact that the code-controlled steganographic method uses a code consisting of a pair of codewords, one of which is the inverse of the other, its code distance is $d = N$, and, therefore, $t = \frac{N-1}{2}$.

On Fig. 3 we show the graphs of the decoding error probability $p_{e\,decode}$ dependence from the length of the codeword N for various values of the error probability p_e in the codeword symbol.

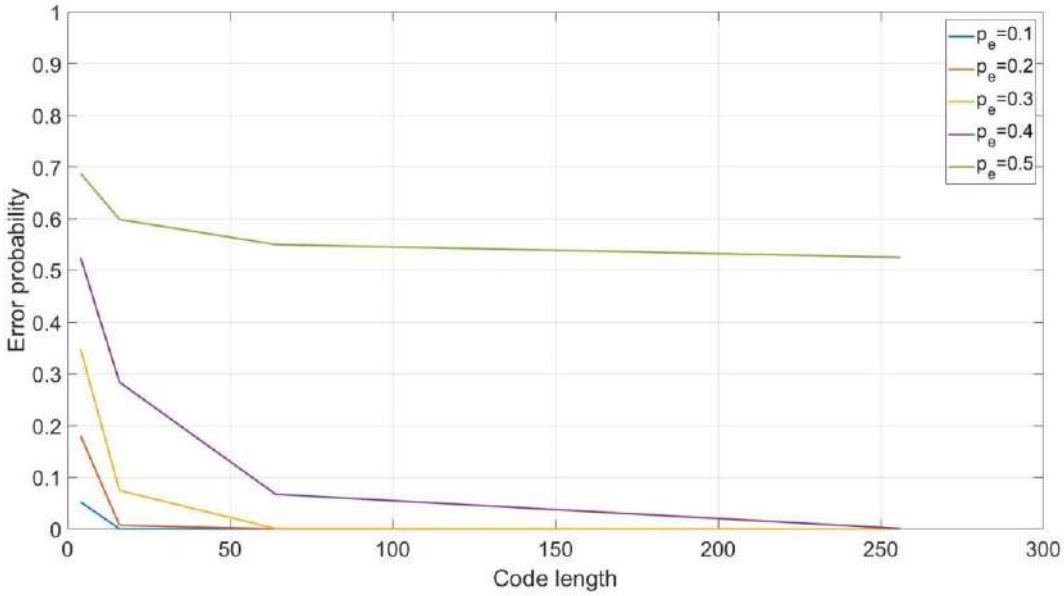


Fig. 3. Graphs of decoding error probability $p_{e\,decode}$ dependence from the codeword length N

Analysis of the data presented in Fig. 3 shows the decrease in the decoding error probability with increasing of codeword length. In this case, for the values of the decoding error probability $p_e \le 0.3$ for the length of the codeword $N = 64$, which corresponds to the value $\mu = 8$, the decoding error probability actually reaches zero.

The obtained results suggest that increasing the length of the codeword is one of the possibilities for increasing the resistance of the stenographic transformation to attacks against the embedded message, although the possibilities here are not unlimited, since an increase in the length of the codeword entails a decrease in the throughput of the generated covert communication channel.

Practical confirmation of the obtained theoretical conclusions are the results of computational experiments, some of which are presented in Fig. 2.

Thus, increasing the resistance of the code-controlled steganographic method to possible attacks by lossy compression, noise, and blurring is directly related to three tasks: increasing the energy of the codeword, which can be achieved by increasing of the absolute values of its elements, increasing the level of selectivity of the codeword, and also increasing of the length of the used codewords.

However, it is obvious here that in the case of an increase in the energy of the codeword, the reliability of the perception of the steganographic message worsens, in the case of an increase in the size of the codewords used, the throughput of the covert communication channel decreases. Increasing the selectivity of the used codewords, in the general case, is the task of optimizing of their structure, which does not lead to a deterioration in the characteristics of the steganographic method.

Conclusions

We note the main results of the research:

1. The definitions of the energy and the selectivity coefficient of the codeword used in the code-controlled steganographic method are introduced and substantiated. The values of the selectivity coefficient of codewords based on the rows of the Walsh-Hadamard matrix used in the code-controlled steganographic method are calculated. The existence of codewords with absolute selectivity is established and substantiated.

2. It has been established that with an increase in the size of the blocks used, there is a tendency to decrease in the selectivity coefficient value due to the presence of the “close neighbor” effect, which, however, occurs due to the use of transformants with similar frequencies that have similar resistance to possible attacks on the embedded message. In this case, the ratio of the sum of abso-

lute values of low-frequency DCT coefficients to the sum of absolute values of all other DCT coefficients grows with the size of the codeword. It has been proven and practically confirmed that an increase in the size of a codeword leads to an increase in the resistance of a code-controlled steganographic transformation.

3. Possible ways of further practical improvement of codewords used in the code-controlled steganographic method are established: increasing of their length, and also increasing of their selectivity. In the general case, the problem of increasing the selectivity of codewords is a problem of optimizing of their structure, the solution of which does not lead to a deterioration in other parameters of the steganographic method, which makes it a priority for further developing the direction of code-controlled embedding of additional information in the spatial domain of the container.

References:

1. Evsutin O., Melman A., Meshcheryakov R. Digital Steganography and Watermarking for Digital Images: A Review of Current Research Directions // IEEE Access, 2020. No. 8. P. 166589-166611. doi: 10.1109/ACCESS.2020.3022779
2. Zhu Z., Zheng N., Qiao T., Xu M. Robust Steganography by Modifying Sign of DCT Coefficients // IEEE Access, 2019. Vol. 7. P. 168613-168628. doi: 10.1109/access.2019.2953504
3. Bansal D., Chhikara R. An improved DCT based steganography technique // International Journal of Computer Applications. Vol. 102, No.14. P. 46-49. doi: 10.5120/17887-8861
4. Bao Z. et al. A robust image steganography based on the concatenated error correction encoder and discrete cosine transform coefficients // Journal of Ambient Intelligence and Humanized Computing. 2020. Vol. 11, No. 5. P. 1889-1901.
5. Rachmawanto E. H. et al.Secure image steganography algorithm based on dct with otp encryption // Journal of Applied Intelligent System, 2017. Vol. 2, No. 1. P. 1-11. doi: 10.33633/jais.v2i1.1330
6. Kadhim I. J., Premaratne P., Vial P. J. High capacity adaptive image steganography with cover region selection using dual-tree complex wavelet transform // Cognitive Systems Research. 2020. Vol. 60. P. 20-32.
7. Valandar M. Y. et al. An integer wavelet transform image steganography method based on 3D sine chaotic map // Multimedia Tools and Applications. 2019. Vol. 78, No. 8. P. 9971-9989.
8. Atta R., Ghanbari M. A high payload steganography mechanism based on wavelet packet transformation and neutrosophic set // Journal of Visual Communication and Image Representation. 2018. Vol. 53. P. 42-54.
9. Emad E. et al. A secure image steganography algorithm based on least significant bit and integer wavelet transform // Journal of Systems Engineering and Electronics. 2018. Vol. 29,No. 3. P. 639-649.
10. Melnik M.A. Compression-resistant steganographic algorithm // Information security. 2012. No. 2(8). P. 99-106.
11. Subhedar M. S., Mankar V. H. Secure image steganography using framelet transform and bidiagonal SVD // Multimedia Tools and Applications. 2020. T. 79. №. 3. P. 1865-1886.
12. Chanu Y. J., Singh Kh. M., Tuithung T. A Robust Steganographic Method based on Singular Value Decomposition // International Journal of Information & Computation Technology, 2014. Vol. 4, No. 7. pp. 717-726.
13. Subhedar M. Image Steganography Using Ridgelet Transform and SVD. Proceedings of the International e-Conference on Intelligent Systems and Signal Processing. Springer, Singapore, 2022. P. 81-91.
14. Bhattacharyya S., Mondal S., Sanyal G. A Robust Image Steganography using Hadamard Transform. International Conference on Information Technology in Signal and Image Processing, Mumbai, 2013. P. 416-426.
15. Sheidaeian H., Zolfaghari B., Zobeiri M. An Efficient and Secure Approach to Multi-User Image Steganography Using CRC-Based CDMA. International Conference on Signal Acquisition and Processing. Singapore, 2011. Vol. 2. pp. 1-5.
16. Amirtharajan R., Rayappan J. B. B. Covered CDMA multi-user writing on spatially divided image. International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace &Electronic Systems Technology (Wireless VITAE), 2011. P. 1-5. doi: wirelessvitae.2011.5940912
17. Sneha P. S., Sankar S., Kumar A. S. A chaotic colour image encryption scheme combining Walsh–Hadamard transform and Arnold–Tent maps // Journal of Ambient Intelligence and Humanized Computing, 2020. Vol. 11, No. 3. P. 1289-1308. doi: 10.1007/s12652-019-01385-0
18. Kobozeva A. A., Horoshko V. A. Information security analysis. Kiev : Izd. GUIKT, 2009. 251 p.
19. Kostyrka O.V. Analysis on the benefits of spatial domain of cover image forsteganography transformation // Informatics and Mathematical Methods in Simulation.2013.No.3. P. 275-282.
20. Gribunin V. G., Okov I. N., Turintsev I. V. Digital steganography. M. : Solon-Press, 2009. 265 p.
21. Kobozeva A.A., Sokolov A.V. Robust Steganographic Method with Code-Controlled Information Embedding // ProblemeleEnergeticiiRegionale. 2021. Vol. 52, No. 4. P. 115-130.
22. Horadam K. J. Hadamard matrices and their applications. Princeton university press, 2012. 280 p.

23. NRCS Photo Gallery // United States Department of Agriculture. URL: https://www.nrcs.usda.gov/wps/portal/nrcs/main/national/newsroom/multimedia/
24. Prokhozhev N. N., Mikhailichenko O. V., and Korobeinikov A. G., Influence of external perturbations on DC coefficients of DCT matrices in grayscale images // Scientific and technical bulletin of information technologies, mechanics and optics. 2008. No. 56. P. 57-62.
25. Demmel J. Computational linear algebra. M. : Mir, 2001. 430 p.
26. Gantmakher F. R. Matrix Theory. M. : Nauka, 1966. 576 p.
27. Mazurkov MI Fundamentals of information transfer theory. Odessa : Science and Technology, 2005. 168p.

Received 05.10.2021

Information about the authors:
Kobozeva Alla Anatolyevna – Doctor of Science, Professor, Odessa Polytechnic National University, Head of the Department of Cybersecurity and Software; e-mail: alla_kobozeva@ukr.net; ORCID: https://orcid.org/0000-0001-7888-0499
Sokolov Artem Viktorovich – PhD, Odessa Polytechnic National University, Associate Professor in the Department of Cybersecurity and Software; e-mail: radiosquid@gmail.com; ORCID: https://orcid.org/0000-0003-0283-7229

УДК 621.391.15 : 519.7 **DOI:10.30837/rt.2021.4.207.03**

А.В. БЕССАЛОВ, д-р техн. наук, О.В. ЦЫГАНКОВА, канд. техн. наук, С.В. АБРАМОВ

ОЦЕНКА ВЫЧИСЛИТЕЛЬНОЙ СЛОЖНОСТИ АЛГОРИТМА CSIDH НА СУПЕРСИНГУЛЯРНЫХ СКРУЧЕННЫХ И КВАДРАТИЧНЫХ КРИВЫХ ЭДВАРДСА

Введение

В статье приведены новые исследования в теме предыдущей работы [1]. Задачи постквантовой криптографии (PQC) сегодня успешно решаются различными алгоритмами, среди которых перспективными, зарекомендовали себя алгоритмы на изогениях суперсингулярных эллиптических кривых [2, 3]. Эффективной альтернативой протоколу SIDH [2] (Supersingular Isogeny Diffi-Hellman) является алгоритм CSIDH [3] (Commutative SIDH) с минимальной из известных длиной ключа. Взамен расширенного поля F_{p^2} в SIDH операции в CSIDH выполняются в простом поле F_p, что для данного p вдвое снижает длину элементов поля и размеры ключей.

Реализации алгоритмов SIDH и CSIDH ранее базировались на быстрой арифметике изогений кривых в форме Монтгомери. В работе [4] предложен новый эффективный метод вычисления изогений нечетных степеней для кривых Эдвардса на основе w-координат Фарашахи – Хоссейни [5]. Эта работа, в свою очередь, базируется на методе Монтгомери дифференциального сложения точек и адаптирует его к кривым Эдвардса. Оптимизация арифметики изогений на кривых Эдвардса в проективных координатах $(W:Z)$ в [4] значительно ускорила алгоритмы их предыдущей работы [6] и позволила авторам получить выигрыш 20 % в скорости выполнения операций по сравнению с реализацией алгоритма на кривых в форме Монтгомери. Формулы вычисления изогений нечетных степеней кривых Эдвардса [7] также содержат компоненты дифференциального сложения точек, что послужило основой метода, предложенного в [4]. Вычисления в классических проективных координатах, как показал наш анализ для изогений малых степеней [8], существенно усложняются с ростом степени изогении и проигрывают по стоимости $(W:Z)$-координатам.

Полные кривые Эдвардса E_d с одним параметром d ($\chi(d)=-1$), определенные в работе [9], имеют хорошо известные преимущества: высокая скорость экспоненцирования точки, универсальность закона сложения точек, аффинные координаты нейтрального элемента группы точек. Введение второго параметра a a кривой $E_{a,d}$ в работе [10] расширило класс кривых в форме Эдвардса и породило, согласно принятой в [11, 12] классификации, два новых класса: скрученные и квадратичные кривые Эдвардса. Они образуют пары квадратичного кручения, которые используются в данной статье для имплементации алгоритма CSIDH.

Вычисление изогений нечетных степеней для полных и квадратичных кривых Эдвардса E_d осуществляется по формулам, определенным теоремами 2 – 4 работы [7]. В предыдущей работе [1] мы обобщили теоремы [7] на кривые в обобщенной форме Эдвардса с двумя параметрами a и d, что позволило в данной статье применить скрученные и квадратичные кривые Эдвардса над полем F_p для имплементации модели CSIDH.

Наш анализ опирается на свойства скрученных и квадратичных кривых Эдвардса, связанных как пары квадратичного кручения [13, 14]. Суперсингулярные кривые этих классов с одинаковым порядком $N_E = p+1 = p+1 = 2^m n, m \geq 3,$ (n – нечетное) существуют лишь при $p \equiv 3 \bmod 4$. Минимальный четный кофактор порядка таких кривых равен 8, тогда для алгоритма CSIDH с нечетным $n = \prod_{i=1}^{K} l_i$. модуль поля F_p следует выбирать как $p = 8n-1$.

С целью адаптации определений для арифметики изогений кривых Эдвардса и кривых в форме Вейерштрасса мы используем модифицированный закон сложения точек [11, 12].

В разд. 1 дан краткий обзор свойств скрученных и квадратичных суперсингулярных кривых Эдвардса (СКЭ) [13 – 15]. В разд. 2 рассматриваются специфичные аспекты имплементации модели алгоритма CSIDH на скрученных и квадратичных СКЭ, приводится модификация алгоритма [3], рассчитаны и табулированы параметры изогенных кривых модели, приведен пример вычислений Алисы и Боба в схеме разделения секрета Диффи – Хеллмана. В разд. 3 дан сравнительный анализ стоимости вычисления параметра d' изогенной кривой E' с использованием $(W:Z)$-координат [4] и классических проективных координат $(X:Y:Z)$[11]. Обсуждается дискуссионный вопрос об отказе от вычисления изогенной функции $\phi(R)$ случайной точки R кривой в алгоритме CSIDH.

1. Свойства скрученных и квадратичных суперсингулярных кривых Эдвардса

Рассмотрим некоторые специфические свойства суперсингулярных кривых Эдвардса (СКЭ) [13, 14]. Эллиптическая кривая *в обобщенной форме Эдвардса* [11] определяется уравнением

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

При квадратичном характере $\chi(ad) = -1$, кривая (1) изоморфна *полной кривой* Эдвардса [9] с одним параметром d:

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

В случае $\chi(ad) = 1, \chi(a) = \chi(d) = 1$ имеет место изоморфизм кривой (1) с *квадратичной кривой Эдвардса* [11]:

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

имеющей, в отличие от (2), параметр d, определенный как квадрат. Для обеих кривых (2) и (3) обычно принимают $a = 1$. В работе [10] кривая (3) и кривая (2) названы *кривыми Эдвардса*. Вместе с тем различие квадратичных характеров этих кривых ведет к кардинально различным их свойствам [11, 12].

Скрученная кривая Эдвардса определена в работе [11] как частный случай кривой (1) при $\chi(ad) = 1, \chi(a) = \chi(d) = -1$.

Мы определяем пару скрученной и квадратичной кривой Эдвардса [11] как пару квадратичного кручения с параметрами $\chi(ad) = 1, a' = ca, d' = cd, \chi(c) = -1$. Так как СКЭ существуют лишь при $p \equiv 3 \bmod 4$[11], то можно принять $c = -1, a' = -a = -1, d' = -d$, где a,d – параметры квадратичной кривой, соответственно a', d' – скрученной кривой. Иначе говоря, переход от квадратичной к скрученной кривой кручения и обратно можно определить как $E_d = E_{1,d} \leftrightarrow E_{-1,-d}$. Соответственно, уравнение скрученной СКЭ при $p \equiv 3 \bmod 4$ из (1) можно записать как

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

Порядок N_E эллиптической кривой над простым полем F_p определяется на основе следа t характеристического уравнения Фробениуса $\varphi^2 + t\phi + p = 0$ как $N_E = p + 1 - t$. Для кривой квадратичного кручения E^t соответствующий порядок будет равным $N_E{}^t = p + 1 + t$. Эллиптическая кривая является суперсингулярной тогда и только тогда, когда над любым расширением простого поля F_p след уравнения Фробениуса $t \equiv 0 \bmod p$, при этом

$\varphi^2 = -p,\ \varphi = \pm\sqrt{-p}$. [14,15]. Иными словами, в алгебраическом замыкании $\overline{F}_p$ суперсингулярная кривая не содержит точек порядка p. Над простым полем F_p такая кривая всегда имеет порядок $N_E = p+1$.

Итак, скрученные и квадратичные СКЭ как пара квадратичного кручения имеют одинаковый порядок $N_E = p+1$, но разную структуру. Кроме двух точек $(0,\pm 1)$, все их точки различны, поэтому изогении одинаковых степеней имеют разные ядра и вычисляются независимо. Обе кривые являются нециклическими в отношении точек четного порядка (содержат по три точки 2-го порядка, две из которых – особые точки $D_{1,2} = \left(\pm\sqrt{\frac{a}{d}}, \infty\right)$ [11]). Квадратичная СКЭ, кроме того, содержит две особые точки 4-го порядка $\pm F_1 = \left(\infty, \pm\frac{1}{\sqrt{d}}\right)$.. Наличие трех точек 2-го порядка ограничивает числом 8 минимальный четный кофактор порядка $N_E = 8n, (n - \textit{нечетное})$ скрученных и квадратичных кривых Эдвардсах [11]. Максимальный порядок точек этих кривых равен $N_E / 2$. Важно, что точки четных порядков в вычислениях алгоритма CSIDH не участвуют.

Для кривой (1) J -инвариант [13, 15]

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

Этот параметр различает изогенные (с разными J -инвариантами) и изоморфные (с равными J -инвариантами) кривые. Так как J -инвариант сохраняет свое значение для всех изоморфных кривых и пар квадратичного кручения, он одинаков для пары скрученных и квадратичных СКЭ ($a = \pm 1$), поэтому в дальнейшем будем пользоваться J -инвариантом $J(d)$. Он является полезным инструментом как при поиске суперсингулярных кривых, так и при построении графов цепочек изогений. Одним из свойств J -инварианта $J(d)$ является

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

Для рассматриваемых классов СКЭ замена $d \to d^{-1}$ дает изоморфизм, а для полных кривых Эдвардса – квадратичное кручение.

2. Модификация алгоритма csiidh на скрученных и квадратичных кривых Эдвардса

Алгоритм PQC CSIDH (Commutative SIDH) предложен авторами [3] для решения той же задачи обмена ключами (SIDH [2]), но на основе изогенных отображений эллиптических кривых в целом как аддитивных абелевых групп. Такое отображение над простым полем F_p определено как класс групповой операции (the class group action) и является коммутативным. В сравнении с известной оригинальной схемой CRS (Couveignes (1997), Rostovtsev, Stolbunov (2004)) на несуперсингулярных кривых использование изогений суперсингулярных кривых позволило кардинально ускорить алгоритм и получить наименьший из известных размер ключа (512 бит в [3]).

Пусть кривая E порядка N_E содержит точки малых нечетных порядков $l_i, i = 1,2,...,K$. Тогда существует изогенная кривая E' того же порядка N_E как отображение степени l_i: $E \to E' = [l_i] * E$. Повторение этой операции e_i раз будем обозначать $[l_i^{e_i}] * E$. Значения экспонент изогений $e_i \in Z$ определяют длину цепочки изогений степени l_i. В работе [3] принят интервал значений экспонент $[-m \le e_i \le m], m = 5, K = 74$, что обеспечивает уровень безопасности 128 бит при атаках квантового компьютера. Отрицательные значения экспоненты e_i означают переход к суперсингулярной кривой квадратичного кручения.

Имплементация алгоритма CSIDH в основном использует быструю арифметику эллиптических кривых Монтгомери $y^2 = x^3 + Cx^2 + x,\ C \neq \pm 2$, содержащих две точки 4-го порядка и, соответственно, имеющие порядок $N_E = 4n(n - \text{нечетное})$ [9]. В работе [4] алгоритм строится на полных СКЭ того же порядка. В настоящей работе мы впервые предлагаем использовать в алгоритме CSIDH скрученные и квадратичные СКЭ, имеющие те же рекордные показатели быстродействия, что и полные кривые Эдвардса [11]. Такая возможность возникает на основе доказанных нами в [1] теорем. При минимальном кофакторе 8 порядок скрученных и квадратичных СКЭ $N_E = 8n$. Таким образом, для этих классов СКЭ с порядком $N_E = 8n = p + 1, \quad n = \prod_{i=1}^{K} l_i.$ модуль поля в алгоритме CSIDH следует выбирать как $p \equiv -1 \bmod 8$.

Не интерактивный обмен ключами по схеме Диффи – Хеллмана включает этапы [3]:

1. **Выбор параметров.** Для малых простых нечетных l_i вычисляется $n = \prod_{i=1}^{K} l_i.$, где значение K определяется уровнем безопасности, и выбирается подходящий модуль поля $p = 2^m \prod_{i=1}^{K} l_i. - 1,\ m \geq 3$ и стартовая эллиптическая кривая E_0.

2. **Вычисление открытых ключей.** Алиса с помощью своего секретного ключа $\Omega_A = (e_1, e_2, .., e_K)$ строит изогенное отображение $\Theta_A = [l_1^{e_1}, l_2^{e_2}, .., l_K^{e_K}]$ и вычисляет изогенную кривую $E_A = \Theta_A * E_0$ как свой открытый ключ. Боб на основе секретного ключа Ω_B и функции Θ_A выполняет те же вычисления и получает свой открытый ключ $E_B = \Theta_B * E_0$. Эти кривые определяются их параметрами с точностью до изоморфизма.

3. **Обмен ключами**. Здесь протокол подобен п.2 с заменой $E_0 \to E_B$ для Алисы и $E_0 \to E_A$ для Боба. Зная открытый ключ Боба, Алиса вычисляет $E_{BA} = \Theta_A * E_B = \Theta_A \Theta_B * E_0$ Аналогичные действия Боба дают результат $E_{AB} = \Theta_B * E_A = \Theta_B \Theta_A * E_0$**,** совпадающий с первым в силу коммутативности групповой операции. В качестве разделенного секрета берется J -инвариант кривой E_{AB} (E_{BA}).

Ниже приводим модификацию алгоритма вычислений Алисы согласно п.2 [3] с использованием изогений скрученных и квадратичных СКЭ.

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

В сравнении с алгоритмом 2 в работе [3] в нашем алгоритме 1, адаптированном к скрученным и квадратичным СКЭ, сделаны модификации:

1. Проверка квадратичности y^2 в п.3 выполняется для уравнения квадратичной кривой Эдвардса (3)

2. При порядке скрученной кривой Эдвардса $N_E = 8n = p+1$ с максимальным порядком точки $N_E/2 = 4n$ для получения точки порядка n достаточно двукратного удвоения случайной точки P. В п.6 это свойство учтено уменьшением одного удвоения в скалярном произведении точки R.

3. Скорректирован п.9 (нельзя сбрасывать индекс i до обнуления e_i в п.10).

4. Обновление числа $k \leftarrow k/l_i$ вместе со сбросом i в п.11 следует делать после обнуления e_i.

Согласно п.10 для каждого l_i вычисляется ровно e_i изогений до обнуления экспоненты e_i. В зависимости от ее знака изогении вычисляются в классе квадратичных ($e_i > 0$) или скрученных СКЭ ($e_i < 0$).

В основе построения изогений нечетных простых степеней для квадратичных кривых Эдвардса лежит теорема 2 [7], а для скрученных кривых Эдвардса – теорема 1 [1]. В последней работе впервые приведены формулы отображений $\phi(P)$ для кривой (1), зависящие от двух параметров a и d. Теорема формулируется ниже.

Теорема 1 [1]. Пусть $G = \{(1,0), \pm Q_1, \pm Q_2, ..., \pm Q_s\}$ – подгруппа нечетного простого порядка $l = 2s+1$ точек $\pm Q_i = (\alpha_i, \pm\beta_i)$, кривой $E_{a,d}$ (1) над полем F_p.

Определим

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

Тогда $\phi(x, y)$ – l-изогения с ядром G из кривой $E_{a,d}$ в кривую $E_{a',d''}$ с параметрами

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

и отображающей функцией

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

или

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

Доказательство теоремы приведено в [1].

Рассмотрим простую модель имплементации алгоритма CSIDH на скрученных и квадратичных СКЭ, образующих пары квадратичного кручения с одинаковым порядком. Такие кривые существуют лишь при $p \equiv -1 \bmod 8$ и имеют порядок $N_E = N_E{}^t = p+1 = cn\ (n - odd),\ c \equiv 0 \bmod 8$. Пусть такая пара кривых содержит ядра 3-го и 5-го порядка при наименьшем значении $n = 15$, тогда минимальное простое $p = 239$ и порядок этих кривых $N_E = 16n = 240$. Параметр d всего семейства 118 квадратичных кривых Эдвардса можно принять как квадраты $d = r^2 \bmod p, r = 2..119$. Из них найдено 30 пар квад-

ратичных и скрученных СКЭ с параметрами $a=\pm 1$ и $\chi(ad)=1$. Квадратичную СКЭ (3) обозначаем E_d, а скрученную СКЭ (4) – как $E_{-1,-d}$. В табл. 1 приведены значения параметра d для пар квадратичных и скрученных СКЭ. Они записаны как квадраты $d=r^2 \bmod p,, r=5..119.$ в порядке нарастания r.

Таблица 1

Значения параметра d квадратичных и скрученных СКЭ $(a=\pm 1)$ при $p=239$ и $N_E=240$

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

Для первой скрученной кривой $E_{-1,-25}=E_{-1,-d}{}^{(0)}$ из табл. 1 можно построить 3- и 5-изогении и найти параметры $d^{(i)}$ цепочки изогенных кривых $E_{-1,-d}{}^{(i)}, i=1,2,...,\pi$, таких что $E_{-1,-d}{}^{(\pi)}=E_{-1,-d}{}^{(0)}$. Параметр a всех изогенных скрученных СКЭ можно зафиксировать как квадратичный невычет $a=-1$ (см. (6)).

Скрученная кривая $E_{-1,-25}$ над полем F_{239} содержит точку 3-го порядка $Q_1=(149,64)$, тогда согласно теореме 3 [7] $A=\prod_{k=1}^{s}\alpha_k=149$, $A^8=8$, $d^{(1)}=A^8(d^{(0)})^3=3$. Вычисленные параметры $d^{(i)}$ цепочки 3-изогенных кривых со стартовым значением $d=d^{(0)}=25$ можно записать как последовательность $d^{(i)}\in\{25,\ 3,\ 10,\ 50,\ 110,25\}$ периода 5. Период цепочки $\pi=5$ делит число всех скрученных СКЭ, равное 30. Задавая другое стартовое значение $d=2$ из табл. 1, можно получить другую последовательность параметров $d^{(i)}\in\{2,61,62,193,5,2\}$. Эти данные используются для скрученных СКЭ при построении функции $[l_1^{e_1}, l_2^{e_2}], l_1=3, e_1<0$.

При положительных значениях экспонент $e_1>0$ результаты аналогичных вычислений для квадратичных СКЭ с другими ядрами $<Q_1>3$-го порядка отличаются от приведенных выше лишь реверсным порядком элементов последовательности $d^{(i)}\in\{25,110,50,10,3,25\}$.

Ядром 5-изогении на скрученной кривой $E_{-1,-25}$ является подгруппа точек 5-го порядка $Q_1=(\alpha_1,\beta_1)=(-95,28)$, $2Q_1=Q_2=(\alpha_2,\beta_2)=(-72,-119)$, $3Q_1=-2Q_1=(\alpha_2,-\beta_2)$, $4Q_1=-Q_1=(\alpha_1,-\beta_1)$, $5Q_1=O=(1,0)$. Она однозначно определяется координатами α_1,α_2 двух точек и уравнением (4). Используя формулу (6) и координаты ядер, можно вычислить элементы последовательности $d^{(i)}\in\{25,\ 2,11,\ 50,193,187,3,61,183,110,5,121,10,62,\ 201,\ 25\}$ параметров цепочки 5-изогенных скрученных СКЭ периода $\pi=15$. Для квадратичных кривых эта последовательность записывается в обратном порядке.

Примем секретные ключи экспонент изогений $\{e_i\}$ Алисы и Боба $\Omega_A=(-1,2),\ \ \Omega_B=(4,-3)$, их функции изогенных отображений соответственно $\Theta_A=[3^{-1},5^2]$, $\Theta_B=[3^4,5^{-3}]$. Вычислим их отрытые ключи $d_A,\ \ d_B$. В качестве стартовой кривой цепочки изогений примем кривую $E^{(0)}=E_{-1,-25}$. Алиса вычисляет параметры 3-х изогенных кривых $E^{(i)}$: одну 3-изогенную скрученную СКЭ и две 5-изогенных квадратичных СКЭ в произвольном порядке. Ее вычисления порождают цепочку изогенных кривых

$E^{(0)} = E_{-1,-25} \to E_{-1,-3} \Rightarrow E_3 \to E_{187} \to E_{193}$. Итак, открытый ключ Алисы $d_A = 193$. Аналогичные вычисления Боба с секретным ключом $\Omega_B = (4,-3)$:

$$E^{(0)} = E_{-1,-25} \Rightarrow E_{25} \to E_{110} \to E_{50} \to E_{10} \to E_3 \Rightarrow E_{-1,-3} \to E_{-1,-61} \to E_{-1,-183} \to E_{-1,-110}$$

дают значение его открытого ключа $d_B = 110$.

Далее, в схеме разделения секретов Алиса, зная открытый ключ Боба, вычисляет изогенную кривую $E_{BA} = [3^{-1}, 5^2] * E_{-1,-110} = E_{-1,-62}$. Тот же результат с помощью функции $E_{AB} = [3^4, 5^{-3}] * E_{-1,-193} = E_{-1,-62}$ получает Боб. Разделенным секретом есть параметр $d_{AB} = 62$.

Отображение (8) точек $P = (x, y)$ кривой $E_A = E_{-1,-25}$ с ядром 3-изогении $G = \{(1,0), \pm Q = (149, \pm 64)\}$ имеет вид

$$\phi_3(x, y) = \left(\frac{x}{149^2} \frac{x^2 + 64^2}{1 + 25 \cdot 64^2 x^2}, \frac{y}{149^2} \frac{x^2 - 149_i^{\,2}}{1 - 25 \cdot 149^2 x^2} \right).$$

Точка максимального нечетного 15-го порядка $P = (-44, -12)$ кривой $E_{-1,-25}$ отображается в точку $P' = (221, 125)$ 5-го порядка кривой $E_{-1,-3}$, точка 5-го порядка $P = (144, 28)$ отображается в точку $P' = (25, 183)$ 5-го порядка, а точка 3-го порядка $P = (149, 64)$ отображается в нейтральный элемент группы – точку $P' = (1, 0) = O$. Как видим, функция $\phi_3(x, y)$ втрое снижает порядки точек прообраза, кратных 3, и не меняет порядки других точек.

Для кривой $E_{-1,-25}$ с ядром 5-го порядка $G = \{(1,0), \pm Q_1 = (-95, \pm 28), \pm Q_2 = (-72, \pm 119)\}$ 5-изогения в форме (8) записывается как

$$\phi_5(x, y) = \left(\frac{x}{155} \frac{x^2 + 28^2}{1 + 25 \cdot 28^2 x^2} \frac{x^2 + 119^2}{1 + 25 \cdot 119^2 x^2}, \frac{y}{155} \frac{x^2 - 95_i^{\,2}}{1 - 25 \cdot 95^2 x^2} \frac{x^2 - 72_i^{\,2}}{1 - 25 \cdot 72^2 x^2} \right).$$

Точка 15-го порядка $P = (-44, -12)$ кривой $E_{-1,-25}$ отображается этой функцией в точку $P' = (-18, 7)$ 3-го порядка кривой $E'_{-1,-2}$, точка 3-го порядка $P = (149, 64)$ отображается в точку $P' = (-18, -7)$ 3-го порядка изогенной кривой, точка 5-го порядка $P = (-95, 28)$ отображается в точку $P' = (1, 0) = O$. Здесь функция $\phi_5(x, y)$ снижает порядки точек прообраза, кратных 5, в пять раз, без изменения порядков других точек.

3. Оценка стоимости вычислений алгоритма csiidh на скрученных и квадратичных кривых Эдвардса в координатах (W:Z) и (X:Y:Z)

Значительный прогресс в эффективности вычисления изогений нечетных степеней СКЭ достигнут в работе [4] на основе использования проективных координат Фарашахи – Хоссейни [5]. Вместе с тем, некоторые оценки стоимости вычислений алгоритма Edwards-CSIDH в [4] не полны и учитывают лишь часть вычислений. В данной статье мы даем более корректный анализ ряда вычислительных затрат в координатах (W:Z) со сравнительной оценкой их в координатах (X:Y:Z).

3.1. Оценка стоимости вычислений изогенной функции

В работе [4] доказана теорема 1, определяющая изогенное отображение нечетной степени $l = 2s + 1$ кривой Эдвардса E_d в кривую $E_d{}'$ в координатах Фарашахи – Хоссейни $w(x, y) = dx^2 y^2$ (или $w(x, y) = x^2 / y^2$). Как и в работе [7], она доказана лишь для кривой Эдвардса E_d ($a = 1$), и неизвестно, применимы ли ее результаты в классе скрученных кривых

Эдвардса $E_{a,d}$ ($\chi(a)=\chi(d)=-1$). Ниже приводим эту теорему для всех кривых в обобщенной форме $E_{a,d}$ (1), которая доказана нами в работе [1]. Вместо взятой за основу формулы (7) в работе [4] мы исходим из более лаконичной формулы (8), полученной нами в теореме 1.

Теорема 2 [1]. Пусть $G=\{(1,0),\pm Q_1,\pm Q_2,...,\pm Q_s\}$ – подгруппа нечетного простого порядка $l=2s+1$ точек $\pm Q_i=(\alpha_i,\pm\beta_i)$, кривой $E_{a,d}$ над полем F_p, и $w_i=d\alpha_i^2\beta_i^2$, $w=dx^2y^2$, $P=(x,y)\in E_{a,d}$. Тогда $w(\phi(x,y))=w(x',y')$ $w(\phi(x,y))=w(x',y')$ есть l-изогения с ядром G из кривой $E_{a,d}$ в кривую $E_{a',d'}$ с параметрами $a'=a^l$, $d'=d^lA^8$, $A=\prod_{i=1}^{s}\alpha_i$, и отображающей функцией

$$w(\phi)=w\prod_{i=1}^{s}\frac{(w-w_i)^2}{(1-ww_i)^2}. \tag{9}$$

Доказательство этой теоремы дано в работе [1].

Подчеркнем, что изогения (9) для w-координаты кривой $E_{a,d}$ (1) не зависит от параметра a и в равной степени справедлива для квадратичных и скрученных кривых Эдвардса, образующих пары квадратичного кручения [11]. Иными словами, функция (9) отображает точки кривой одного из этих двух классов в точки кривой того же класса.

Реализация вычислений изогений (9) для полных кривых Эдвардса дана в работе [4]. Для вычисления параметров $d^{(i)}$ цепочки изогений в проективных координатах вводится дополнительный параметр С в уравнение кривой E_d (2). Для пары квадратичной и скрученной СКЭ (3), (4) при $p\equiv 3 \bmod 4$ мы принимаем $a=\pm 1$, $d=ar^2 \bmod p$, $r\in[2,...,(p-1/2)]$ и определим кривую

$$E_{C,D}:\ \ Cx^2+aCy^2=C+aDx^2y^2,\quad D=dC,\quad \chi(d)=1. \tag{10}$$

При $a=\pm 1$ получаем проективное уравнение соответственно квадратичной (3) и скрученной (4) СКЭ как пары квадратичного кручения..

Переход к проективным координатам $(W:Z)$ позволяет избежать инверсий в формуле (9), при этом для кривой (10) при С=1:

$$W'=W\prod_{i=1}^{s}(WZ_i-W_iZ)^2,$$

$$Z'=Z\prod_{i=1}^{s}(ZZ_i-WW_i)^2.$$

Здесь для каждого s выполняется $4sM+2M+2S$ операций в поле ($M=$ умножение, S – возведение в квадрат). Если ввести промежуточные формулы

$$H=(W+Z)(W_i-Z_i),\qquad J=(W-Z)(W_i+Z_i),$$

$$2W'=W\prod_{i=1}^{s}(H_i-J_i)^2,$$

$$2Z'=Z\prod_{i=1}^{s}(H_i+J_i)^2,$$

то требуется всего $4sM+2S$ операций при вычислении одной изогенной функции (9). Подчеркнем, что в этой оценке, приведенной в [4], не учтены стоимости вычислений параметров $(W_i,Z_i,)$ ядер изогений. Они определены ниже.

3.2. Вычисление точек ядра изогении и параметра d' изогенной кривой в координатах (W:Z)

Для каждой изогенной кривой E' прямое вычисление параметра d' согласно теоремам [7] осуществляется по формуле (6) $d' = d^l (\prod_{i=1}^{s} \alpha_i)^8$.

В работе [4] для расчета d' в *w*-координатах используется формула

$$d' = d^l \prod_{i=1}^{s} \frac{(1+w_i)^8}{4^4}, \quad w_i = d\alpha_i^2\beta_i^2. \tag{11}$$

На первый взгляд, вычисления по формуле (6) проще, так как не требуют для каждого i дополнительно $2M+S$ операций для расчета $w_i = d\alpha_i^2\beta_i^2$ в (11). Однако в первом случае вычисления выполняются на основе рекуррентного удвоения точек ядра в классических проективных координатах $(X:Y:Z)$, а во втором – в координатах $(W:Z)$, что потребовало сравнительного анализа стоимости вычислений при двух подходах.

В проективных *w*-координатах $(D':C')$ имеем

$$D' = D^l \prod_{i=1}^{s} (Z_i + W_i)^8 \tag{12}$$

$$C' = C^l \prod_{i=1}^{s} (2Z_{i\,i})^8, \quad d' = D'/C' \tag{13}$$

Авторы [4] оценивают стоимость вычислений (12), (13) как $2M(s-1)+6S$. В эту оптимистичную оценку не входят стоимости вычислений d^l, W_i, Z_i. В соответствии с п.8 алгоритма 1 известной после SM случайной точки R является лишь одна точка ядра $Q_1 = (\alpha_1, \beta_1)$, с помощью которой рекуррентно вычисляются точки $Q_i = (\alpha_i, \beta_i), i = 2,3,...,s,$ и координаты $w_i = d\alpha_i^2\beta_i^2$. Оценим эти затраты.

Для расчета координат $(W_i, Z_i,)$ ядер простых нечетных порядков l_i достаточно $(s-1)$ раз удвоить точку $Q_1 = (\alpha_1, \beta_1)$ с координатами $(W_1, 1)$. Используя уравнение кривой (1), закон удвоения запишем как [10, 11]

$$2(\mathrm{x}_1, \mathrm{y}_1) = \left(\frac{x_1^2 - ay_1^2}{1 - dx_1^2y_1^2}, \frac{2x_1y_1}{1 + dx_1^2y_1^2} \right) = \left(\frac{x_1^2 - ay_1^2}{1 - w_1}, \frac{2x_1y_1}{1 + w_1} \right) = (\mathrm{x}_2, \mathrm{y}_2).$$

Отсюда

$$w_2 = d\left(\frac{x_1^2 - ay_1^2}{1 - w_1} \cdot \frac{2x_1y_1}{1 + w_1} \right)^2 = 4w_1 \left(\frac{(x_1^2 - ay_1^2)}{(1 - w_1^{\,2})} \right)^2$$

В последней формуле сомножитель в числителе преобразуется к виду

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

В итоге

$$w_2 = \frac{4w_1(d(1 + w_1)^2 - 4aw_1)}{d(1 - w_1^2)^2} .$$

В проективных координатах $(W_i, Z_i,)$ можно записать

$$W_2 = 4W_1(d(Z_1 + W_1)^2 - 4aW_1),$$

$$Z_2 = d(Z_1 + W_1)^2(Z_1 - W_1)^2.$$

Рекуррентное удвоение с учетом $d = D/C$ дает

$$W_{i+1} = 4W_i(d(Z_i + W_i)^2 - 4aW_i), \quad i = 1,2,...,s-1, \tag{14}$$

$$Z_{i+1} = d(Z_i + W_{i1})^2(Z_i - W_i)^2. \tag{15}$$

Стоимость вычислений (14), (15) с учетом стоимости расчета W_1 составляет $(4M + 2S)(s-1) + 2M + S$. В итоге вместе с вычислениями (12), (13) суммарную стоимость вычислений можно оценить равной $(6M + 2S)(s-1) + 2M + 7S$.

3.3. Вычисление точек ядра изогении и параметра d' изогенной кривой в проективных координатах (X:Y:Z)

Используя уравнение кривой (1), закон удвоения запишем в форме, не зависящей от параметра d [11]:

$$2(\mathrm{x}_1, \mathrm{y}_1) = \left(\frac{x_1^2 - ay_1^2}{2 - x_1^2 - ay_1^2}, \frac{2x_1y_1}{x_1^2 + ay_1^2} \right)$$

Подсчет числа возведений в квадрат и умножений в поле и с учетом $a = \pm 1$ дает суммарную стоимость удвоения точки в координатах (X:Y:Z) $4M + 3S$ [10, 11].

Рекуррентное удвоение точки ядра $Q_i = (\alpha_i, \beta_i),$, после замены обозначений $\alpha_i \to \mathrm{x}_i$, $\beta_i \to \mathrm{y}_i$, определяется формулами:

$$X_{i+1} = (X_i^2 - aY_i^2)(X_i^2 + aY_i^2), \; i = 1,2,...,s-1, \tag{16}$$

$$Y_{i+1} = 2X_iY_i(2Z_i^2 - X_i^2 - aY_i^2), \tag{17}$$

$$Z_{i+1} = (2Z_i^2 - X_i^2 - aY_i^2)(X_i^2 + aY_i^2), \tag{18}$$

Заметим, что для каждого X_i и Z_i возведение в квадрат осуществляется в следующей итерации, что позволяет соответствующие произведения квадратов возводить в 4-ю степень вместо 8-й. Стоимость вычислений (16) – (18) составляет $(4M + 3S)(s-1)$.

Взамен формул (12), (13) расчета параметра d' в проективных координатах получаем:

$$D' = D^l \left(\prod_{i=1}^{s} X_i^2 \right)^4, \tag{19}$$

$$C' = C^l \left(\prod_{i=1}^{s} Z_i^2 \right)^4, \tag{20}$$

Стоимость вычислений (19), (20) составляет $2M(s-1) + 4S$. Вместе с удвоением точек ядра (16) – (18) суммарная стоимость равна $(6M + 3S)(s-1) + 4S$.

Можно заключить, что вычисления параметра d' в w-координатах (стоимость равна ($(6M + 2S)(s-1) + 2M + 7S$)) более эффективны в сравнении с координатами (X:Y:Z) с экономией sS для больших s числа полевых операций возведений в квадрат. Ясно, что это связано с более эффективным удвоением точек ялра в w-координатах. Вблизи верхней границы степеней изогений $l_{\max} = 587, s = 293$ [3] этот выигрыш близок к 300S.

Дискуссионным является вопрос о необходимости вычисления изогенной функции $R' = \phi(R)R$ в п.10 алгоритма 1. Для изогении $\phi(R)$ степени l_i точка $R' \in E'$ имеет порядок, не содержащий сомножителя l_i, и, таким образом, бесполезна для нахождения следующего ядра в цепочке изогений данной степени. Для этой цели следует вновь найти случайную точку R'

кривой E′, содержащей точку точку порядка l_i. Это осуществляется с помощью скалярного умножения (SM) во внешнем цикле алгоритма 1.

Конечной целью алгоритма разделения секретов CSIDH является нахождение общего параметра d_{AB} кривой E_{AB}. Для каждого шага в цепочке изогений $E \to E'$ необходим лишь расчет параметра $d' = \psi(d, Q)$ на основе параметров d и ядра $< Q >$ домена E. Этот расчет вовлекает два SM случайных точек R и $(s-1)$ рекуррентных удвоений точек $< Q >$. Таким образом, построение и вычисление достаточно сложной функции $\phi(R)$ не является необходимым для реализации алгоритма CSIDH. Она используется лишь в конце цепочки изогений при $R = Q, \phi(Q) = (1,0)$, однако это известное свойство не требует проверки. Часть вычислений в алгоритме, связанных с расчетом функции $\phi(R)$, можно сэкономить.

Результаты имплементации модели Эдвардс-CSIDH [4] в проективных координатах $(W : Z)$ утверждают, что он не быстрее модели Монтгомери-CSIDH в координатах $(X : Z)$ на 20 %. Заметим, что эта модель построена на полных кривых Эдвардса с порядком. $N_E = p + 1 = 4n$ (n – нечетное). На основе теорем 1 и 2 [1], в данной работе мы показали, как реализовать такую модель на скрученных и квадратичных СКЭ, образующих пары квадратичного кручения. Преимуществом этих классов кривых перед полными кривыми Эдвардса является отсутствие трудоемкой инверсии параметра $d \to d^{-1}$, необходимой при переходе к полной кривой квадратичного кручения. Это лишь ускоряет выполнение алгоритма. Однако при одинаковом максимальном порядке точки $4n$ порядок этих кривых $N_E = 8n$ вдвое больше в сравнении с полными, что вряд ли существенно.

Можно заключить, что метод вычисления изогений нечетных степеней в координатах $(W : Z)$, предложенный в [4], с использованием полных и скрученных СКЭ, позволяет реализовать наиболее быстрые на сегодня вычисления при построении PQC протокола CSIDH и подобных. Доказанные в работе [1] теоремы открывают для их имплементации классы скрученных и квадратичных кривых Эдвардса.

В статье впервые приведены пример такой имплементация для простой модели алгоритма CSIDH и оценки стоимости вычислений параметров изогенных кривых. Наибольшие вычислительные затраты в алгоритме CSIDH связаны со скалярным умножением SM случайных точек, которые требуют скорее экспериментальной оценки. Много научных работ сегодня посвящены теме Constant time CSIDH [16, 17 и др.] и предлагают различные алгоритмы защиты от атак побочного канала. Нами планируются дальнейшие исследования в этой теме.

Список литературы:

1. 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).
2. Jao and L. de Feo. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies // Post-Quantum Cryptography, pp. 19-34 (2011).
3. Castryck W., Lange T., Martindale C., Panny L., Renes J. CSIDH: An efficient post-quantum commutative group action // Peyrin, T., Galbraith, S. (eds.) Advances in Cryptology {ASIACRYPT 2018. pp. 395{427. Springer International Publishing, Cham (2018).
4. Suhri Kim, Kisoon Yoon, Young-Ho Park, and Seokhie Hong. Optimized Method for Computing Odd-Degree Isogenies on Edwards Curves. Security and Communication Networks, 2019.
5. 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).
6. Suhri Kim, Kisoon Yoon, Jihoon Kwon, Seokhie Hong , and Young-Ho Park Efficient Isogeny Computations on Twisted Edwards Curves Hindawi Security and Communication NetworksVolume.
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. 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.

9. 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.

10. Bernstein Daniel J., Birkner Peter , Joye Marc , Lange Tanja, Peters Christiane. Twisted Edwards Curves // IST Programme under Contract IST–2002–507932 ECRYPT,and in part by the National Science Foundation under grant ITR–0716498, 2008. P. 1-1.

11. Бессалов А.В. Эллиптические кривые в форме Эдвардса и криптография : монография. Киев : Политехника, 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. Vol. 53, Is. 1 (2017). P. 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 Analysist. 2019. 55(3). P. 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 Analysist. 2019. 55(5). P. 731–741.

15. Washington L.C. Elliptic Curvres. Number Theory and Cryptography. Second Edition. CRC Press, 2008.

16. H. Onuki, Y. Aikawa, T. Yamazaki, T. Takagi. A Faster Constant-time Algorithm of CSIDH keeping Two Points. ASIACRYPT, 2020.

17. 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 apper at COSADE 2019).

Поступила в редколлегию 01.11.2021

Сведения об авторах:

Бессалов Анатолий Владимирович – д-р техн. наук, профессор, Киевский университет имени Бориса Гринченко, профессор кафедры информационной и кибернетической безопасности, факультет информационных технологий и управления, Украина; email: bessalov@ukr.net; ORCID: https://orcid.org/0000-0002-6967-5001

Цыганкова Оксана Валентиновна – канд. техн. наук, Національний Технічний Університет України «Київський Політехнічний Інститут», Фізико-технічний Інститут, старший преподаватель кафедры математических методов защиты информации, Украина; email: oksana.valent@gmail.com

Абрамов Сергей Вадимович – Киевский университет имени Бориса Гринченко, аспирант кафедры информационной и кибернетической безопасности, факультет информационных технологий и управления, Украина; ORCID: https://orcid.org/0000-0002-5145-2782

УДК 004.043 **DOI:10.30837/rt.2021.4.207.04**

В.В. ДУБІНА, Р.В. ОЛІЙНИКОВ, д-р техн. наук

МЕТОДИ ТА ЗАСОБИ ДЕАНОНІМІЗАЦІЇ ТРАНЗАКЦІЙ В БЛОКЧЕЙН

Вступ

Забезпечення належної безпеки в комп'ютерних мережах – це основна умова захисту даних від різного виду загроз. Велика кількість факторів може мати негативний вплив на ефективне функціонування мережі. Загрози можуть з'явитися під час помилок та різних збоїв у роботі системи або внаслідок навмисних дій зловмисника, що може призвести до розголошення або втрати конфіденційних даних. Через це сучасні мережі все більш потребують належного захисту. Суттєві переваги перед стандартними підходами зберігання даних мають технології розподіленого реєстру, які сьогодні набувають широкого розповсюдження, і можуть бути ефективно використані для боротьби зі зростаючою кількістю загроз.

До такого типу мереж відноситься і технологія блокчейн. Усі її учасники знаходяться в рівному становищі і одночасно володіють всією доступною інформацією. Кожен зберігає у себе точний список операцій, які були здійснені за весь час, і будь-які зміни, внесені до реєстру, одразу будуть виявлені користувачем [1, 2]. Через це блокчейн складно атакувати, адже для того, щоб досягти успіху, зловмиснику необхідно атакувати усі копії.

Системи на основі подібних мереж набувають активного розвитку і поширення. Розробники, передбачаючи масштаби нових досягнень, почали активно створювати цифрові валюти з різними властивостями та можливостями, платформи смарт-контрактів, цифрові платформи для голосування, стійкі до шахрайства тощо [3]. Таким чином, поєднуючи усі можливості, блокчейн мережі знаходять застосування в областях, що стосуються фінансових операцій, ідентифікації користувачів або створення нових технологій кібербезпеки.

Однак водночас велика кількість можливостей блокчейн-систем часто привертає увагу зловмисників. В більшості випадків зловмисники намагаються маніпулювати процесом досягнення консенсусу, щоб змінити інформацію, що вноситься до реєстру. Тому все більше мережі, які генерують і обслуговують цифрові активи, піддаються різноманітним атакам [4], а питання відстеження підозрілої активності і своєчасного захисту користувачів мережі залишається актуальним.

Дану роботу присвячено виявленню основних властивостей технології блокчейн, дослідженню принципів обробки даних і визначенню можливих шляхів деанонімізації транзакцій, як засіб для попередження зловживання криптовалютою у мережі.

В роботі проведено аналіз сучасних блокчейн-систем, визначено актуальні проблеми технології, досліджено принципи формування і обробки транзакцій, а також на прикладі сучасних інструментів відстеження розглянуто можливі засоби аналізу блокчейн мереж, досліджено принципи обробки і властивості анонімності транзакцій у сучасних блокчейн системах.

1. Принципи формування та обробки транзакцій

Технологія блокчейн створює структуру даних з властивими її якостями безпеки. Вона заснована на принципах криптографії, децентралізації і консенсусу, які забезпечують довіру до учасників мережі і здійснених транзакцій. Як правило, в більшості технологій розподіленого реєстру дані упорядковані в блоках, і кожен з них містить одну або декілька транзакцій. Кожен новий блок підключається до усіх попередніх в криптографічний ланцюжок таким чином, що втручання стає неможливим [5]. Усі транзакції всередині блоків перевіряються і узгоджуються за допомогою механізму консенсусу, який гарантує, що кожна транзакція підтверджена більшістю валідаторів. Жоден користувач в мережі не може змінити запис транзакцій [2].

В залежності від алгоритму консенсусу обраної блокчейн-системи визначаються й певні особливості процесу видобутку блоків, адже від нього залежать такі характеристики, як: швидкість створення блоку, розмір ланцюжка блоків, обсяг середньої відправленої транзакції, швидкість підтвердження та інше. Але перш за все необхідно розібратися з тим, що представляє собою транзакція всередині блокчейн-мережі.

Під поняттям транзакції розуміють передачу криптовалюти або будь-якої іншої інформації з однієї адреси на іншу. При цьому, на відміну від банківських транзакцій, реального фізичного об'єкту передачі не існує, користувачі отримують криптовалюту через транзакцію і витрачають так само.

Пріоритет попадання операцій в новий блок наступний [6]:

1) персональні операції власників пулу;

2) розподіл прибутку на гаманці майнерів;

3) комерційні операції.

Процес перевірки та запису є негайним і неперервним. Користувач вказує адресу одержувача і кількість валюти, яку хоче відправити, та завіряє відправку транзакції своїм ключем. Відразу ж після цього транзакція надходить в пов'язане з гаманцем ядро і зберігається спеціальній зоні для непідтверджених транзакцій, що називається мемпулом. Якщо обрана з них транзакція буде схвалена більшістю вузлів, то вона записується в блок. Кожен блок містить перелік всіх транзакцій з відміткою часу та геш кожного попереднього блоку, завдяки якому їх можна розрізняти між собою, створивши безперервний ланцюжок. Для обробки кожного наступного блоку майнерам необхідно підтверджувати попередні транзакції, записані в більш ранніх блоках ланцюжка. Чим більше транзакція їх отримає, тим більш надійною вона буде вважатися. Після обробки і появи в блокчейн реєстрі транзакція вважається дійсною.

Транзакції у системі є публічними, тому усі учасники мережі мають змогу відстежувати весь потік криптовалюти, що надсилається між адресами. Однак більшість власників криптоактивів не бажають, щоб історії їх транзакцій і інформація облікового запису розкривалися іншим [1]. Як правило, користувачі не здатні виявити ніякі чужі особисті дані, адже кожній новій транзакції надається новий номер, що являє собою набір випадкових цифр. Він є свого роду захистом від небажаного втручання та ускладненням для атак [7]. Але у випадку, якщо навіть одна з транзакцій стане ідентифікованою і буде визначений її власник, то існує ймовірність, що окрім його історії переведень й власники інших транзакцій стануть відомі також.

Наявність проблеми, що полягає у відсутності повної конфіденційності, стало поштовхом для розробки нових анонімних платіжних блокчейн систем [1][8]. Найвідомішими прикладами таких криптовалют є: Monero, Dash, Zcash тощо [9]. Таким чином, анонімна або орієнтована на конфіденційність монета – це різновид криптовалют, головною метою яких є збереження приватності своїх користувачів.

На сьогодні існує декілька шляхів щодо підвищення анонімності у мережі блокчейн. Перша технологія заснована на змішуванні монет, ідея якої полягає в поєднанні кількох платежів в одну транзакцію, після чого розподіл коштів з пулу відбувається між відповідним одержувачами [1], друга – технологія доказів, заснованих на поліномах, такі як доказ з нульовим розголошенням – Zero-Knowledge Proof, який дозволяє зберігати і обмінюватися даними в захищеному вигляді, гарантуючи невтручання в процес комунікації третіх осіб.

Таким чином, анонімні транзакції є чудовим рішенням у забезпеченні конфіденційності учасників мережі. Це безумовне право користувачів, які бажають зберегти свої дії у секреті. Однак у той же час потрібно пам'ятати, що наявність такої анонімності в системі сьогодні все частіше стає приводом для проведення фінансових махінацій у мережі. У зв'язку з цим з'явилася необхідність в контролі за діями у блокчейн мережах та вдосконаленні усіх існуючих на даний час аспектів кіберзахисту.

2. Методи деанонімізації транзакцій

Дослідження деанонімізації криптовалют можна виконати двома засобами. Першим з них є аналіз ланцюжка транзакцій за допомогою відповідних мережевих інструментів, який полягає у відстеженні транзакцій по мережі та накопиченні загальнодоступних відомостей про них, а також пов'язуванні їх з особистими даними користувача [10]. Інший метод – це аналіз протоколу та мережі, який використовує характеристики розповсюдження транзакцій з криптовалютою для визначення вихідної IP-адреси нової транзакції [11, 12].

На сьогодні можна обирати серед комерційних послуг та інструментів з відкритим кодом, що забезпечують програмний доступ. Для відстеження шляху переміщення транзакцій до кінцевого одержувача дозволяють провести розглянуті далі сервіси.

Blockchain Explorer [13] – це один з найбільш відомих інструментів аналізу ланцюжка блоків. Він пропонує ряд можливостей для відстеження окремих транзакцій, а також надає інформацію у вигляді графіків і статистики всієї мережі. Крім того, з його допомогою можна провести аналіз стосовно руху коштів по мережі. На головній сторінці сервісу можемо побачити діаграми, що відображають зміни цін на криптовалюту за останній день, тиждень або місяць, а також сумарний розмір непідтверджених транзакцій в байтах. Крім того, маємо можливість детального перегляду інформації, що надає нам ще більшу кількість діаграм, які побудовані за валютною статистикою, деталями блоку, інформацією про їх видобуток, мережевою активністю, кількістю активних гаманців, а також ринковими сигналами. Також тут нам одразу відомі які і ким були отримані останні блоки, їх розмір, а також список непідтверджених транзакцій та суми, які були передані. Відображені відомості також можна розглянути детальніше і дізнатися час передачі окремої транзакції в мережу, комісію, яка була сплачена за її обробку, розмір транзакції, перелік адрес і сум з витраченими і отриманими коштами.

Matbea.net [14] – це послуга, яка дозволяє користувачам встановлювати належність біткоїн-адрес. Даний інструмент надає користувачам можливість шукати інформацію по транзакціям, адресам, блокам, xPub або yPub і видає результат у вигляді детальної текстової статистики. Послуга перекладена на кілька іноземних мов та має зрозумілий інтерфейс.

ORS CryptoHound [15] – це ще один інструмент дослідження мережі на базі штучного інтелекту, який використовується для дослідження Біткоїн та Ефіріум адрес і надає результати у вигляді списків, діаграм або таблиць. Інструмент пропонує можливості відстеження коштів за конкретною адресою, відображення залишку на балансі, візуалізацію відношень адрес і всіх транзакцій, що проведені нею, дозволяє виконувати статистичний розрахунок вартості монет, а також формування банківських звітів.

Сервіс Glassnode [16] являє собою аналітичну компанію, що займається аналітикою блокчейн мереж і надає оперативну інформацію про стан ринку, пропонуючи відображення результатів в різних категоріях.

Використання подібних інструментів з відкритим кодом є досить зручним за рахунок їх доступності, однак деякі з них вимагають багато часу для дослідження окремих ділянок мережі та транзакцій і проводити такий аналіз вручну стає неефективним. До того ж, щоб вчасно виявити загрозу і попередити атаки, необхідно мати здатність передбачення методів, які можуть застосувати зловмисники в мережі.

3. Відстеження транзакцій з використанням платформи GraphSense

Усі основні методи деанонімізації поєднала у собі система GraphSense Cryptoasset Analytics. Інструмент дозволяє реалізовувати пошук серед криптовалютних адрес, блоків, транзакцій та тегів, а також виявляти кластери, пов'язані з певною адресою. Цей проєкт розроблений австрійськими дослідниками, з метою допомогти користувачам відслідкувати переміщення коштів у мережі і виявити будь-які аномалії. Даний інструмент поєднує у собі можливості сучасних комерційних варіантів аналітики мереж та загальнодоступних з відкритим кодом [17]. GraphSense надає панель інструментів для базових досліджень мережі та

забезпечує гнучкість для виконання дослідницьких задач з наданням обчислень у вигляді графів. Система являє собою платформу для аналізу криптоактивів з забезпеченням повної незалежності даних, алгоритмічної прозорості та масштабованості. GraphSense має відкритий вихідний код і є безкоштовним. Окрім цього, надає інформаційну панель Dashboard для мережевих досліджень і, що є найголовнішим, повний контроль даних для виконання розширених завдань аналітики [18].

Під поняттям активу розуміємо економічний ресурс, що має певну цінність для користувача. Криптоактив, у свою чергу, це призначений для обміну віртуальний актив із використанням криптографії. Розрізняють такі види криптоактивів, як: власні криптовалюти (Native Cryptocurrencies), гарним прикладом яких є платіжна система Bitcoin і токени (Tokens), що розгорнуті на таких платформах, як Ethereum. З точки зору використання можна визначити токени оплати (Payment Tokens), токени безпеки (Security Tokens) і службові токени (Utility Tokens) [17].

Система проводить аналіз транзакцій в мережі у реальному часі, щоб отримати уявлення про їх функції і статистику. Особлива увага приділяється виявленню так званих аномалій, тобто ідентифікації тих транзакцій, які відхиляються від стандартних структур. Це дозволяє виявляти і відстежувати потенційно зловмисні дії на ранніх стадіях.

Інструмент має ряд особливостей, такі як [18]:

- можливість міжвалютного пошуку у системі за адресою, тегом, транзакцією або блоком у декількох регістрах криптовалюти;
- перевірка метаданих, властивостей вузлів та їх взаємодії;
- перегляд та переміщення по транзакціям, виявлених з різних реєстрів;
- підтримка аналітики на основі даних через REST API;
- автоматичний пошук шляхів транзакцій, які з'єднують два вузли;
- механізми Apache Spark та Cassandra в основі, задля досягнення лінійної масштабованості;
- використання інструменту BlockSci для аналізу ланцюжків блоків та фільтрації CoinJoins;
- програмне забезпечення є відкритим і має ліцензію MIT.

GraphSense надає можливість працювати з такими криптовалютами, як: Bitcoin, Bitcoin Cash, Ethereum, Litecoin і Zcash, а також іншими валютами моделі UTXO [5] [17].

Візуальна панель управління Dashboard працює у будь-якому сучасному веб-браузері і дозволяє виконувати перевірку блоків, транзакцій, адрес та сутностей, а також навігацію по ним. Таким чином, користувачі можуть відстежувати грошові потоки та будувати графи за результатами їхніх досліджень [17].

В процесі введення символів у поле пошуку система сама генерує можливі варіанти. Після того як ввели бажані дані для пошуку, на панелі управління з'являється графічне відображення питомої адреси у вигляді блоку, де відображається кількість відношень на вхідній та вихідній сторонах, а також завантажений суб'єкт для цієї адреси, який контролює кластером з 12 адрес, що обчислено методом кластеризації (рис. 1).

Address	First usage	Last usage	Final balance	Total received
122x97UkuMsT6hNQnDs3ytYwsKaPreQ4cK	03/25/2017 6:10:40 PM	03/26/2017 2:29:54 AM	0 BTC	0.0116 BTC
13wDiidMjFhcrd75zRkN6DNjBbMmetHZjq	03/26/2017 2:29:54 AM	03/29/2017 9:41:47 AM	0 BTC	5.9574 BTC
169rGApQW68tiprsy851tCZ6ACmLnmXkj4	07/26/2018 5:59:22 PM	07/29/2018 10:10:05 PM	0 BTC	0.15 BTC
✔ 18NSAybFEhLa6AG3gxEN1hiaRJoSvvbnDb	12/15/2016 4:37:11 AM	01/20/2020 3:43:06 PM	0 BTC	14.3924 BTC
19yijwxaFSzQ11GNeBHwpAYv29qJt2e4wT	10/02/2018 5:30:09 AM	01/06/2020 10:51:32 PM	0 BTC	0.9848 BTC
1AR3DiQftXZCNEGyhMg1kRs83tr2Ao6J1Z	12/17/2017 10:33:41 PM	01/06/2020 10:51:32 PM	0 BTC	0.0983 BTC
1JPeBHn5pYVudEFvgPqjpq9pbjdsAAR3vC	08/22/2017 5:09:50 AM	01/06/2020 10:51:32 PM	0 BTC	0.0077 BTC
1MupxiyR1HuGMrGU4trLxFwaRyRDm2W5gx	07/29/2018 10:10:05 PM	01/06/2020 10:51:32 PM	0	

Showing 1 to 9 of 12 entries

Рис. 1. Кластер адрес

Задача кластеризації полягає в ідентифікації схожих адрес, які при цьому є окремими входами однієї транзакції, і додаванні їх в одну групу, визначивши як ті, що належать одному власнику [19].

Також сервіс завантажує детальну статистику підключеної адреси, яка відображає інформацію про кількість проведених транзакцій, в яких адреса використовувалась в якості введення або виведення, кількість адрес, з яких було отримано та надіслано монети, дати першого та останнього використання, період активності та суму отриманих коштів, значення яких також можна конвертувати між валютами долара або євро. В цьому ж вікні можемо переглянути перелік проведених транзакцій, вхідних та вихідних адрес у вигляді таблиць (рис. 2). Також є можливість провести пошук окремої транзакції або адреси зі списку за необхідністю.

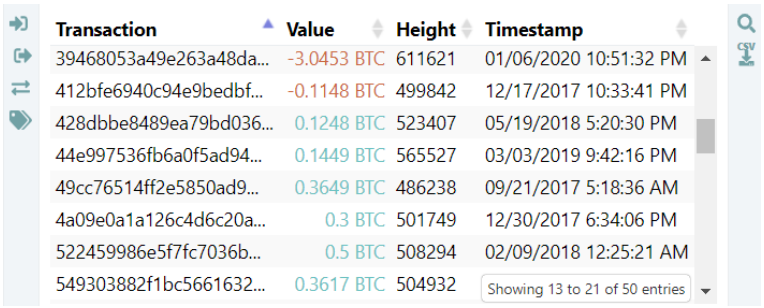


Рис. 2. Перелік проведених транзакцій

Платформа GraphSense надає можливість додатково дослідити кожне вхідне та вихідне відношення за допомогою побудови адресних графів і їх сутностей з усіма деталями. Можна обрати будь-яку адресу з таблиць і додати її до існуючого блоку (рис. 3).

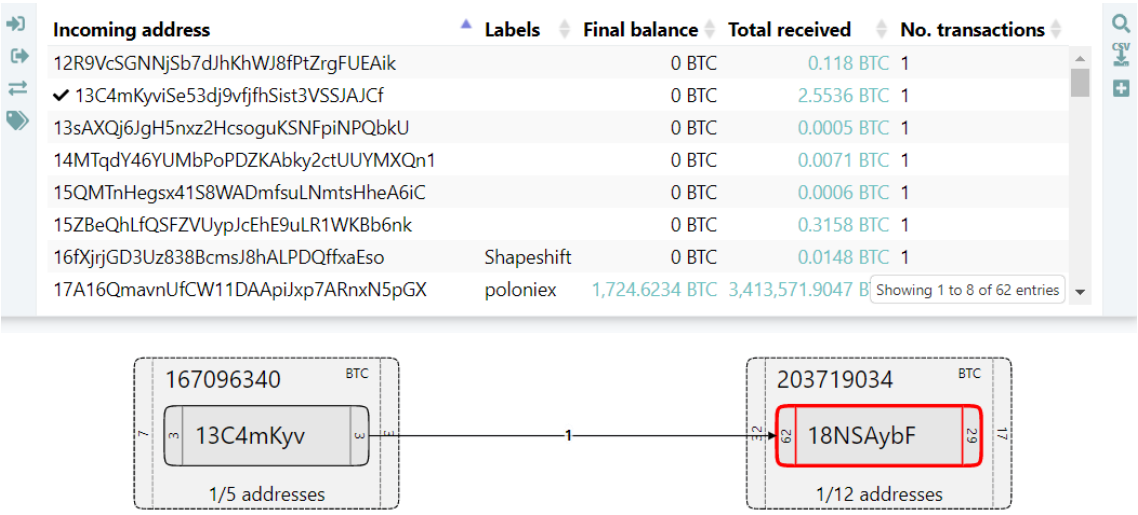


Рис. 3. Відображення вхідного відношення

Обравши транзакцію для детального перегляду можна дізнатися до якого блоку її було включено, час і дату її проведення, суму, яка була надіслана, побачити її джерело і призначення, тобто усі вихідні адреси, на які вона була надіслана.

Аналізуючи перелік транзакцій, як на вхідній, так і на вихідній сторонах, можна побачити, що існують адреси з відповідними мітками. Це теги, що є спільним позначенням адрес та сутностей криптоактивів деяких реальних комерційних організацій, таких як криптовалютні біржі, майнінг-пули та інші (рис. 4).

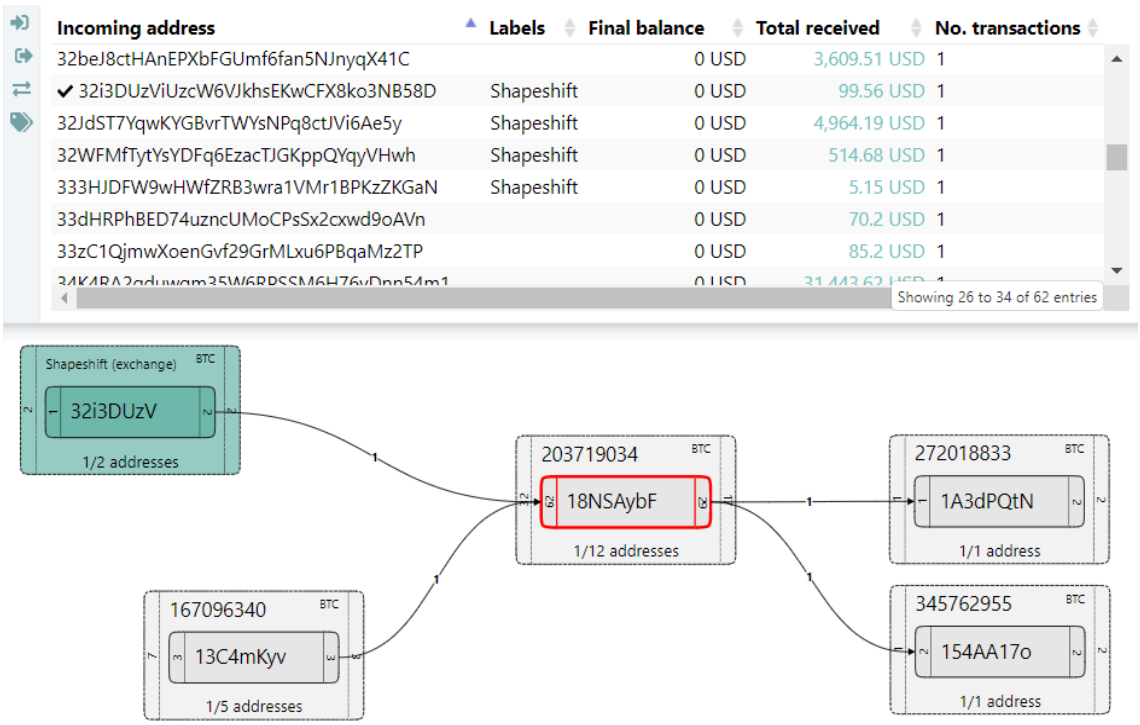


Рис. 4. Тегування адрес

Тегування є важливою функцією, адже, взаємодіючи з певними службами та призначаючи їх адресам зручні для обробки мітки, можна ідентифікувати клієнтів як ті, що належать і керуються відомими криптовалютними організаціями, групувати їх за відповідними тегами та категоріями і проводити ефективний аналіз мережі, відстежуючи операції відомих учасників. Платформа GraphSense використовує для цього файлову структуру TagPacks.

Даний інструмент є зручним у використанні, при цьому він пропонує велику кількість можливостей з високим рівнем ефективності, дозволяючи його користувачам отримувати статистику за запитом за досить швидкий час.

В перспективі, продовжуючи вдосконалення платформи і забезпечуючи зростаючий набір її функцій, GraphSense може стати гарним інструментом для тих підприємств і організацій, що займаються криптоактивами, для наукових досліджень, а також можливим вирішенням виникаючих проблеми щодо дотримання та регулювання безпечних відносин у Блокчейн мережах.

Висновки

Транзакції в блокчейн-мережі проводяться публічно, і кожен користувач в будь-який час може переглянути їх. Це досягається за рахунок прозорості, що є однією з головних відмінних рис технології. Однак не завжди учасники бажають, щоб інформація про стан їх заощадження і історії транзакцій були повністю відомі іншим. Конфіденційність користувачів може бути збережена за рахунок анонімних транзакцій.

Анонімність транзакцій – одна з причин популярності криптовалют та широкого поширення технології блокчейн. Однак її наявність у мережі є основою виникнення нечесних транзакцій, фінансових махінацій і атак на систему. На сьогодні найбільш актуальною проблемою Блокчейн мереж є зловживання криптовалютою з метою проведення злочинних дій. Тому з'явилася необхідність у постійному контролі за діями користувачів, у зв'язку з цим почалась активна розробка інструментів аналізу мережі, які здатні відстежувати історії здійснених транзакцій. Сьогодні можна обирати між комерційними послугами аналізу та інструментами з відкритим кодом.

Існуюча методологія деанонімізації транзакцій передбачає відстеження всієї історії їх просування по мережі. Для аналізу ланцюжка і збору даних можна використовувати такі

інструменти, як: Blockchain Explorer, Matbea.net, CryptoHound, Glassnode. Зручний та ефективний сервіс GraphSense дозволяє виконувати розширені завдання аналітики в реальному часі, з результатами у вигляді графів і таблиць з усією історією транзакцій, що дозволяє додатково досліджувати кожне вхідне і вихідне відношення за допомогою побудови адресних графів і спостерігати за всім ланцюжком, виявляючи аномальну поведінку у мережі.

Список літератури:

1. Rui Zhang, Rui Xue, Ling Liu. Security and Privacy on Blockchain // ACM Computing Surveys. 2019. Vol. 52, No. 3, Article 51. 34 p.
2. Distributed Ledger Technology: beyond block chain. A report by the UK Government Chief Scientific Adviser, 2016. 88 p.
3. Aaron Wright, Primavera De Filippi. Decentralized Blockchain Technology and the Rise of Lex Cryptographia, 2015. 58 p.
4. Колесников П.И., Бекетнова Ю.М., Крылов Г.О. Технология блокчейн. Анализ атак, стратегии защиты. 2017. 67 p.
5. What is blockchain security? *IBM*: веб-сайт. URL: https://www.ibm.com/topics/blockchain-security
6. Transactions in the BTC blockchain. *EXMO*: веб-сайт. URL: https://info.exmo.me/en/education/transactions-in-btc-blockchain/
7. A Survey on the Adoption of Blockchain in IoT: Challenges and Solutions / M.A. Uddin and others. Blockchain: Research and Applications, 2021. 80 p.
8. Harry Halpin, Marta Piekarska. Introduction to Security and Privacy on the Blockchain. IEEE European Symposium. 2017. 3 p.
9. Бедрій Т. А., Ісмайлов К. Ю., Медведенко С. В. Використання знань про особливості криптовалют у протидії злочинності // Кібербезпека в Україні: правові та організаційні питання: матеріали III Всеукр. наук.-практ. конф. Одеса, 2018. С. 140-144.
10. Androulaki E., Karame G. O., Roeschlin M., Scherer T., & Capkun S. Evaluating user privacy in Bitcoin // Financial Cryptography and Data Security – 17th International Conference, FC 2013, Revised Selected Papers. Vol. 7859 LNCS, pp. 34-51.
11. Philip Koshy, Diana Koshy, and Patrick McDaniel. An analysis of anonymity in bitcoin using p2p network traffic. 2014. Financial Cryptography, 2014.
12. Biryukov A., Khovratovich D., Pustogarov I. Deanonymisation of clients in Bitcoin P2P network, CoRR, Vol. abs, 2014.
13. Офіційний веб-сайт Blockchain Explorer. URL: https://www.blockchain.com/en/explorer
14. Офіційний веб-сайт Matbea.net. URL: https://matbea.net/
15. Офіційний веб-сайт ORS CryptoHound. URL: https://www.c-hound.ai/
16. Офіційний веб-сайт Glassnod. URL: https://studio.glassnode.com/
17. Bernhard Haslhofer and others. GraphSense: A General-Purpose Cryptoasset Analytics Platform. 2021. 16 p.
18. Офіційний сайт GraphSense. URL: https://graphsense.info/
19. Данильчук Р. К., Жураковська О. С. Задача кластеризації адрес в мережі Блокчейн // Міжнар. наук. журнал «Інтернаука». Київ, 2018. № 9(49). Т. 1. С. 43-46.

Надійшла до редколегії 12.10.2021

Відомості про авторів:

Дубіна Валерія Вадимівна – Харківський національний університет радіоелектроніки, магістрант, кафедра безпеки інформаційних технологій, факультет комп'ютерної інженерії та управління, Україна; email: valeriia.dubina@nure.ua; ORCID: https://orcid.org/0000-0002-8653-8025

Олійников Роман Васильович – д-р техн. наук, професор, Харківський національний університет імені В.Н. Каразіна, професор кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук; Україна; e-mail: roman.oliinykov@nure.ua; ORCID: https://orcid.org/0000-0002-3494-0493

УДК 003.026:004.056 **DOI:10.30837/rt.2021.4.207.05**

О.Є. ПЕТРЕНКО, канд. техн. наук, О.С. ПЕТРЕНКО, канд. техн. наук,
О.В. СЄВЄРІНОВ, канд. техн. наук, О.І. ФЄДЮШИН, канд. техн. наук,
А.В. ЗУБРИЧ, Д.В. ЩЕРБИНА

АНАЛІЗ ШЛЯХІВ ПІДВИЩЕННЯ СТІЙКОСТІ КРИПТОАЛГОРИТМІВ НА АЛГЕБРАЇЧНИХ РЕШІТКАХ ЩОДО ЧАСОВИХ АТАК

Вступ

Запропонований у 1994 році алгоритм Шора довів можливість факторизації числа за допомогою квантового комп'ютера з достатньою кількістю кубітів за поліноміальний час. Вказаний факт ставить під сумнів можливість застосування асиметричних криптосистем, таких як RSA. Поширене використання алгоритму в багатьох криптографічних додатках обумовило необхідність пошуку альтернативних крипостійких алгоритмів. З 2016 року Національний інститут стандартизації та технологій об'явив конкурс на вибір алгоритмів стійких до атак в постквантовий період. Результати конкурсного відбору будуть представлені у 2022 році. В теперішній час розроблено алгоритми NTRUEncrypt, NTRUSign, Falcon [1, 2], стійкість яких обумовлена складністю розв'язання задачі пошуку короткого вектору алгебраїчної решітки. Проблемним питанням при застосуванні алгоритмів є той факт, що вони ще мало досліджені, використовують обмежене коло параметрів, для яких була доведена крипостійкість до відомих атак. Алгоритми Falcon, NTRUEncrypt увійшли у другий тур конкурсу NIST та знаходяться на стадії ретельного вивчення. Запропоноване коло параметрів придатних до застосування унеможливлює поширене використання вказаних алгоритмів та не може зробити їх універсальним для вирішення широкого кола завдань в порівнянні з алгоритмом RSA. Дане проблемне питання вимагає подальших досліджень алгоритмів, що застосовують алгебраїчні решітки NTRU з метою розширення кола безпечних до застосування параметрів. Метою статті є дослідження алгоритмів, стійкість яких базується на пошуку короткого вектору решітки, з визначенням параметрів стійких до часових атак.

1. Алгоритми NTRUENCRYPT, NTRUSIGN

NTRUEncrypt – криптосистема з відкритим ключем, також відома як NTRU алгоритм шифрування, він являється решіткою на основі альтернативи RSA і ECC (Elliptic – curve cryptography) і основана на розв'язанні задачі, що пов'язана з пошуком найкоротшого вектору в решітці.

Алгоритм оснований на передбачуваній складності факторизації деяких многочленів із усіченого кільця многочленів в приватні два многочлена з дуже малими коефіцієнтами. Криптоаналіз криптосистеми тісно пов'язаний з алгоритмічною проблемою редукції решітки в певному класі. Для забезпечення криптографічної стійкості необхідним є проведення дослідження, яке дозволяє здійснити ретельний вибір параметрів, стійких до існуючих атак.

Оскільки і шифрування, і дешифрування використовують тільки просте поліноміальне множення, ці операції дуже швидкі в порівнянні з іншими схемами асиметричного шифрування, такими як RSA, ElGamal і криптографія на основі еліптичних кривих. Однак NTRUEncrypt [1] та пов'язаний з ним алгоритм цифрового підпису NTRUSign [2] ще не пройшли такий же обсяг криптографічного аналізу в розгорнутій формі.

Алгоритм NTRU та побудована на його основі асиметрична криптосистема базуються на перетвореннях на алгебраїчних решітках. NTRUEncrypt є ймовірно стійкою системою, тобто для зашифрування повідомлень використовують випадковий елемент. За цієї умови кожне повідомлення має багато шифротекстів. Стійкість криптосистеми NTRUEncrypt визначена експериментальним шляхом та базується на факті складності знаходження короткого вектору алгебраїчної решітки. Перевагою даної системи є факт, що шифрування, розшифрування повідомлення та процес створення ключів є швидким і легким в реалізації.

Алгоритми NTRUEncrypt, NTRUSign залежить від параметрів, які є цілими числами та можуть бути представлені у поліноміальному вигляді. Для того щоб параметри не сприяли виникненню випадкових помилок, при дешифруванні необхідно включати контрольні біти у кожній блок повідомлення.

Для побудови математичної моделі алгоритму використовують наступні параметри:

– N – розмірність кільця поліномів, що використовують при шифруванні повідомлень;

– p – натуральне число, що приймає участь в шифруванні та дешифруванні повідомлення;

– q – натуральне число, що приймає участь в шифруванні, дешифруванні повідомлення та при визначенні відкритого ключа;

– k – таємний ключ від якого залежить стійкість від атак;

– d_i (i=1,2) – розподіли коефіцієнтів многочленів, які застосовуються при формуванні відкритого та таємного ключів.

При генерації ключів розглядають кільце зрізаних поліномів $R = Z[x]/\left(x^N - 1\right)$. Кожний елемент кільця може бути представлений в поліноміальному $f = \sum_{s=0}^{N-1} f_s x^s$ або векторному вигляді $(f_0, f_1, f_2, ..., f_{N-1})$. Усі коефіцієнти полінома є цілими числами. Зменшити складність обчислення операції множення поліномів в кільці зрізаних поліномів можливо за рахунок застосування операції "згортки" за правилом: нехай необхідно перемножити 2 полінома $f = \sum_{s=0}^{N-1} f_s x^s$ та $g = \sum_{s=0}^{N-1} g_s x^s$ в кільці зрізаних поліномів $R = Z[x]/\left(x^N - 1\right)$. Результатом множення $h = f \otimes g$ є поліном виду: $h = \sum_{s=0}^{N-1} h_s x^s$, коефіцієнти якого обчислюються за формулою: $h_s = \sum_{i=0}^{s} f_i g_{s-i} + \sum_{i=s+1}^{N-1} f_i g_{N+s-i}$.

Дане правило дозволяє зменшити обчислювальну складність множення поліномів в $R = Z[x]/\left(x^N - 1\right)$ шляхом відсутності необхідності приводити по $\mathrm{mod}\left(x^N - 1\right)$ доданки, ступінь яких більше ніж *N*.

Параметри *p* та *q* необов'язково повинні бути простими числами, але обов'язково вони повинні задовольняти умовам: НСД(p, q)=1, параметр p повинен бути значно меншим за *q*. Використовуючи значення *p* та *q* випадково обирають 2 полінома f та g. Поліном f належить кільцю зрізаних поліномів $R = Z[x]/\left(x^N - 1\right)$ з розподілом коефіцієнтів по закону розподілу з параметром d_1. Це означає, що в поліномі f міститься d_1 коефіцієнтів, які дорівнюють 1, d_1 – 1 коефіцієнтів, які дорівнюють -1 та всі інші коефіцієнти дорівнюють 0. Такий розподіл коефіцієнтів обумовлює наявність оберненого полінома до полінома f Поліном g належить кільцю зрізаних поліномів $R = Z[x]/\left(x^N - 1\right)$ з розподілом коефіцієнтів по закону розподілу з параметром d_2. Це означає, що в поліномі g міститься d_2 коефіцієнтів, які дорівнюють 1, d_2 – 1 коефіцієнтів, які дорівнюють -1 та всі інші коефіцієнти дорівнюють 0. Застосовуючи коефіцієнти полінома f будують поліноми $f_p \equiv f(\mathrm{mod}\, p)$, $f_q \equiv f(\mathrm{mod}\, q)$. Отримані поліноми мають обернені поліноми в кільці зрізаних поліномів $R_p = Z_p[x]/\left(x^N - 1\right)$ та $R_q = Z_q[x]/\left(x^N - 1\right)$. Щодо поліномів, які отримані редукцією полінома g по модулю *p* та *q*, то вони не мають обернених поліномів в кільці зрізаних поліномів $R_p = Z_p[x]/\left(x^N - 1\right)$ та $R_q = Z_q[x]/\left(x^N - 1\right)$.

Відкритий ключ обчислюють за правилом: $h \equiv pf_q^{-1} \otimes g (\mathrm{mod}\, q)$. Слід зазначити, що поліном h та числа p та q – є відкритими параметрами, а поліном f та f_q^{-1} – таємними. Для зашифрування повідомлень випадковим чином обирають поліном r, який має розподіл коефіцієнтів d_3 в кільці зрізаних поліномів $R = Z[x]/(x^N - 1)$ та відкритий ключ h. Це означає, що в поліномі h міститься d_3 коефіцієнтів, які дорівнюють 1, d_3 коефіцієнтів, які дорівнюють -1 та всі інші коефіцієнти дорівнюють 0. Повідомлення m шифрується наступним чином: $c \equiv r \otimes h + m (\mathrm{mod}\, q)$. Розшифрування повідомлення здійснюють в два етапи.

Спочатку обчислюють поліном з цілими коефіцієнтами з проміжку $\left(\frac{-q}{2}, \frac{q}{2}\right)$ за формулою $a \equiv f \otimes c (\mathrm{mod}\, q)$. Далі обчислюють $f_q^{-1} \otimes a$.

Вказаний алгоритм шифрування має недолік, який пов'язаний з появою параметрів, що сприяють появі помилок, тому для кожного блоку повідомлення необхідно включати контрольні біти. Причина появи таких помилок полягає в невірному центруванні повідомлення. Позбутися її можливо шляхом обчислення полінома $a \equiv f \otimes c (\mathrm{mod}\, q)$ з цілими коефіцієнтами в проміжку $\left(\frac{-q}{2} + x, \frac{q}{2} + x\right)$ для невеликого значення x від'ємного чи додатного. Якщо даний алгоритм не спрацює, тоді повторюють процедуру шифрування.

Із процедури розшифрування можна дійти до висновку, що криптосистема NTRU являється вірогідною, тому зі зашифрованого тексту відкритий текст не завжди відновлюється правильно. Коректний вибір многочленів f, g, r дозволяє понизити вірогідність такої помилки до 2^{-100}.

2. Аналіз параметрів алгоритмів NTRUENCRYPT, NTRUSIGN.

Криптосистема NTRU володіє декількома перевагами, а саме: велика швидкість роботи і збільшення стійкості при фактично тієї самої довжині ключа, що і в RSA. Із мінусів поки що один – необхідність застосовувати тільки рекомендовані параметри. Саме ця вимога визивала загальну незадоволеність свого часу, коли виникла необхідність перехода на елептичні криві і сприяла усіяким підозрам про наявність лазійок, які полегшували у подальшому конструкторам шифру криптоаналіз. В табл. 1 представлено параметри для алгоритму NTRU, що рекомендовані до використання [3]. Рівномірний розподіл, який застосовується для вибору поліномів f, g ключової пари алгоритму, дозволяє обмежити норму короткого вектору решітки довжиною $2n$. Застосування рівномірного розподілу з точки зору атаки "грубої сили" дає непоганий результат та дозволяє для параметра $n = 503$ обрати коефіцієнти поліному f з 10^{235} варіантів, що в свою чергу зводить імовірність отримати коефіцієнти повним перебором до величини 2^{-705}.

Таблиця 1

Рекомендовані параметри для NTRU

	n	p	q	кількість одиниць в многочленах		
				f	g	r
NTRU 167:3	167	3	128	61	20	18
NTRU 251:3	251	3	128	50	24	16
NTRU 503:3	503	3	256	216	72	55
	n	p	q	кількість одиниць в многочленах		
				f	g	r
NTRU 167:2	167	2	127	45	35	18
NTRU 251:2	251	2	127	35	35	22
NTRU 503:2	503	2	253	155	100	65

Однак алгоритм NTRU має обмежене число параметрів, придатних до застосування в криптоперетвореннях, що повязано з вразливістю даного алгоритму до часових атак [4]. Згідно з вимогами конкурсу, який був оголошений Національним інститутом стандартизації та технологій США (NIST), на кращі асиметричні алгоритми шифрування та генерації цифрових підписів, було запропоновано розробити криптоалгоритми, які будуть стійкими крім стандартного набору атак до атак по бічних каналах та часових атак. При прийнятті рішень щодо стандартизації алгоритмів Національний інститут стандартизації та технологій спирається на доказ стійкості запропонованих параметрів, а також розробку та тестування контрзаходів для розширених атак по бічних каналах та часових атак. Алгоритм NTRU пройшов до другого туру конкурсу та все ще розглядається як альтернативний варіант для стандартизації. Одним з проблемних питань алгоритму NTRU є питання, що обумовлені обмеженим числом стійких до криптоаналізу параметрів та нестійкістю алгоритму до часових атак. Її сутність полягає в тому, що зловмисник може посилати довільно зашифровані тексти $c(x)$ одержувачу, такі що коефіцієнти $a(x)$ повністю залежить від секретного ключа $f(x)$. Витік в такому випадку відбувається до того, як буде перевірено дійсність $c(x)$. Тому, час виконання кроку дешифрування залежить від цих коефіцієнтів. Зловмисник може використати це, ретельно вимірявши, скільки часу займає операція дешифрування, і зробивши висновок з цього про значення коефіцієнтів секретного ключа.

Для усіх криптографічних конструкцій, які використовують алгебраїчні решітки, необхідним є генерація стійкого відкритого базису випадкової решітки. У таких криптографічних конструкціях можливо використати функцію з потаємним входом. Покращити криптографічну стійкість алгоритму до часових атак та атак по бічних каналах можливо шляхом використання для алгоритму NTRU дискретного нормального (Гаусівського) розподілу для генерації поліномів f, g, де в якості потаємного входу виступає середнє квадратичне відхилення нормального (Гаусівського) закону розподілу. Вибір середнєквадратичного відхилення σ при використанні функції з потаємним входом є важливим параметром, який необхідно встановити для забезпечення стійкості алгоритму. Достатньою умовою для рівня безпеки, встановлених Національним інститутом стандартизації та технологій, є умова прийняти значення параметра $\sigma \leq 1.312\,||B||_{GS}$, де $||B||_{GS}$ – це норма Грамма – Шмідта, яка дорівнює максимальному значенню Евклідової норми серед векторів, що отримано в процесі ортогоналізації Грамма – Шмідта. Вектори для обчислення норми Грамма – Шмідта обирають серед

базисних векторів, які задають решітку. У даному випадку $\sigma \leq 1.55\sqrt{q}$, де число q є простим числом, яке обчислюється за формулою: $q = k \cdot 2^n + 1$. Для забезпечення рівнів безпеки, згідно з вимогами Національного інституту стандартизації та технологій, покращити запропоновані параметри, які наведено в табл. 1, можливо, прийнявши $q = k \cdot 2^n + 1 = \mathrm{q} = 3 \cdot 4 \cdot 1024 + 1 = 3 \cdot 2^{12} + 1 = 12289$. Тоді при формуванні поліномів f, g використовується дискретний нормальний розподіл, який називають вибіркою Гауса з стандартним квадратичним відхиленням $\sigma = 1{,}17\sqrt{\frac{q}{2n}}$ та математичним сподіванням, яке дорівнює 0. Знаходиться вибірка за допомогою функції щільності імовірностей нормального (Гаусівського) закону розподілу, яка має вигляд $f_{\sigma,a}(x) = e^{\frac{-\pi\|x-a\|^2}{\sigma^2}}$. Для створення нормального (Гаусівського) розподілу необхідно висунути ряд умов. По-перше, необхідно запропонувати дискретний Гаусівський розподіл над цілими числами з усіма властивостями, які очікуються від вибірки для широкого застосування. Дискретний нормальний (Гаусівський) розподіл має бути простим і модульним, що дозволить спростити аналіз отриманих результатів. Необхідно довести безпечність вказаного дискретного розподілу відносно часових атак.

Простота та модульність є першим аспектом, який слід прийняти до уваги. На високому рівні структура потребує лише два компоненти (базовий компонент та компонент відхилення) та поєднує їх простим способом за допомогою "чорного ящика".

Універсальність алгоритму є другим його аспектом. Алгоритм вибірки Гауса за допомогою дискретного нормального (Гаусівського) розподілу працює з довільним математичним сподіванням та стандартним квадратичним відхиленням. Крім того, не передбачено застосування попереднього обчислення: враховуючи фіксовану базову вибірку параметра (Z_n) max, структура дозволяє здійснювати вибірку з множини алгебраїчних решіток DZ для будь-якого (Z_n) max.

Для досягнення постійного часу перетворень застосовується вибірка Гауса за допомогою дискретного нормального (Гаусівського) розподілу, на основі якого створюють вибірку з відхиленням. Вибірка Гауса відрізняється від нормального розподілу та обирає для побудови дискретного розподілу значення z, використовуючи функцію $D_{S,\sigma,a}(z) = f_{\sigma,a}(z) / f_{\sigma,a}(S)$, де z приймає лише цілі додатні значення. Якщо математичне сподівання дорівнює нулю значення $f_{\sigma,a}(S) = \sigma\sqrt{2\pi}$. Для створення дискретної вибірки застосовується таблиця, доступ до якої здійснюється за постійний час. З огляду на те, що запропонована вибірка використовує лише цілі значення та працює як дискретний набір випадкових послідовностей, виникає питання щодо відповідності характеристик отриманого дискретного розподілу до характеристик нормального розподілу. Вирішити дане питання можливо шляхом перевірки отриманих випадкових значень на відповідність до нормального розподілу. Здійснюють дану перевірку на основі різних статистичних тестів та критеріїв. Одним з таких критеріїв є критерій Пірсона, який дозволяє перевірити відповідає вибірки з генеральної сукупності властивостям генеральної сукупності.

Набір тестів SAGA [5] дозволяє перевірити, чи дійсно вибірка Гауса, яка отримана за допомогою дискретного нормального розподілу, має властивості, притаманні нормальному закону розподілу. Використовуються стандартні статистичні інструменти, які дозволяють перевірити роботу алгоритму, що реалізує дискретну вибірку Гауса з точки зору коректності отримання середнього значення, стандартного відхилення, асиметрії і ексцеса. Крім того, вказаний інструмент перевіряє нормально розподілені вихідні дані алгоритму чи ні. Вказана перевірка здійснюється на основі критерія Пірсона. Асиметрія і ексцес нормального розподілу вимірюють відповідно симетрію і плосковершинність або гостровершинність щільності ймовірності розподілу. Повний статистичний аналіз цих тестів було реалізовано за допомогою Python клас Univariate Samples, який приймає в якості аргументів ініціалізації очікуване середнє значення (mu), очікуване стандартне відхилення (sigma) і список спостережуваних одновимірних Гаусових вибірок (data). Крім одновимірного застосування, вказаний набір тестів SAGA, можливо застосувати і для багатовимірного випадку. Дана властивість дозволяє використати тести для багатовимірних випадків, а саме для побудови дискретного нормального багатовимірного (Гаусівського) розподілу для генерації базисів алгебраїчних решіток.

Багатомірні тести на перевірку вихідних даних вибірки Гауса також спрямовані на перевірку отримання нормального розподілу при заданих вхідних параметрах. Вказані тести дозволяють виявити випадки, коли при реалізації алгоритму вибірки Гауса з цілими числами високорівнева схема (наприклад, схема підписів) використовує її неправильно і призводить до некоректного значення багатомірної вибірки Гауса.

Крім того, тести SAGA розроблені для роботи в загальному вигляді, незалежно від техніки, вимагаючи при цьому лише введення або список одномірних або багатомірних вибірок Гауса. SAGA може застосовуватись до будь-якої криптографічної схеми на основі решітки, що вимагає застосування вибірки Гауса. Пошук нових наборів параметрів алгоритмів NTRU, які є стійкими до часових атак, здійснено з застосовуванням Гаусівської дискретної вибірки замість рівномірного розподілу для побудови ключів. Для запуску роботи тестів на першому

кроці обирають прийнятні з точки зору криптостійкості значення середньоквадратичного відхилення. Враховуючи той факт, що значення середньоквадратичного відхилення пов'язане з нормою короткого вектору алгебраїчної решітки, прийнятними значеннями для середньоквадратичного відхилення. В ході дослідження реалізовано тести SAGA для перевірки відповідності властивостей вибірок Гауса нормальному розподілу. Реалізація тестів SAGA для деяких значень середньоквадратичного відхилення та математичного сподівання з можливого діапазону та прийнятних для застосування в криптоперетвореннях на алгебраїчних решітках довжинах поліномів з перевіркою отриманих вибірок Гауса на відповідність нормальному розподілу наведено в табл. 2 – 5.

Відповідно до результатів, наведених в табл. 2 – 5, вибірки Гауса, які створені за допомогою дискретного нормального (Гаусівського) розподілу, мають такі ж самі властивості що й для нормального розподілу.

Таблиця 2

Перевірка тестів SAGA для параметрів алгоритму NTRU для ступеня полінома 509

Довжина поліному	509		
Середнє значення	0.00197	0.06680	0.01965
Середньоквадратичне відхилення	0.81690	0.82177	0.82424
Коефіцієнт асиметрії	-0.00362	-0.12402	-0.03644
Ексцес	-1.50146	-1.50876	-1.52716
Хі-2 статистичний	472.782	528.205	491.059
Хі-2 р-значення (повинне бути більше 0.001)	$5.67*10^{-98}$	$6.89*10^{-110}$	$6.70*10^{-102}$
Чи поліном дійсний?	Так	Так	Так

Таблиця 3

Перевірка тестів SAGA для параметрів алгоритму NTRU для ступеня полінома 677

Довжина поліному	677		
Середнє значення	-0.00739	-0.00739	-0.00739
Середньоквадратичне відхилення	0.81253	0.81253	0.81253
Коефіцієнт асиметрії	0.01350	0.01350	0.01350
Ексцес	-1.48521	-1.48521	-1.48521
Хі-2 статистичний	612.838	612.838	612.838
Хі-2 р-значення (повинне бути більше 0.001)	$4.06*10^{-127}$	$4.06*10^{-127}$	$4.06*10^{-127}$
Чи поліном дійсний?	Так	Так	Так

Таблиця 4

Перевірка тестів SAGA для параметрів алгоритму NTRU для ступеня полінома 701

Довжина поліному	701		
Середнє значення	0.00999	0.00999	0.00999
Середньоквадратичне відхилення	0.80026	0.80026	0.80026
Коефіцієнт асиметрії	-0.01795	-0.01795	-0.01795
Ексцес	-1.43830	-1.43830	-1.43830
Хі-2 статистичний	645.538	645.538	645.538
Хі-2 р-значення (повинне бути більше 0.001)	$3.76*10^{-134}$	$3.76*10^{-134}$	$3.76*10^{-134}$
Чи поліном дійсний?	Так	Так	Так

Таблиця 5

Перевірка тестів SAGA для параметрів алгоритму NTRU для ступеня полінома 821

Довжина поліному	821		
Середнє значення	-0.01340	-0.01340	-0.01340
Середньоквадратичне відхилення	0.81165	0.81165	0.81165
Коефіцієнт асиметрії	0.02447	0.02447	0.02447
Ексцес	-1.48163	-1.48163	-1.48163
Xi-2 статистичний	739.597	739.597	739.597
Xi-2 p-значення (повинне бути більше 0.001)	$2.12*10^{-154}$	$2.12*10^{-154}$	$2.12*10^{-154}$
Чи поліном дійсний?	Так	Так	Так

З огляду на це, дискретні вибірки Гауса можна застосувати для покращення стійкості алгоритму NTRU до часових атак.

Застосовуючи статистичні тести SAGA над поліномами криптографічних перетворень NTRU, було зроблено висновок, що дискретна Гаусівська вибірка дозволяє генерувати стійкі до часових атак параметри, використовуючи в якості середньоквадратичного відхилення норму або довжину короткого базису (вектору) решітки.

Список літератури:

1. Hoffstein J., Lieman D., Pipjer J., Silverman J. NTRU: A public key cryptosystem // Conference International Algorithmic Number Theory Symposium Springer, Berlin, Heidelberg Pages 267-288 Publication date 1998/6/21.
2. Alagic G., Alperin-Sheriff J., Apon D., Cooper D., Dang Q., Miller C., Moody D., Peralta R., Perlner R., Robinson A., Smith-Tone D. and Y.-K. Liu. Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process. National Institute of Standards and Technology, Interagency/Internal Report 8240, 2019.
3. IEEE Standard Specification for Public Key Cryptographic Techniques Based on Hard Problems over Lattices', Institute of Electrical and Electronics Engineers, IEEE Standard 1363.1-2008, 2009.
4. Kocher P. C. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems // Advances in Cryptology – CRYPTO'96, in Lecture Notes in Computer Science, vol. 1109, Springer, Berlin, Heidelberg, 1996. P. 104–113.
5. Isochronous Gaussian Sampling: From Inception to Implementation. With James Howe and Thomas Prest and Thomas Ricosset. In the proceedings of PQ-Crypto 2020.

Надійшла до редколегії 08.11.2021

Відомості про авторів:

Петренко Ольга Євгенівна – канд. техн. наук, доцент, Харківський національний університет радіоелектроніки, доцент кафедри безпеки інформаційних технологій, факультет комп'ютерної інженерії та управління; Україна; email: olha.petrenko@nure.ua; ORCID: https://orcid.org/0000-0002-7862-5399

Петренко Олексій Сергійович – канд. техн. наук, Харківський національний університет Повітряних Сил, заступник начальника науково-дослідного відділу наукового центру Повітряних Сил; Україна; email: alexwgs78@gmail.com; ORCID: https://orcid.org/0000-0001-9903-7388

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

Федюшин Олександр Іванович – канд. техн. наук, доцент, Харківський національний університет радіоелектроніки, доцент кафедри безпеки інформаційних технологій, факультет комп'ютерної інженерії та управління; Україна; email: oleksandr.fediushyn@nure.ua; ORCID: http://orcid.org/0000-0002-3600-405X

Зубрич Артем Віталійович – Харківський національний університет радіоелектроніки, студент кафедри безпеки інформаційних технологій, факультет комп'ютерної інженерії та управління; Україна; email: artem.zubrych@nure.ua

Щербина Денис Вадимович – Харківський національний університет радіоелектроніки, магістрант кафедри безпеки інформаційних технологій, факультет комп'ютерної інженерії та управління; Україна; email: denys.shcherbyna@nure.ua

УДК 004.056.55 **DOI:10.30837/rt.2021.4.207.06**

В.І. РУЖЕНЦЕВ, д-р техн. наук, О.І. ФЕДЮШИН, канд. техн. наук, С.А. КОХАН

АНАЛІЗ СТІЙКОСТІ ARX СХЕМ ШИФРУВАННЯ ДО ІНТЕГРАЛЬНОЇ АТАКИ ТА АТАКИ НЕЗДІЙСНЕНИХ ДИФЕРЕНЦІАЛІВ

Вступ

Серед малоресурсних криптоалгоритмів перспективними вважаються Addition- Rotation-XOR (ARX) схеми, тобто алгоритми, які використовують лише три види операцій: Addition – модульне додавання, Rotation – циклічний зсув та XOR додавання. У попередніх роботах [1, 2] було обрано найбільш відомі алгоритми цього класу, розроблено зменшені моделі (розмір блоку 16 бітів) цих алгоритмів та проаналізовано стійкість до атак диференційного, лінійного криптоаналізу, а також ступінь нелінійності цих ARX перетворень. Однак на основі аналізу літератури з описом атак на ARX алгоритми зроблено висновок про високу ефективність інтегральної атаки та атаки нездійсненних диференціалів проти цих алгоритмів. Отже метою цієї роботи є аналіз стійкості 16-бітних ARX перетворень до більш спеціалізованих та ефективних для цього виду перетворень інтегральної атаки та атаки нездійсненних диференціалів.

Для досягнення мети потрібно обрати та реалізувати методи аналізу стійкості до інтегральної атаки та атаки нездійсненних диференціалів і застосувати їх до обраних зменшених ARX алгоритмів.

Зменшені ARX моделі та початковий аналіз стійкості

В цій частині наведено опис використаних в роботі 16-бітних ARX моделей, більшість з яких вже були представлені та розглядались в роботах [1, 2], а також основні результати аналізу цих схем з наведених робіт.

Перша ARX-схема ChaCha – це quarter-round потокового алгоритму Chacha 2 [3] зі зменшеним розміром підблоків. 16-бітовий блок схеми складається з чотирьох 4-бітових підблоків (рис. 1).

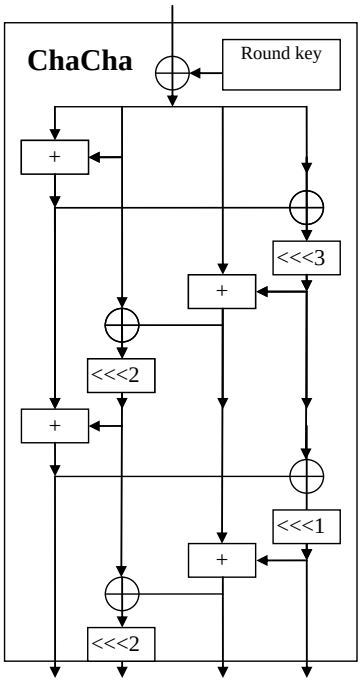


Рис. 1. ChaCha схема

Друга ARX-схема Speckey – це спрощена схема алгоритму Speck [4]. Спрощення полягає у відсутності двох операцій циклічного зсуву, які в оригінальному варіанті передували операціям модульного додавання. 16-бітовий блок схеми Speckey складається з двох 8-бітових підблоків (рис. 2).

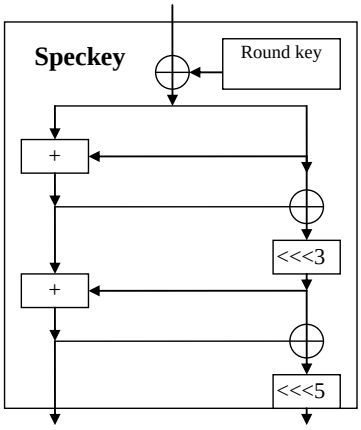


Рис. 2. Speckey схема

Зменшена модель циклу алгоритму Simon [4] представлена на рис. 3.

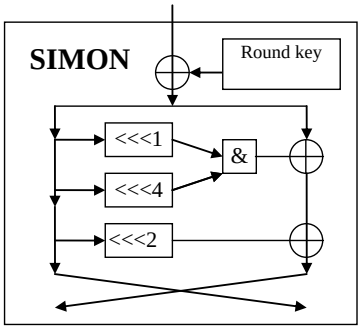
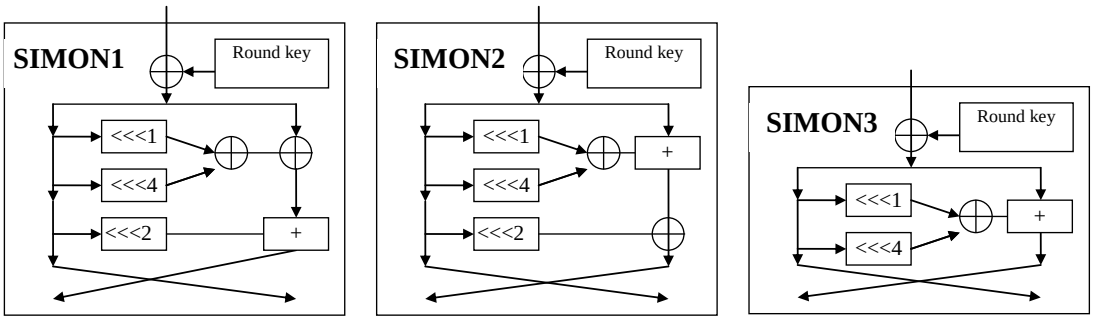


Рис. 3. Схема циклової функції шифру Simon

В роботі також розглядаються модифікації Simon1, Simon2, Simon3, які представлено на рис. 4 та які замість операції AND та деяких операцій XOR використовують модульне додавання.



а *б* *в*

Рис. 4. Модифікації циклової функції шифру Simon

Наступна ARX-схема – це зменшена схема алгоритму Chaskey [5]. 16-бітовий блок схеми Chaskey складається з чотирьох 4-бітових підблоків (рис. 5).

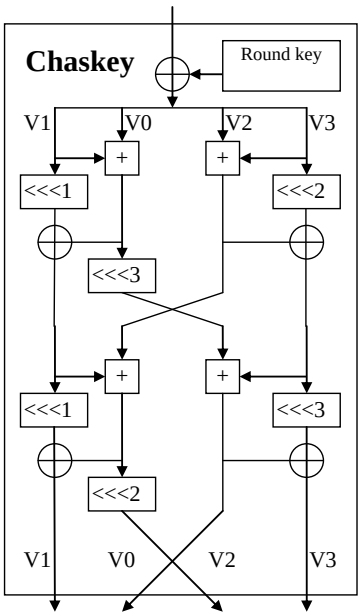


Рис. 5. Схема циклової функції схеми Chaskey

Ще одна ARX-схема – це зменшена схема S-блоку з алгоритма Sparkle, який в [6] названий Alzette. 16-бітовий блок зменшеної схеми Alzette складається з двох 8-бітових підблоків (рис. 6).

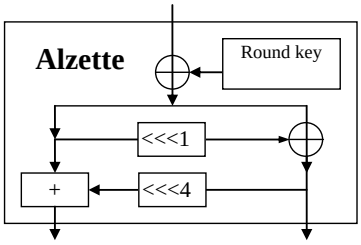


Рис. 6. Циклова функція схеми Alzette

У табл. 1 представлено кількість і формат операцій для розглянутих вище схем.

Таблиця 1

Кількість та формат операцій в одному циклі шифруючих перетворень (без додавання ключа)

Шифруючі схеми	Модульне додавання (Addition)	Циклічний зсув (Rotation)	XOR
Speckey	2*8 bit	2*8 bit	2*8 bit
ChaCha	4*4 bit	4*4 bit	4*4 bit
Simon	1*8 bit	3*8 bit	1*8 bit +1 AND
Simon1	1*8 bit	3*8 bit	2*8 bit
Simon2	1*8 bit	3*8 bit	2*8 bit
Simon3	1*8 bit	2*8 bit	1*8 bit
Chaskey	4*4 bit	4*4 bit	4*4 bit
Alzette	1*8 bit	2*8 bit	1*8 bit

В роботах [1, 2] схеми використовували одну операцію XOR додавання з ключем на початку перетворень і, потім, деяку кількість циклових перетворень. Аналіз показників криптографічної стійкості зменшених моделей (16 бітний блок та ключ) в [1, 2] продемонстрував, що майже для усіх з них можливо отримати показники випадкової підстановки при використанні певної кількості циклів. Виключенням стала схема алгоритму Simon – не дозволяє отримати ці показники навіть при великій кількості циклів. Схеми, що оперують

4-бітними та 8-бітними підблоками показували схожі результати. Так, схеми з 4-бітними блоками потребували 60 – 72 ARX операцій, а схеми з 8-бітними блоками потребували 32-36 ARX операцій для досягнення диференційних та лінійних показників випадкових підстановок. Підсумкові таблиці з мінімальною кількістю циклів та кількістю елементарних операцій для забезпечення показників випадкової підстановки з робіт [1, 2] представлено у табл. 2, 3.

Таблиця 2

Кількість 8-бітних операцій для забезпечення стійкості проти диференційних, лінійних та алгебраїчних атак

Шифруючі схеми	Мінімальна кількість циклів	Кількість 8-бітних операцій			
		Addition	Rotation	Xor	Всього
Speckey	6	12	12	12	36
Simon2	6	6	18	12	36
Simon3	8	8	16	8	32
Alzette	9	9	18	9	36

Таблиця 3

Кількість 4-бітних операцій для забезпечення стійкості проти диференційних, лінійних та алгебраїчних атак

Шифруючі схеми	Мінімальна кількість циклів	Кількість 4-бітних операцій			
		Addition	Rotation	Xor	Всього
ChaCha	6	24	24	24	72
Chaskey	5	20	20	20	60

Аналіз стійкості до інтегральної атаки

Інтегральний криптоаналіз є одним з найбільш ефективних видів нападу на найпоширеніший у світі шифр Rijndael і його варіант – AES зі зменшеною кількістю циклів. Аналіз робіт, присвячених криптоаналізу ARX-алгоритмів, показав, що і для цього класу шифрів атака є однієї з найбільш успішних.

Інтегральною атака названа тому, що в атаці розглядається проходження через перетворення шифру суми станів. Тут під різними станами розуміються деякі проміжні значення блоків даних у процесі їхнього зашифрування. Подібно тому, як у диференційній атаці виконується "транспортування" різності через перетворення шифру, у даній атаці через цикли шифру проводиться значення суми деякої кількості станів.

Якщо є можливість з високою ймовірністю визначити значення деяких бітів суми станів після r циклів шифрування, то це означає, що може бути організована інтегральна атака на (r+1)-цикловий шифр.

Для проведення аналізу стійкості ARX схем до інтегральної атаки був використаний метод [7]. У табл. 4 наведено алгоритм для тестування стійкості.

Таблиця 4

Алгоритм пошуку R-циклових інтегралів

	Вхідні дані: 16 бітне R-циклове шифруюче перетворення E. Num_key – кількість випадково обраних ключів.
1	Перебір всіх 16 варіантів позиції пасивного біта у вхідному блоці
1.1	Перебір Num_key варіантів ключа k.
1.1.1	Формування 2^{15} 16 бітних вхідних станів x
1.1.2	Зашифрування кожного з 2^{15} 16 бітних вхідних станів: $E_k(x)$
1.2	Перевірка наявності збалансованих бітів (XOR сума на всій множині криптограм дорівнює 0) в криптограмах для поточного варіанта позиції пасивного біта на вході
	Вихідні дані: Знайдені збалансовані біти в криптограмах – R-циклові інтеграли.

Цей алгоритм було використано для пошуку інтегралів для всіх 16-бітних ARX схем.

Кількість ключів Num_key в роботі [7] запропоновано 10, але в експериментах використовували 32.

Одним з найбільш цікавих висновків аналізу стало те, що жодна з розглянутих зменшених моделей (16-бітний блок та ключ) з лише однією операцією XOR додавання з ключем (саме такий варіант перетворень розглядався в роботах [1, 2]) не забезпечує відсутності інтегралів при будь-якій кількості циклів.

Для всіх варіантів схеми Simon (чотири схеми, що представлені на рис. 3, 4) потрібно використовувати щонайменше три операції XOR додавання з ключем, щоб, використовуючи вказану у табл. 5 кількість циклів, забезпечити відсутність інтегралів.

Таблиця 5

Кількість 8-бітних операцій для забезпечення відсутності інтегралів

Схема	Мінімальна кількість XOR додавань з ключем	Мінімальна кількість циклів	Кількість ARX операцій			
			Addition	Rotation	Xor	Всього
Speckey	2	5	10	10	10	30
simon	3	10	10	30	20	60
Simon1	3	7	7	21	14	42
Simon2	3	7	7	21	14	42
Simon3	3	7	7	21	14	42
Alzette	2	9	9	18	9	36

Таблиця 6

Кількість 4-бітних операцій для забезпечення відсутності інтегралів

Схема	Мінімальна кількість XOR додавань з ключем	Мінімальна кількість циклів	Кількість ARX операцій			
			Addition	Rotation	Xor	Всього
ChaCha	2	10	40	40	40	120
Chaskey	2	6	24	24	24	72

Для інших схем (Speckey, Alzette, ChaCha, Chaskey) потрібно використовувати щонайменше дві операції XOR додавання з ключем для можливості забезпечення відсутності інтегралів при належній кількості циклів (див. табл. 5, 6).

Важливо також те, що подальше збільшення кількості операцій XOR додавання з ключем не змінює мінімальної кількості циклів для забезпечення стійкості для усіх схем, що розглядаються.

З табл. 5 бачимо, що кращій результат стійкості до інтегральної атаки серед схем, що оперують 8-бітовими блоками, демонструє схема Speckey. Ця схема потребує 30 операцій для забезпечення відсутності інтегралів. Найгірший результат демонструє Simon – 60 операцій. Серед схем, що оперують 4-бітовими блоками (див. табл. 6), краща – Chaskey – 72 операції, гірша ChaCha – 120 операцій. На відміну від результатів, що були представлені в роботах [1, 2], відмінності між кращими та гіршими схемами більш суттєві – майже в два рази.

Якщо порівнювати всі розглянуті схеми і рахувати, що одна 8-бітова операція еквівалентна двом 4-бітовим, то найуспішнішою схемою з точки зору стійкості до інтегральної атаки можна вважати Speckey.

Аналіз стійкості до атаки нездійснених диференціалів

Криптоаналітичний метод називається атакою нездійснених диференціалів (НД), оскільки використовує диференціали спеціального виду – ті, котрі не можуть здійснитися, тобто мають нульову ймовірність. Атака нездійснених диференціалів на r-цикловий шифр стає можливою, коли є $(r\text{-}1)$-цикловий НД.

Атака є однією з найбільш ефективних для сучасних алгоритмів шифрування, у тому числі і для ARX алгоритмів.

Алгоритм, який було використано для пошуку НД, наведено у табл. 7.

Таблиця 7

Алгоритм пошуку НД

Вхідні дані: Шифруюче перетворення E. Пуста строка таблиці різності відповідного розміру.	
1	Перебір всіх варіантів вхідної різності d
1.1	У строку таблиці різності запусують всі «0»
1.2	Перебір Num_key варіантів ключа k
1.2.1	Перебір всіх варіантів вхідного значення x
1.2.1.1	Інкрементуємо ячійку з індексом $E_k(x)$ xor $E_k(x$ xor $d)$
1.3	Перевіряємо строку таблиці різності на наявність «0». Кожен такий «0» відповідає НД
	Вихідні дані: Знайдені НД.

Алгоритм з табл. 5 було використано для пошуку інтегралів для всіх 16-бітних ARX схем. Експериментально визначено кількість ключів Num_key = 32, яка потрібна для того, щоб при певній кількості циклів не існувало НД. Відомо, що при малій кількості ключів завжди існують НД для будь-якої кількості циклів.

Як і в попередньому розділі важливим для забезпечення стійкості виявилась кількість операцій XOR додавання з ключем. Знову лише одна операція XOR додавання з ключем (саме такий варіант перетворень розглядався в роботах [1, 2]) не забезпечує стійкості при будь-якій кількості циклів для всіх схем.

Щонайменше дві операції XOR додавання з ключем достатньо для лише для двох схем: Chaskey та Speckey. Для всіх інших схем потрібно не менше трьох операцій XOR додавання з ключем для забезпечення відсутності нездійснених диференціалів (див. табл. 8, 9).

Таблиця 8

Кількість 8-бітних операцій для забезпечення відсутності нездійснених диференціалів

Схема	Мінімальна кількість XOR додавань з ключем	Мінімальна кількість циклів	Кількість ARX операцій			
			Addition	Rotation	Xor	Всього
Speckey	2	5	10	10	10	30
simon	3	9	9	27	18	54
Simon1	3	7	7	21	14	42
Simon2	3	6	6	18	12	36
Simon3	3	6	6	18	12	36
Alzette	3	9	9	18	9	36

Таблиця 9

Кількість 4-бітних операцій для забезпечення відсутності нездійснених диференціалів

Схема	Мінімальна кількість XOR додавань з ключем	Мінімальна кількість циклів	Кількість ARX операцій			
			Addition	Rotation	Xor	Total
ChaCha	3	9	36	36	36	108
Chaskey	2	5	20	20	20	60

Порівнюючи результати аналізу наявності інтегралів (табл. 5, 6) та нездійснених диференціалів (табл. 8, 9) для зменшених 16-бітних ARX схем, можна побачити, що для досягнення відсутності нездійснених диференціалів потрібно або стільки, або на 1 менше циклів, ніж для досягнення відсутності інтегралів. Але для деяких схем (Alzette, ChaCha) при цьому потрібно більше XOR додавань з ключем.

Підсумкові дані щодо кількості циклів, кількості XOR додавань з ключем та кількості елементарних ARX перетворень, які потрібні для того, щоб перетворення не відрізнялись від випадкової підстановки, наведено в табл. 10, 11 (дані отримані на основі табл. 2, 3, 5, 6, 8, 9).

Таблиця 10

Кількість 8-бітних операцій для забезпечення показників випадкової підстановки

Схема	Мінімальна кількість XOR додавань з ключем	Мінімальна кількість циклів	Кількість ARX операцій			
			Addition	Rotation	Xor	Всього
Speckey	2	6	12	12	12	36
Simon	3	10	10	30	20	60
Simon1	3	7	7	21	14	42
Simon2	3	7	7	21	14	42
Simon3	3	8	8	24	16	48
Alzette	3	9	9	18	9	36

Таблиця 11

Кількість 4-бітних операцій для забезпечення показників випадкової підстановки

Схема	Мінімальна кількість XOR додавань з ключем	Мінімальна кількість циклів	Кількість ARX операцій			
			Addition	Rotation	Xor	Total
ChaCha	3	10	40	40	40	120
Chaskey	2	6	24	24	24	72

На основі табл. 10 можна виділити найкращі 8-бітові схеми: Speckey та Alzette. При цьому Speckey потребує меншої кількості XOR додавань з ключем. Найгірші показники продемонструвала схема Simon, яка потребує майже вдвічі більшої кількості операцій (60 проти 36). Серед 4-бітних схем (табл. 11) кращою є Chaskey, яка потребує 72 4-бітних операції. Якщо рахувати, що одна 8 бітова операція еквівалентна двом 4-бітовим, то ця схема еквівалентна кращій 8-бітній схемі Speckey.

Висновки

1. Проаналізовано показники криптографічної стійкості зменшених моделей (16 бітний блок та ключ) відомих та поширених сьогодні ARX алгоритмів шифрування: Chacha, Speckey, Simon, Chaskey, Sparkle та їх модифікації до найбільш ефективних для цього класу алгоритмів атак: інтегральна атака та атака нездійснених диференціалів. Продемонстровано, що для більшості з них можливо отримати показники випадкової підстановки при використанні певної кількості циклів та певної кількості XOR додавань з ключем.

2. Одним з цікавих висновків аналізу стало те, що жодна з розглянутих зменшених моделей (16 бітний блок та ключ) з лише однією операцію XOR додавання з ключем (саме такий варіант перетворень розглядався в роботах [1, 2]) не забезпечує відсутності інтегралів та нездійснених диференціалів при будь-якій кількості циклів, що, на наш погляд, свідчить про більшу ефективність атак, що розглядаються в цій роботі, а також про важливість операцій додавання з ключем в загальній криптографічній стійкості ARX алгоритмів. Так, для всіх варіантів схеми Simon (чотири схеми, що представлені на рис. 3, 4), Alzette і ChaCha потрібно використовувати щонайменше три операції XOR додавання з ключем, щоб, використовуючи вказану у табл. 5, 6 кількість циклів, забезпечити відсутність інтегралів та нездійснених диференціалів. Для інших двох схем – Speckey і Chaskey – достатньо двох таких операцій.

3. Підсумкові дані аналізу наведено в табл. 10, 11 (дані отримані на основі табл. 2, 3, 5, 6, 8, 9). Ці таблиці відображають кількість циклів, кількість XOR додавань з ключем та кількість елементарних ARX перетворень, які потрібні для того, щоб ARX перетворення не відрізнялись від випадкової підстановки. На основі табл. 10, 11 можна виділити найкращі та найгірші ARX перетворення. Кращі 8-бітові схеми: Speckey та Alzette (потребують по 36 ARX операцій). При цьому Speckey потребує меншої кількості XOR додавань з ключем, тому має перевагу. Найгірші показники продемонструвала схема Simon, яка потребує значно більшої кількості операцій – 60. Серед 4-бітних схем (табл. 11) кращою є Chaskey, яка потребує 72 4-бітних операції. Якщо рахувати, що одна 8-бітова операція еквівалентна двом 4-бітовим, то ця схема еквівалентна кращій 8-бітній схемі Speckey.

Список літератури:

1. Руженцев В.І. Порівняльний аналіз ARX схем шифрування // Радіотехніка. 2020. Вип. 202. С. 79 – 86.

2. Victor Ruzhentsev. Comparative analysis of ARX transformations // Book of Abstracts 20th Central European Conference on Cryptology, June 24 – 26, 2020, Zagreb, Croatia. P. 42-43.

3. Daniel J. Bernstein. Chacha, a variant of Salsa20. SASC 2008 –the State of the Art in Stream Ciphers. See also https://cr.yp.to/chacha.html, 2008.

4. R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, and L. Wingers. The SIMON and SPECK families of lightweight block ciphers // Cryptology ePrint Archive, Report 2013/404, 2013. http://eprint.iacr.org/2013/404.

5. Nicky Mouha, Bart Mennink, Anthony Van Herrewege, Dai Watanabe, Bart Preneel, and Ingrid Verbauwhede. Chaskey: An effcient MAC algorithm for 32-bit microcontrollers // Antoine Joux and Amr M. Youssef, editors, SAC 2014: 21st Annual International Workshop on Selected Areas in Cryptography, volume 8781 of Lecture Notes in Computer Science, pages 306–323. Springer, Heidelberg, August 2014. Doi:10.1007/978-3-319-13051-4_19

6. Lightweight cryptography project of the American National Institute of Standards and Technology. https://csrc.nist.gov/projects/lightweight-cryptography.

7. J. Ren, S. Chen. Cryptanalysis of Reduced-Round SPECK. IEEE Xplore. Vol. 7, 2019. P. 63045-63056. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8715440.

Надійшла до редколегії 05.11.2021

Відомості про авторів:

Руженцев Віктор Ігорович – д-р техн. наук, доцент, Харківський національний університет радіоелектроніки, професор кафедри безпеки інформаційних технологій; Україна; e-mail: viktor.ruzhentsev@nure.ua, ORCID: http://orcid.org/0000-0002-1007-6530

Федюшин Олександр Іванович – канд. техн. наук, доцент, Харківський національний університет радіоелектроніки, доцент кафедри безпеки інформаційних технологій; Україна; e-mail: oleksandr.fediushyn@nure.ua, ORCID: http://orcid.org/0000-0002-3600-405X

Кохан Сергій Анатолійович – Харківський національний університет радіоелектроніки, аспірант кафедри безпеки інформаційних технологій; Україна; e-mail: serhii.kokhan@nure.ua

УДК 003.026:004.056 **DOI:10.30837/rt.2021.4.207.07**

Д.В. ГАРМАШ

СИЛЬНІ ТА СЛАБКІ СТОРОНИ АЛГОРИТМУ НА ОСНОВІ БАГАТОВИМІРНИХ ПЕРЕТВОРЕНЬ RAINOW ТА ЙОГО ЗДАТНІСТЬ БЛОКУВАТИ АТАКИ СТОРОННІМИ КАНАЛАМИ

Вступ

Багатовимірні квадратичні схеми є перспективним рішенням для потреби квантових систем, стійких до атак від квантового комп'ютера. Однак, оскільки цей клас відносно молодий і багато схем цього класу були порушені в минулому, існує дуже мало їх реалізацій, особливо на вбудованих мікроконтролерах. Щоб оцінити, чи можуть ці схеми колись замінити чинні стандарти, необхідно знати, наскільки ефективно їх можна впровадити на різних платформах. У процесі цієї роботи дано теоретичне введення до багатовимірних квадратичних схем. Впроваджуються схеми, які певний час витримували атаки: Unbalanced Oil and Vinegar (UOV), Rainbow та enTTS. Особлива увага приділяється виявленню усіх загальних моментів схеми Rainbow.

Основна інформація про Rainbow, як він влаштований

Наразі криптосистеми, що засновані на квадратичних поліномах, пройшли за останні 10 років суттєвий розвиток та визнання. Теоретичною основою конструкцій Oil-Vinegar є доведена теорема, згідно з якою вирішення (визначення) набору багатоваріантних поліноміальних рівнянь над кінцевим полем є експоненційно складною проблемою, хоча це є у загальному випадку як необхідною, так і достатньою умовами [2].

Цей напрямок досліджень пов'язаний з появою конструкції Мацумото та Імаї, в тому числі з використанням рівняння лінеаризації [1]. Далі Патарін та його співробітники доклали великих зусиль для розробки безпечних багатоваріантних криптосистем. Один з конкретних напрямків, яким займались Патарін та його співробітники, пов'язаний з рівняннями лінеаризації Dragon, Oil and Vinegar, Unbalanced Oil-Vinegar [1]. Побудова механізму ЕП Rainbow на основі Oil and Vinegar, Unbalanced Oil-Vinegar грунтується на тому, що певні квадратичні рівняння можна легко розв'язати, якщо є можливість вгадувати декілька варіантів [1].

Нехай k буде кінцевим полем. Ключовою конструкцією є відображення (карта) F від k^{o+v} до k^{o}:

$$F(x_1,...,x_0,x_1^{'},...,x_v^{'}) = F(x_1,...,x_0,x_1^{'},...,x_v^{'}),...,F_0(x_1,...,x_0,x_1^{'},...,x_v^{'}) \quad (1)$$

і кожна F_l у формі

$$F(x_1,...,x_0,x_1^{'},...,x_v^{'}) = \sum a_{l,i,j}x_i x_j + \sum b_{l,i,j}x_i^{'}x_j^{'} + \sum c_{l,i}x_i + \sum d_{l,i}x_j^{'} + c_l, \quad (2)$$

де x_i, $i = 1,...,o$ - це Oil значення та $x_j^{'}$, $j = 1,...,v$ значення Vinegar у кінцевому полі k.

Потрібно звернути увагу на схожість наведеної вище формули з рівняннями лінеаризації. Такий тип поліномів називається "поліномом Oil-Vinegar". Причина, по якій вона називається схема "Oil-Vinegar", пов'язана з тим, що в квадратичному вимірі змінні Oil та Vinegar не змішуються повністю. Це дозволяє легко знайти одне рішення для будь-якого рівняння виду

$$F(x_1,...,x_0,x_1^{'},...,x_v^{'}) = (y_1,...,y_o), \quad (3)$$

коли $(y_1,...,y_o)$ дано. Щоб знайти одне рішення, потрібно лише випадковим чином вибрати значення для Vinegar змінних та підключити їх до рівнянь вище, що дасть набір o лінійних рівнянь з o змінними. Це має, з імовірністю, близькою до 1, дати рішення. Якщо цього не сталося, можна спробувати ще раз, вибравши різні значення для Vinegar змінних, поки не вдасться знайти рішення [4].

Це сімейство криптосистем розроблено спеціально для схем підписів, де потрібно лише знайти одне рішення для даного набору рівнянь, а не унікальне рішення. Застосовуючи відображення (карту F), ми «приховуємо» її, складаючи її з лівої та правої сторін за двома оборотними афінними лінійними відображеннями L_1 та L_2. Оскільки L_1 знаходиться на k^o, а L_2 на k^{o+v}, це генерує квадратичне відображення (карту)

$$F^{-} = L_1 \circ F \circ L_2 \tag{4}$$

від k^{o+v} до k^o.

Збалансована схема Oil-Vinegar характеризується тим, що $o = v$, але її удосконалили Кіпніс та Шамір, використовуючи матриці, що відносяться до білінійних форм, визначених квадратичними поліномами [3].

Для незбалансованої схеми Oil-Vinegar, $v > o$, показано, що конкретна атака має складність приблизно $q^{v-o-1}o^4$, коли $v \approx o$. Це означає, що якщо o не надто велике (менше ніж 100) і дане фіксоване поле розміром q, тоді $v - o$ має бути досить великим, але також не надто великим, щоб забезпечити безпеку схеми.

Однак слід зауважити, що в цій схемі документ, що підписується, є вектором у k^o, а підпис – вектором у k^{o+v}. Це означає, що підпис має принаймні вдвічі більший розмір документа, і при великому $v + o$ система стає менш ефективною.

В рамках статті пропонується конструкція, яка використовує конструкцію Oil-Vinegar кілька разів, так що в підсумку підпис буде лише трохи довшим за документ. Отже, ця схема набагато ефективніша. Її називають схемою Rainbow.

Сильні та слабкі сторони алгоритму

1) Короткі підписи. Підписи, отримані схемою підписів Rainbow, мають розмір, що приблизно вдвічі перевищує відповідний рівень безпеки. Тому Rainbow виробляє одні з найкоротших підписів всіх існуючих схем цифрового підпису (як класичного, так і постквантового).

2) Скромні обчислювальні вимоги. Оскільки Rainbow вимагає простої операції лінійної алгебри над невеликим кінцевим полем, її можна ефективно реалізувати на пристроях з низькою вартістю, без необхідності криптографічного співпроцесору.

3) Простота. Дизайн схем Rainbow надзвичайно простий. Тому схема вимагає лише мінімальних знань з алгебри, щоб зрозуміти і реалізувати її. Ця простота також означає, що існує не так багато структурних схем, які можуть бути використані для атаки на Rainbow. Тому малоймовірно, що існують додаткові структури, які можуть бути використані для атаки схеми, які не були виявлені протягом більше ніж 12 років строгого криптоаналізу.

4) Суттєве випробовування часом. Як вже було зазначено, Rainbow базується на добре відомій UOV схемі, яка була винайдена ще у 1999 році. Саму схему Rainbow було створено у 2005 році, а останній напад, який потребував зміни параметрів, стався у 2008 році. За цей час було створено безліч спроб зламати цю схему, але досі Rainbow залишається однією з найбільш захищених схем підпису.

5) З іншого боку головним недоліком Rainbow є великий розмір публічних та приватних ключів, виправлення якого є важливим в наших дослідженнях [3, 4].

Здатність алгоритму RAINBOW протидіяти атаці сторонніми каналами

Криптографічні системи повинні бути захищені від широкого кола атак, включаючи атаки сторонніми каналами. Атака сторонніми каналами належить до фізичної атаки, яка являє собою будь-яку атаку, засновану на інформації, отриманій в результаті фізичної реалізації криптографічних систем, а не на грубій силі чи теоретичних недоліках криптографічних алгоритмів. Основним принципом атаки бічного каналу є те, що інформація бічного каналу, така як споживання енергії, електромагнітні витоки, інформація про синхронізацію або навіть звук, може забезпечити додаткові джерела інформації про секрети в криптографічних

системах, наприклад криптографічні ключі, часткова інформація про стан, повна або часткові звичайні тексти, які можна використовувати для розбиття криптографічних систем. Загальні класи атаки бічних каналів включають аналіз синхронізації, аналіз потужності, електромагнітний аналіз, аналіз несправностей, акустичний криптоаналіз, аналіз залишків даних та атаки аналізу молоткових рядів [7].

Атаки аналізу несправностей мають на меті маніпулювати екологічними умовами криптографічних систем, таких як напруга, годинник, температура, випромінювання, світло і вихровий струм, щоб генерувати несправності під час секретних обчислень, наприклад множення та інверсії в кінцевому полі, і спостерігати за пов'язаною поведінкою, яка може допомогти криптоаналітику зламати криптографічні системи. Атаки аналізу несправностей можна спроєктувати, просто підсвітивши транзистор лазерним променем, що змушує деякі біти приймати неправильні значення. Ідея використання несправності, індукованої під час секретного обчислення, для вгадування секретного ключа практично спостерігалася в реалізаціях RSA, що використовують китайську теорему про залишки [7].

Атака аналізу потужності може надати детальну інформацію, спостерігаючи за енергоспоживанням криптографічних систем, що приблизно поділяється на простий аналіз потужності (SPA) та аналіз диференціальної потужності (DPA). У сімействі атак аналізу потужності DPA представляє особливий інтерес і є статистичним тестом, який вивчає велику кількість сигналів енергоспоживання для отримання секретних ключів.

Можна виділити наступні атаки:

- атака диференціального аналізу потужності на SFLASH;
- атака на секретні ключі від модуля SHA-1 схем SFLASH.
- атака стороннього каналу на enTTS, яка використовує диференціальний аналіз потужності та аналіз несправностей для атаки двох афінних перетворень та центральної трансформації карти. Цей метод показує, що можна отримати всі секретні ключі enTTS.

Оскільки конструкція Rainbow включає два афінні перетворення та перетворення центральної карти, такі методи мають потенціал для отримання її секретних ключів. Таким чином, обговорюється захист від можливої атаки бічного каналу для Rainbow, а контрзаходи описані нижче:

- Нехай це повідомлення і кожен елемент у полягає в $GF((2^4)^2)$;
- Береться випадковий вектор $y'(y_0', y_1', ..., y_{25}')$, кожен елемент якого полягає в $GF((2^4)^2)$;
- Обчислюється $y'' = y' + y$;
- Обчислюється $\bar{y}' = Ay' + b$ та $\bar{y}'' = Ay''$, де A – матриця 26x26, b – вектор розміру 26;
- Обчислюється $\bar{y} = \bar{y}' + \bar{y}''$, що еквівалентно $\bar{y} = Ay + b$;
- Розраховано перше афінне перетворення; тоді ми беремо випадкові байти для Vinegar-змінних;
- Двічі перевіряються випадкові байти для захисту від атак аналізу несправностей;
- Обчислюються багатовимірні поліноміальні оцінки та розв'язування систем лінійних рівнянь до завершення перетворення центральної карти;
- $\bar{x}(\bar{x}_0, \bar{x}_1, ..., \bar{x}_{42})$ – це результат трансформації центральної карти; після цього береться два випадкових вектори $\bar{x}'$ та $\bar{x}''$, де $\bar{x} = \bar{x}' + \bar{x}''$, та елементи полягають в $GF((2^4)^2)$;
- Обчислюється $\bar{x}' = C\bar{x}'$ та $\bar{x}'' = C\bar{x}'' + d$, де C – матриця 43x43, b – вектор розміру 43;
- Обчислюється $\bar{x} = \bar{x}' + \bar{x}''$, що еквівалентно $x = Cx + d$;
- $x(x_0, x_1, ..., x_{42})$ це схема підпису Rainbow для $y(y_0, y_1, ..., y_{25})$.

Використовується аналіз несправностей для атаки випадкових байтів у центральних перетвореннях карти; таким чином ми двічі перевіряємо випадкові байти для захисту від атак аналізу несправностей. Також використовується аналіз диференціальної потужності для атаки модуля SHA-1; таким чином, ми беремо метод захисту афінних перетворень. Однак

зазначений вище контрзахід є теоретичним; потрібна можливість впровадити та перевірити це на апаратному забезпеченні [8].

Висновки

1. Постквантова криптографія – частина криптографії, яка залишається актуальною і при появі квантових комп'ютерів і квантових атак. Так як за швидкістю обчислення традиційних криптографічних алгоритмів квантові комп'ютери значно перевершують класичні комп'ютерні архітектури, сучасні криптографічні системи стають потенційно вразливими до криптографічних атак. Більшість традиційних криптосистем спирається на проблеми факторизації цілих чисел або завдання дискретного логарифмування, які будуть легко розв'язані на досить великих квантових комп'ютерах, що використовують алгоритм Шора.

2. Багато криптографів ведуть розробку алгоритмів, незалежних від квантових обчислень, тобто стійких до квантових атак. Ці задачі розглянуто на другому етапі конкурсу NIST США.

3. Схема підпису Rainbow виглядає надійною проти великої кількості методів криптоаналізу та проти атак сторонніми каналами.

4. У зв'язку з можливістю появи потужного квантового комп'ютера актуальними є завдання створення постквантових алгоритмів ЕП. В цьому напрямі уже розпочато дослідження, в певній мірі визначено математичні основи, на яких можуть бути побудовані постквантові алгоритми ЕП. Для цього можна застосувати схему Rainbow.

5. Реалізація квантово-захищених алгоритмів вимагає великих матеріально-технічних ресурсів. Вказане пов'язане з великими довжинами ключів та загальних параметрів. Сучасний рівень розвитку техніки дозволяє оптимістично ставитися до можливості ефективної реалізації квантово-захищених алгоритмів.

6. Мультиваріативні квадратичні перетворення можуть бути застосованими для розроблення постквантового стандарту ЕП. Вони вже були використані для побудови схем підпису, але всі спроби побудувати надійну схему поки не були успішними. Попередній аналіз показав, що мультиваріативні квадратичні перетворення можуть вирішити проблему захищеності від атак на основі квантових комп'ютерів, але для цього ще потрібно провести величезний обсяг досліджень та робіт, а також вкласти значні ресурси.

7. Попередній аналіз показує, що розміри загальних параметрів та ключів не викликають сумнівів відносно криптографічної стійкості стандарту, розробленого на основі мультиваріативного квадратичного перетворення. Але залишається проблема просторової складності, яка пов'язана зі значними довжинами загальних параметрів та відкритих ключів.

Список літератури:

1. Lili Chen, Stephen Jordan, Yi-Kai-Liu, Dustin Moody, Rene Peralta, Ray Perlner, Daniel Smith-Tone. Report on Post – Quatum Cryptography. Nistir 8105 (draft).

2. Інтернет-ресурс. Режим доступу http://www.nkj.ru/archive/articles/5309/

3. Горбенко Ю.І. Методи побудування та аналізу, стандартизація та застосування криптографічних систем : монографія ; заг. ред. І.Д. Горбенко. Харків : Форт, 2015. 959 с

4. Потій О.В, Горбенко Ю.І., Ганзя Р.С., Пономар В.І. // Матеріали V-ї міжнар. наук.-техн. конф. «Захист інформації і безпеки інформаційних систем». Львів, 2016, 02.06 – 03.06. С. 52.

5. Reinier Broker. Constructing supersingular elliptic curves // J. Comb. Number Theory, (3): pp. 269–273, 2009.

6. McGrew D., Curcio M. Hash-Based Signatures draft-mcgrew-hash-sigs00[Електронний ресурс] / D. McGrew, M. Curcio. Режим доступу: https://tools.ietf.org/html/draftmcgrew-hash-sigs-00.

7. Lili Chen, Stephen Jordan, Yi-Kai-Liu, Dustin Moody, Rene Peralta, Ray Perlner, Daniel Smith-Tone. Report on Post – Quantum Cryptography. NISTIR 8105 (DRAFT). https://www.google.com.ua/search?

8. Bernstein D. J. Grover vs. McEliece // N. Sendrier, editor, Post-Quantum Cryptography, Third International Workshop, PQCrypto 2010, Darmstadt, Germany, May 25-28, 2010. Proceedings, volume 6061 of Lecture Notes in Computer Science, pages 73–80. Springer, 2010.

Надійшла до редколегії 07.11.2021

Відомості про авторів:

Гармаш Дмитро Васильович – Харківський національний університет імені В. Н. Каразіна, аспірант кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук; Україна; e-mail: dmytro.harmash96@icloud.com

УДК 004.7:517.9 **DOI:10.30837/rt.2021.4.207.08**

Є. В. КОТУХ, канд. техн. наук, В. О. ЛЮБЧАК, канд. фіз.-мат. наук,
О. П. СТРАХ, канд. фіз.-мат. наук

ОДИН ПІДХІД ДО ПОБУДОВИ ІНДИВІДУАЛЬНИХ МАТЕМАТИЧНИХ МОДЕЛЕЙ ЗАХИСТУ У БЕЗДРОТОВИХ СЕНСОРНИХ МЕРЕЖАХ

Вступ

Бездротова сенсорна мережа (БСМ) – це група «розумних» датчиків з інфраструктурою бездротового зв'язку, призначеною для моніторингу умов навколишнього середовища. Ця технологія є базовим поняттям Інтернету речей (IoT). БСМ можуть передавати конфіденційну інформацію, працюючи у незахищеному середовищі. Через це в проєктуванні мережі потрібно враховувати відповідні заходи безпеки. Однак обчислювальні обмеження вузлів, обмежений простір для зберігання даних, нестійке джерело живлення, ненадійний канал зв'язку та операції без нагляду є значними перешкодами для застосування технічних методів кібербезпеки у цих мережах.

Існують математичні моделі щодо вивчення поширення шкідливого програмного забезпечення (ПЗ) у БСМ, які можуть бути глобальними (ураховують топологію зв'язку між вузлами БСМ, але не враховують їх індивідуальних характеристик) [1 – 8], або індивідуальними (ураховують індивідуальні особливості вузлів, але не враховують глобальний характер їх взаємодії) [9 – 15] моделями. Крім того, існуючі моделі можна класифікувати за типами взаємодії (неперервні [3 – 5] та дискретні [1, 2, 6 – 8, 9 – 15], детерміновані [1, 3 – 5, 7, 10 – 14] та стохастичні [2, 6, 8, 9, 15] тощо) та використанням математичного апарату (системи диференціальних рівнянь у частинних похідних (СДРЧП) [3, 4, 8], системи звичайних диференціальних рівнянь (СЗДР) [1, 5, 7], клітинні автомати (КА) [9, 10, 12], ланцюги Маркова (ЛМ) [2, 6, 11], агентне моделювання [13 – 15] тощо). Існуючі моделі мають певну специфіку та можливості щодо застосування їх до побудови стратегії захисту БСМ від шкідливого програмного забезпечення. Але також вони мають певні недоліки. Зокрема, ураховуючи особливості отримання даних щодо стану тієї чи іншої групи вузлів БСМ, цей процес не можна розглядати у суто неперервному або суто дискретному за часом режимі. Ці два фактори мають бути поєднані.

У статті розглянуто нову неперервно-дискретну модель поширення шкідливого ПЗ через вузли бездротової сенсорної мережі, яка базується на системі так званих динамічних рівнянь з імпульсним впливом на часовій шкалі.

Опис моделі

Розглянемо деяку бездротову сенсорну мережу. Її неперервне функціонування можна спостерігати лише на деяких інтервалах часу; на інших же інтервалах можливості спостереження обмежуються окремими точковими передачами відповідної інформації. Тож для побудови моделі виникає необхідність використовувати математичні об'єкти на неперервно-дискретних проміжках часу. Однією з теорій, яка дозволяє це зробити, є теорія динамічних рівнянь на часових шкалах [16]. Ключовими поняттями цієї теорії, необхідними нам у подальшому, є часова шкала ($\mathbb{T}$) – довільна замкнена непорожня підмножина множини дійсних чисел, оператор стрибка вперед $\sigma(t) := \inf\{\forall s \in \mathbb{T} : s > t\}$, дельта похідна ($x^{\Delta}$), яка є узагальненням понять звичайної похідної та різницевого оператора, а також матрична експоненціальна функція $e_A(t,s)$ [16].

Нехай досліджувана БСМ має певні топологічні характеристики і кожен її вузол перебуває в одному з класів:

1) сприйнятливому *S*, де датчики не заражені шкідливим ПЗ, але мають сприйнятливі до такого ПЗ індивідуальні обчислювальні характеристики;

2) виявленому *E*, через датчики якого пройшло шкідливе ПЗ, але вони не можуть передати його на суміжні датчики через індивідуальні характеристики останніх та особливості самого отриманого ПЗ, а також їх власні характеристики;

3) зараженому *I*, датчики якого заражені шкідливим ПЗ та мають можливість робити спроби зараження інших;

4) відновленому *R*, датчики якого набувають тимчасового імунітету, після успішного видалення шкідливого ПЗ, чи встановлення виправлень безпеки;

5) віджилому *D*, в якому датчики не підлягають відновленню (наприклад, їх потужність швидко вичерпалася, коли вони були заражені шкідливим ПЗ; або через фізичні пошкодження, не пов'язані з ПЗ, не можуть працювати тощо).

На індивідуальні особливості, через які кожний вузол БСМ перебуває у тому чи іншому класі, впливають різні чинники, зокрема такі фактори, які не пов'язані з особливостями шкідливого програмного забезпечення: тип сенсорного вузла, його обчислювальна потужність, рівень споживання енергії, можливість передачі та прийому інформації, метод збору даних, протоколи маршрутизації тощо.

Для побудови моделі функціонування мережі визначимо деякий вектор $x(t) = col(x_1, x_2, x_3, x_4, x_5)$ – вектор кількісних значень вузлів мережі кожного із наведених вище п'яти класів (*S, E, I, R, D*) у кожний момент часу t спостереження. То, якщо розглядати функціонування вузлів мережі без можливих вторгнень, моделлю мережі буде деяка система динамічних рівнянь на часовій шкалі виду

$$x^{\Delta} = A(t)x + f(t), \tag{1}$$

де $x(t) \in C^1_{rd}(\mathbb{T}_{(t_0)}; \mathbb{R}^5)$ – 5-вимірний вектор-стовпчик *rd*-неперервних, Δ-диференційованих [16] функцій, $\mathbb{T}_{(t_0)} := [t_0; \infty)_{\mathbb{T}} = [t_0; \infty) \cap \mathbb{T}$; $A(t)$ – (5×5)-вимірна матриця, компоненти якої є *rd*-неперервними функціями; $f(t) \in C_{rd}(\mathbb{T}_{(t_0)}; \mathbb{R}^5)$ – *rd*-неперервна вектор-функція. У цій моделі значення t_0 визначає початковий момент часу спостереження, а компоненти $A(t)$ та $f(t)$ – характеристики детермінованого зв'язку між п'ятьма класами вузлів всієї бездротової сенсорної мережі. Крім того, певні індивідуальні особливості вузлів (зокрема, їх робочий цикл, людський фактор обслуговування тощо) у деякі моменти часу дають можливість визначати кількісні параметри самої мережі, які математично можна описати як деякі крайові умови у системі (1). Зокрема, у ці умови буде входити початкова умова щодо наявної кількості вузлів у початковий момент часу t_0:

$$x_1(t_0) + x_2(t_0) + x_3(t_0) + x_4(t_0) + x_5(t_0) = n.$$

Всі такі умови можна відобразити за допомогою лінійного векторного функціонала $\ell : \mathbb{R}^5 \to \mathbb{R}^m$, де m – загальна кількість умов. Тож, з урахуванням системи (1) матимемо крайову задачу:

$$\begin{gathered} x^{\Delta} = A(t)x + f(t), \\ \ell x = \alpha, \end{gathered} \tag{2}$$

де $\alpha \in \mathbb{R}^m$ – m-вимірна вектор-константа. Оскільки ж умова $m = 5$ не передбачається, то крайова задача (1), (2) є нетеровою. Необхідні та достатні умови розв'язання таких задач за допомогою методу псевдообернених матриць [17] були отримані в роботі [18].

Врахуємо тепер, що під впливом шкідливого ПЗ у визначені моменти часу t_k $(k = 1, 2, \ldots)$ відбувається зміна параметрів БСМ, яка не споріднена з її природним функціонуванням. Фактори цих змін можуть бути пов'язані, наприклад, із самим типом шкідливого ПЗ, механі-

змом його розповсюдження чи ціллю поширення шкідливого коду. Тоді такі моменти часу $t_k\ (k=1,2,\ldots,p)$ у запропонованій моделі будуть визначати наявність відповідної імпульсної дії:

$$x(t_k+0)=B_k x(t_k)+a_k,\quad k=1,2,\ldots,p. \tag{3}$$

Умови існування розв'язків нетерової крайової задачі, яка складається з лінійної неоднорідної динамічної системи (1), крайової умови (2) та імпульсної дії (3), були отримані в роботі [19] у вигляді такого результату.

Теорема. *Якщо* $A(t)\in C_{rd}(\mathbb{T}_{(t_0)};\mathbb{R}^{5\times 5})$, $B_k\in M_5(\mathbb{R})$, $k=\overline{1,p}$, *то неоднорідна крайова задача* (1), (2), (3) *є розв'язною тоді й тільки тоді, коли неоднорідності* $f(t)\in C_{\mathrm{rd}}\left([a;b]_{\mathbb{T}_+}/\{t_k\};\mathbb{R}^5\right)$, $a_k\in\mathbb{R}^5$, $\forall k=\overline{1,p}$ *та* $\alpha\in\mathbb{R}^m$ *задовольняють умови*

$$P_{Q_d^*}(\alpha-\ell F(\cdot))=\theta_d, \tag{4}$$

де $P_{Q_d^*}$ *–* $(d\times m)$*-вимірна матриця, що складається з* $d:=m-\operatorname{rank}Q$ *лінійно незалежних рядків матриці* $(m\times m)$*-вимірної матриці-проєктора* $P_{Q^*}:\mathbb{R}^m\to N(Q^*)$, $P_{Q^*}:=I_m-QQ^+$, Q^+ *–* $(5\times m)$*-вимірна матриця, що є єдиною псевдооберненою за Муром – Пенроузом* [17] *до матриці* $Q=\ell S_A(\cdot,t_0)$ *– сталої* $(m\times 5)$*-вимірної матриці,* $S_A(t,s)$ *– асоційована з послідовністю* $\{B_k,t_k\}_{k=1}^p$ *та нормована в точці* t_0 *матриця імпульсних переходів, яка має вигляд*:

$$S_A(t,s)=\begin{cases} e_A(t,s), & t_{k-1}\le s\le t\le t_k;\\ e_A(t,t_k+0)(I+B_k)e_A(t_k,s), & t_{k-1}\le s\le t_k<t<t_{k+1};\\ e_A(t,t_k+0)\prod\limits_{s<t_j\le t}\left[(I+B_j)e_A(t_j,t_{j-1}+0)\right]\left(I+B_i\right)e_A(t_i,s), & t_{i-1}\le s<t_i<\ldots<t_k<t<t_{k+1}, \end{cases}$$

$F(t)=\int\limits_{t_0}^{t}S_A(t,\sigma(s))f(s)\Delta s+\sum\limits_{a<t_j<t}S_A(t,t_j+0)a_j$. *Лише для тих і тільки тих неоднорідностей* f, a_k, α, *для яких виконується умова* (4), *задача* (1), (2), (3) *матиме* r*-параметричну* $(r:=5-\operatorname{rank}Q)$ *сім'ю лінійно незалежних розв'язків виду*

$$x(t;c_r)=S_A(t,t_0)P_{Q_r}c_r+G\left(\begin{bmatrix} f\\ a_k\\ \alpha\end{bmatrix}\right)(t),\quad c_r\in\mathbb{R}^r, \tag{5}$$

де P_{Q_r} *–* $(5\times r)$*-вимірна матриця, що складається з* r *лінійно незалежних стовпців* (5×5)*-вимірної матриці-проєктора* $P_Q:\mathbb{R}^5\to N(Q)$, $P_Q:=I_5-Q^+Q$,

$G\left(\begin{bmatrix} f\\ a_k\\ \alpha\end{bmatrix}\right)(t):=F(t)+S_A(t,t_0)Q^+\left\{\alpha-\ell\int\limits_{t_0}^{\cdot}S_A(\cdot,\sigma(s))f(s)\Delta s-\ell\sum\limits_{a<t_j<\cdot}S_A(\cdot,t_j+0)a_j\right\}$ *– узагальнений оператор Гріна неоднорідної крайової задачі* (1), (2), (3).

Тож, фактично маючи відповідні чисельні значення неоднорідностей, які, очевидно, отримуються з відповідних умов зв'язності класів вузлів, їх індивідуальних характеристик та особливостей дії шкідливого програмного забезпечення, можна змоделювати функціонуван-

ня всієї бездротової сенсорної мережі у вигляді крайової задачі для імпульсної динамічної системи на часовій шкалі виду

$$x^{\Delta} = A(t)x + f(t),\ t \in \mathbb{T}_{(t_0)}$$
$$x(t_k + 0) = B_k x(t_k) + a_k, \quad k = 1, 2, \ldots, p,$$
$$\ell x = \alpha,$$

яка за виконання визначених умов (4) дає прогнозовані наслідки у вигляді розв'язків (5).

Для запобігання небажаних наслідків через поширення шкідливого ПЗ, використовуючи запропоновану модель, маємо різні можливості, зокрема коригування умов, які впливають на параметри неоднорідностей f, a_k та α.

Висновки

Сучасний рівень розвитку техніки та технологій характеризується постійним розширенням різноманіття й складності механічних та керованих об'єктів, функціонування яких відбувається в неперервно-дискретному за часом режимі. Одним із таких об'єктів є процес поширення шкідливого програмного забезпечення у бездротових сенсорних мережах, постійне зростання тенденцій до яких обумовлене їх використанням як єдиного виду самоорганізованої мережі передачі даних з найменшою трудомісткістю та маловитратністю.

Слід зазначити, що попри тривалу історію сенсорних мереж, концепція їх побудови остаточно не сформувалася. Тож вивчення певних властивостей таких мереж є дуже важливим як для вітчизняної, так і для світової науки. Більш того, для стратегічно важливих галузей країни, зокрема оборонної, захист бездротових сенсорних мереж є дуже важливою складовою.

Запропоновано нову модель поширення шкідливого програмного забезпечення, яка описується деякою крайовою задачею для імпульсної динамічної системи на часовій шкалі.

Список літератури:

1. Liu B. Malware propagations in wireless ad hoc networks / B. Liu, W. Zhou, L. Gao, H. Zhou, T. H. Luan, S. Wen // IEEE Trans. Dependable Secur. Comput. 2018. Vol. 15. P. 1016–1026.
2. Wu X. Nodes availability analysis of NB-IoT based heterogeneous wireless sensor networks under malware infection / X. Wu, Q. Cao, J. Jin, Y. Li, H. Zhang // Wirel. Commun. Mob. Comput. 2019. Vol. 2019.
3. Queiruga-Dios A., Encinas A. H., Martín-Vaquero J., Encinas L. H. Malware propagation models in wireless sensor networks: a review, 2016 // International Joint Conference «SOCO'16-CISIS'16-ICEUTE'16». 2017. Vol. 527. P. 648–657.
4. Zhu L., Zhao H., Wang X. Stability and bifurcation analysis in a delayed reaction-diffusion malware propagation model // Comput. Math. Appl. 2015. Vol. 69. P. 852–875.
5. Feng L. Modeling and stability analysis of worm propagation in wireless sensor network / L. Feng, L. Song, Q. Zhao, H. Wang // Math. Probl. Eng. 2015. Vol. 2015. P. 1–8.
6. Shen S. A non-cooperative non-zero-sum game-based dependability assessment of heterogeneous WSNs with malware diffusion / S. Shen, H. Ma, E. Fan, K. Hu, S. Yu, J. Liu, Q. Cao // J. Netw. Comput. Appl. 2017. Vol. 91. P. 26–35.
7. Acarali D. Modelling the spread of botnet malware in IoT-based wireless sensor networks / D. Acarali, M. Rajarajan, N. Komninos, B. B. Zarpelão // Secur. Commun. Netw. 2019. Vol. 2019. https://doi.org/10.1155/2019/3745619.
8. Shen S. SNIRD: disclosing rules of malware spread in heterogeneous wireless sensor networks / S. Shen, H. Zhou, S. Feng, J. Liu, Q. Cao // IEEE Access. 2019. Vol. 7. P. 92881–92892.
9. Wang Y., Li D., Dong N. Cellular automata malware propagation model for WSN based on multi-player evolutionary game // IET Netw. 2018. Vol. 7. P. 129–135.
10. A. M. del Rey, J. H. Guillén, G. R. Sánchez. Modeling malware propagation in wireless sensor networks with individual-based models // Conference of the Spanish Association for Artificial Intelligence. Springer. Cham. Switzerland. 2016. P. 194–203.
11. Wang T. Propagation modeling and defending of a mobile sensor worm in wireless sensor and actuator networks / T. Wang, Q. Wu, S. Wen, Y. Cai, H. Tian, Y. Chen, B. Wang // Sensors. 2017. Vol. 17(1). P. 139.
12. Batista F. K. , Á. M. del Rey, Quintero-Bonilla S. , Queiruga-Dios A. A SEIR model for computer virus spreading based on cellular automata, 2017 // International Joint Conference «SOCO'17-CISIS'17-ICEUTE'17». 2018. Vol. 649. P. 641–650.

13.Bose A., Shin K. G. Agent-based modeling of malware dynamics in heterogeneous environments // Secur. Commun. Netw. 2013. Vol. 6. P. 1576–1589.

14.Hosseini S., Azgomi M. A., Rahmani A. Agent-based simulation of the dynamics of malware propagation in scale-free networks // Simulation. 2016. Vol. 92. P. 709–722. https://doi.org/10.1177/0037549716656060

15.Batista F. K., del Rey A. M., Queiruga-Dios A. A new individual-based model to simulate malware propagation in wireless sensor networks // Sensors. 2020. Vol 8 (3). P. 410. https://doi.org/10.3390/math8030410.

16.Bohner M., Peterson A. Dynamic equations on time scales. An introduction with applications. MA. Boston : Birkhauser Boston Inc, 2001.

17.Boichuk A. A., Samoilenko A. M. Generalized inverse operators and fredholm boundary-value problems. Netherlands. Utrecht: Koninklijke Brill NV. 2004.

18.Agarwal R. Fredholm boundary value problems for perturbed systems of dynamic equations on time scales / R. Agarwal, M. Bohner, A. Boˇichuk, O. Strakh // Mathematical Methods in the Applied Sciences. 2014. https://doi.org/10.1002/mma.3356.

19.Strakh O. P. Linear noetherian boundary-value problems for impulsive dynamic systems on a time scale // Journal of Mathematical Sciences. 2014. Vol. 201 (3). P. 400–406. https://doi.org/10.1007/s10958-014-1999-4.

Надійшла до редколегії 01.10.2021

Відомості про авторів:

Котух Євген Володимирович – канд. техн. наук, доцент, доцент кафедри кібербезпеки, Сумський державний університет, Україна, e-mail: yevgenkotukh@gmail.com; ORCID 0000-0003-4997-620X; Google Scholar: https://scholar.google.com/citations?user=5BH3EG4AAAAJ

Любчак Володимир Олександрович – канд. фіз.-мат. наук., доцент, завідувач кафедри кібербезпеки, Сумський державний університет, Україна, e-mail: v.liubchak@dcs.sumdu.edu.ua; ORCID 0000-0002-7335-6716

Страх Олександр Петрович – канд. фіз.-мат. наук, старший викладач кафедри кібербезпеки, Сумський державний університет, Україна, e-mail: o.strakh@dcs.sumdu.edu.ua; ORCID 0000-0002-7680-5716

РАДІОЛОКАЦІЯ І РАДІОНАВІГАЦІЯ
РАДИОЛОКАЦИЯ И РАДИОНАВИГАЦИЯ
RADIOLOCATION AND RADIONAVIGATION

УДК 004.89: 621.396 **DOI:10.30837/rt.2021.4.207.09**

В.В. ЖИРНОВ, канд. техн. наук, С.В. СОЛОНСКАЯ, канд. техн. наук,
И.Ю. ШУБИН, канд. техн. наук

ОЦЕНКА ЭФФЕКТИВНОСТИ ОБРАБОТКИ РАДИОЛОКАЦИОННЫХ ИЗОБРАЖЕНИЙ НА ОСНОВЕ ИНТЕЛЛЕКТУАЛЬНОГО АНАЛИЗА ПРОЦЕССОВ

Введение

Приводятся результаты разработки метода, создания программ и экспериментальных исследований системы автоматического обнаружения радиолокационных отметок воздушных объектов и их распознавания с обработкою реальных записей в обзорных РЛС. Актуальность этих работ – создание универсальных алгоритмов автоматической обработки информации для обеспечения эффективного обнаружения полезных сигналов за счет накопления как сигнальной (энергетической), так и смысловой информации в анализируемой ячейке и в ее окрестности в сложных условиях малых сигналов.

Существующие методы автоматизации обнаружения радиолокационных отметок воздушных объектов и их распознавания [1, 2] не учитывают смысловую сторону процессов и не позволяют создавать эффективные системы автоматической обработки радиолокационных сигналов. Поэтому перспективно создание и использование символьной модели отметок сигналов, включающей в себя образ изучаемого объекта и семантическую составляющую процесса обработки радиолокационных сигналов.

В известных радиолокационных информационных системах [1, 2] анализируются межпериодные изменения сигнальной обстановки, но ограничиваются созданием геометрического образа. Если объект точечный и подвижный, то формируется образ из пачки принятых элементарных отраженных сигналов в виде протяженной по азимуту отметки. Если же объект протяженный, например, облака, дождевые тучи, стаи птиц, локальные воздушные неоднородности «ангел-эхо» и т.д., то из принятых сигналов формируется образ этого объекта. Известны также операции в интеллектуальных информационных системах (ИИС), где используются алгоритмы анализа процессных знаний, в основе которых лежит модель действий человека-оператора и которые связаны с возможностью параллельного восприятия информации с последующим принятием решения по анализу признаков [3 – 6]. Эффективным средством математического описания смысловой информации является алгебра конечных предикатов и предикатных операций.

Задачи обнаружения и распознавания радиолокационных объектов [2, 5] характеризуются высоким уровнем априорной неопределенности. Это та предварительно известная информация, которая должна использоваться при обнаружении и распознавании радиолокационных объектов. Пути преодоления трудностей решения этих задач сходны и достаточно сложны. Есть отличия между способами обнаружения и распознавания объектов.

Символьная модель отметок воздушных объектов с учетом ее образной и семантической составляющих

Предикатные признаки символьной модели отметок воздушных объектов – это математическое описание процедур и отношений при восприятии и анализе сигналов оператором в виде различительных признаков или свойств. В нашем случае это система элементарных или первоначальных (унарных и бинарных) предикатных признаков, а также математическое описание предикатных признаков символьных моделей отметок точечных и протяженных воздушных объектов.

В ходе исследований использовались экспериментальные данные (рис. 1), полученные при записи отраженных сигналов обзорной РЛС сантиметрового диапазона (длительность импульса 1 мкс, частота зондирования 365 Гц). На рисунке приведены распределения амплитуд изображений радиолокационных отметок в матрице размером 129×129 реальных записей сигналов РЛС. В разработанную модель входят процедуры формализации и анализа геометрического сигнального образа отметки от наблюдаемых воздушных объектов на основе алгебры предикатов [7 – 10] и операции создания предикатной модели семантической составляющей для распознавания наблюдаемых объектов локации.

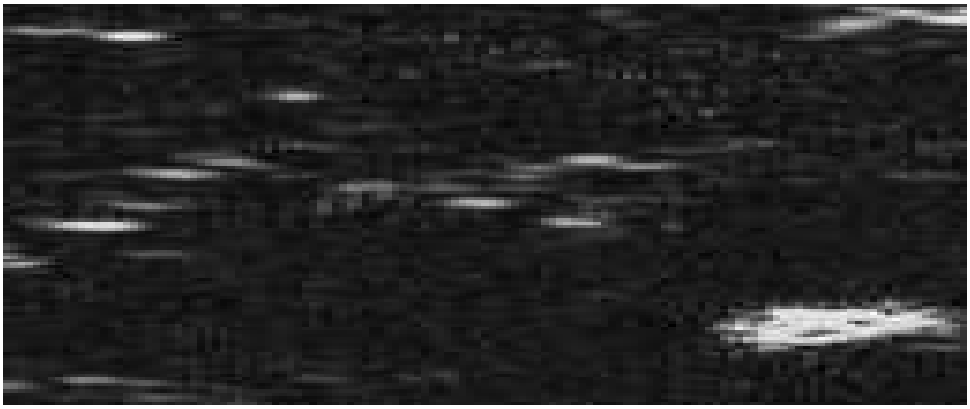


Рис. 1. Распределение амплитуд изображений РЛ отметок в матрице размером 129×129 реальных записей сигналов РЛС сантиметрового диапазона

Пусть $M = \{q_{11}, q_{12}, ..., q_{ij}, ..., q_{mn}\}$ – множество, представляющее собой прямоугольную матрицу $\|A\|$ размерностью $M \times N$, состоящее из элементов $k = m \times n$ – значений амплитуд сигналов в элементах обработки зоны обзора РЛС, а B – некоторое из его подмножеств $B \subseteq M$, амплитуды сигналов которого q_{ij} превышают пороговые значения V_{ij}. Составляем набор логических элементов t_{ij} по следующему принципу: если $q_{ij} \in B$, то $t_{ij} = 1$; если $q_{ij} \notin B$, то $t_{ij} = 0$, $i = \overline{1,m}$, $j = \overline{1,n}$. B элементов обработки, превысивших порог, с характеристикой $(t_{11}, t_{12}, \cdots, t_{ij}, \cdots, t_{mn})$, запишется формулой $A(x) = t_{11}x^{q_{11}} \vee ... \vee t_{mn}x^{q_{mn}} = \bigvee\limits_{i=1,\,j=1}^{mn} t_{ij}x^{q_{ij}}$. Здесь выражение $x^{q_{ij}}$ – форма узнавания события. Когда $x = q_{ij}$, то $x^{q_{ij}} = 1$.

Предикатные признаки символьной модели отметок воздушных объектов

Элементарные предикатные признаки символьной модели отметок воздушных объектов и их распознавания в общем виде – это система n унарных и бинарных предикатов Z_j. Для радиолокационных систем обзора пространства это могут быть: унарный предикат Z_{pij} наличия сигнала в a_{ij} информационной ячейке и бинарные предикаты $Z_{d\,ij}$, $Z_{a\,ij}$ ухода сигнала в соседние по дальности и по азимуту ячейки [7 – 10].

При таких исходных условиях эти предикатные признаки формируются по правилам:

$$Z_{p\,ij} = 1, \text{ при } A_{ij} > 0, \tag{1}$$

$$Z_{d\,ij} = 1, \text{ при } A_{i-1\,j} > 0 \wedge \mathrm{Z}_{p\,ij} = 1, \tag{2}$$

$$Z_{a\,ij} = 1, \text{ при } \mathrm{Z}_{p\,ij} = 1 \wedge A_{ij-1} > 0. \tag{3}$$

Далее получены предикатные признаки символьной модели отметок точечных и протяженных воздушных объектов как совокупности предикатных признаков наличия и ухода сигнала в соседние по азимуту и по дальности ячейки. Это процесс формирования

предикатного признака отметки точечного объекта как совокупности предикатных признаков $Z_{a\,ij}$ соседней за l_n ячейки (n – количество сигнальных импульсов в пачке; l_1 и l_n – номера начала и конца пачки) зондирований РЛС, имеющего процедурный характер отношений и позволяющего получить информацию о пачке отраженных сигналов от точечного подвижного объекта.

Если имеется предикатный признак Z_{aij+l_1} соседней по азимуту ячейки, то на следующем шаге обработки проверяется наличие предикатного признака Z_{aij+l_2} в информационной ячейке a_{ij+l_2}.

$$Z_{aij+l_2} = (A_{ij} > 0 \wedge Z_{p\,i+l_2\,j} = 1) = 1 \tag{4}$$

Решая уравнение (4), находим значения l_2 и составляем предикатное уравнение

$$Z_{aij+l_2+1} = (A_{ij+l_2} > 0 \wedge Z_{p\,ij+l_2+1} = 1) = 1 \tag{5}$$

На n-м шаге предикатное уравнение имеет вид

$$Z_{aij+l_n} = (A_{ij+l_{n-1}} > 0 \wedge Z_{p\,ij+l_n} = 1) = 1 \tag{6}$$

В результате решения системы n предикатных уравнений (4) – (6) определяются все значения $l_1 \cdots l_n$ и символьная модель отметки точечного воздушного объекта в виде предикатного уравнения

$$Z_{mij} = \overset{l_n}{\underset{l_1}{\wedge}} Z_{ai,\,j+l_n} = Z_{ai,\,j+l_1} \wedge Z_{ai,\,j+l_2} \wedge Z_{ai,\,j+l_{n-1}} \wedge Z_{ai,\,j+l_n} = \overset{l_n}{\underset{l_1}{\wedge}} Z_{ai,\,j+l_n} \tag{7}$$

Виды символьных изображений радиолокационных отметок для точечных и воздушных объектов, полученные в результате модельных экспериментов, приведены на рис. 2.

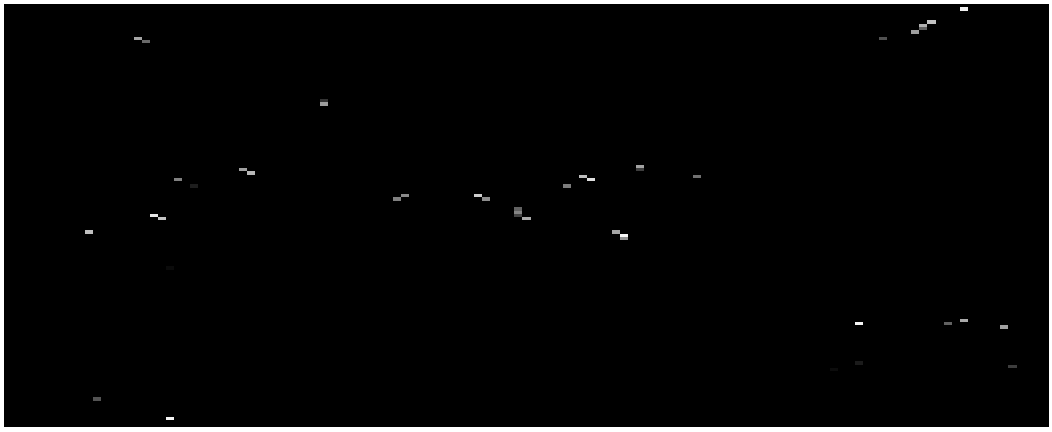


Рис. 2. Виды символьных изображений отметок

Для оценки энергетического признака символьной модели отметки введено понятие накопленной энергии пачки [7] как суммы амплитуд ячеек пачки в направлении, определяемом вектором (l_n) согласно предикатному уравнению (7). С учетом распределения амплитуд

в пределах пачки (l_n) и, используя данные о форме, определяем энергетический признак пачки сигналов (отметок) подвижных воздушных объектов как суммарную амплитуду:

$$I_{m2}=\sum_{l_1}^{l_n} q_{i,j+l_n} Z_{ai,j+l_n}. \quad (8)$$

По виду предикатного признака символьной модели отметки (7), найденного из системы предикатных уравнений (4) – (6), и по энергетическому признаку этой пачки, определенному как суммарная амплитуда в виде (8), осуществляется процедура распознавания отметок точечных воздушных объектов.

Если имеется предикатный признак $Z_{d\,i+k_1 j}$ соседней ячейки по дальности, то в следующем шаге обработки проверяется наличие предикатного признака $Z_{d\,i+k_2 j}$ в информационной ячейке $a_{i+k_2 j}$.

$$Z_{d\,i+k_2 j}=(A_{ij}>0\wedge Z_{p\,i+k_2 j}=1)=1 \quad (9)$$

Решая уравнения (12), найдем значения k_2 и составим предикатное уравнение:

$$Z_{d\,i+k_2+1 j}=(A_{i+k_2 j}>0\wedge Z_{p\,i+k_2+1 j}=1)=1 \quad (10)$$

На *n*-м шаге предикатное уравнение имеет вид

$$Z_{d\,i+k_n j}=(A_{i+k_{n-1} j}>0\wedge Z_{p\,i+k_n j}=1)=1 \quad (11)$$

В результате решения системы *n* предикатных уравнений (9) – (11) находим все значения $k_1\cdots k_n$ и запишем формулу столбца символьной модели протяженного объекта в виде предикатного уравнения:

$$Z_{cdij}=\bigwedge_{k_1}^{k_n} Z_{di+k_n,j}=Z_{di+k_1,j}\wedge Z_{di+k_2,j}\wedge Z_{di+(k_n-1),j}\wedge Z_{di+k_n,j}=1 \quad (12)$$

Если одновременно формируются бинарные предикаты $Z_{d\,ij}$ и $Z_{a\,ij}$. Это означает, что сигнал в исследуемую ячейку переходит и из соседней по дальности $a_{i-1\,j}$ ячейки и из соседней по азимуту a_{ij-1} ячейки. При этом начинает формироваться предикатный признак Z_{bij} символьной модели сигнальных отметок для протяженных воздушных объектов. В этом случае в следующем шаге обработки проверяется наличие столбца символьной модели протяженного объекта Z_{cdij} в информационной ячейке $a_{i+k_2,\,j+l_2}$ следующего по номеру $j+l_2$ зондирования РЛС [10].

$$Z_{d\,i+k_2,\,j+l_2}=(A_{ij+l_2}>0\wedge Z_{p\,i+k_2 j+l_2}=1)=1 \quad (13)$$

Решая уравнения (13), находим значения k_2 и l_2 составим предикатное уравнение:

$$Z_{d\,i+k_2+1,\,j+l_2}=(A_{i+k_2,\,j+l_2}>0\wedge Z_{p\,i+k_2+1,\,j+l_2}=1)=1 \quad (14)$$

На *n*-м шаге предикатное уравнение имеет вид

$$Z_{di+k_n,j+l_2}=(A_{i+k_{n-1},j+l_2}>0\wedge Z_{pi+k_n,j+l_2}=1)=1 \qquad (15)$$

В результате решения системы n предикатных уравнений (16) – (18) находим все значения $k_1\cdots k_n$ и запишем форму (вид) столбца протяженного объекта в виде предикатного уравнения:

$$Z_{cdij+l_2}=\bigwedge_{k_1}^{k_n} Z_{di+k_n,j+l_2}=Z_{di+k_1,j+l_2}\wedge Z_{di+k_2,j+l_2}\wedge Z_{di+(k_{n-1}),j+l_2}\wedge Z_{di+k_n,j+l_2}=1 \qquad (16)$$

В результате решения систем предикатных уравнений, подобных уравнениям (13) – (16), находим все возможные значения параметров столбцов символьной модели протяженного объекта Z_{cdij} для $j+l_1\cdots j+l_n$ азимутальных направлений и значение предикатного признака Z_{bij} символьной модели неподвижного протяженного объекта как решение предикатного уравнения

$$Z_{bij}=(\bigwedge_{l_1,k_1}^{l_n,k_n} Z_{cdi+k,j+l}=1)=\bigwedge_{l_1}^{l_n}(\bigwedge_{k_1}^{k_n} Z_{cdi+k,j+l}=1)=1. \qquad (17)$$

Для оценки энергетического признака символьной модели сигнальных отметок для протяженных воздушных объектов введено понятие накопленной энергии протяженного объекта [7, 10] как сумму амплитуд ячеек символьной модели протяженного объекта в направлениях, определяемых векторами (k_n,l_n) согласно предикатному уравнению (17). С учетом распределения амплитуд в пределах символа (k_n,l_n) и, используя данные о форме, определяем энергетический признак символа протяженных неподвижных воздушных объектов как суммарную амплитуду в виде

$$I_{b2}=\sum_{k_1,l_1}^{k_n,l_n} q_{i+k_n,\,j+l_n}\,Z_{cdi+k,\,j+1}. \qquad (18)$$

По виду предикатного признака символьной модели сигнальных отметок для протяженных неподвижных объектов, найденного из системы предикатных уравнений (9) – (12) и (13) – (17), и по энергетическому признаку символьной модели, определенному как суммарную амплитуду в виде (18), осуществляется процедура распознавания протяженных воздушных объектов.

Для оценки эффективности метода, созданных программ проведены модельные эксперименты с использованием записей радиолокационных сигналов. При этом использованы специальные методы обработки цифровой и логической информации [11 – 15]. Апробация проведена в соответствии с правилом, если: 1) отметке соответствуют предикатный признак символьной модели сигнальной отметки для протяженных неподвижных объектов, то отметка относится к классу ангел-эхо; 2) отметке соответствует предикатный признак символьной модели пачки сигналов, то отметка относится к классу воздушных объектов. По результатам экспериментов все они были правильно идентифицированы. Эксперименты показали, что при малых значениях отношения сигнал/помеха, которые не превышают 10 дБ, вероятность обнаружения и распознавания воздушных объектов выше, чем при обработке традиционными методами, а при значениях более 15 дБ результаты приближаются к оптимальным.

Выводы

Приведены результаты апробации метода обработки радиолокационных изображений на основе интеллектуального анализа процессов для системы автоматического обнаружения радиолокационных отметок воздушных объектов и их распознавания. Метод основан на

определении системы предикатных признаков, позволяющей описать семантическую составляющую символьной модели отметок. Приводятся процедуры формирования предикатных признаков символьной модели точечных и протяженных воздушных объектов как совокупности предикатных признаков наличия и ухода (смещения) сигнала в соседние по азимуту и по дальности ячейки. Создано алгоритмически – программное обеспечение с обработкой реальных записей обзорных РЛС. Показано как по величинам параметров геометрического образа символьного изображения определяется принадлежность отметки к точечному или протяженному воздушному объекту. В результате семантического анализа стационарности флуктуаций пачки идентифицируется принадлежность отметок подвижным или неподвижным воздушным объектам. Исследованы семантические составляющие распознавания, которые подобны алгоритмам принятия решений человеком-оператором. Распознавание отметок проводится путем решения разработанных уравнений предикатных операций.

Список литературы:

1. Jianping Ou, Jun Zhang, and Ronghui Zhan. Processing Technology Based on Radar Signal Design and Classification // International Journal of Aerospace Engineering. Vol. 2020, pp. 1-19. Article ID 4673763. https://doi.org/10.1155/2020/4673763.
2. Skolnik M. I. (eds) (2021) Radar Handbook, McGraw-Hill, New York.
3. Berkler Katrin. Trends in artificial intelligence / Editorial team Janis Eitner (V.i.S.d.P.), Katrin Berkler, Henning Köhler, Roman Möhlmann. Fraunhofer-Gesellschaft e.V., 2018. p.p. 1-32.
4. Левыкин В.М., Чалая О.В. Модель жизненного цикла знаний – емкого бизнес-процесса // УСыМ. 2017. №1. С. 68-85.
5. Журавлев, Ю. И. Об алгебраическом подходе к решению задач распознавания или классификации / Ю. И. Журавлев // Проблемы кибернетики. 2005. Вып. 33. С. 5–68.
6. Russell S. (2019) Human compatible: Artificial intelligence and the problem of control, Penguin.
7. Solonskaya S., Zhirnov V. (2018). Intelligent analysis of radar data based on fuzzy transforms // Telecommunications and Radio Engineering, 77(15), pp.1321-1329.
8. You He; Jianjuan Xiu; Xin Guan. Radar Data Processing with Applications // Publisher John Wiley & Sons. 2017. https://app.knovel.com/web/toc.v/cid:kpRDPA0001/viewerType:toc/. ISBN978-1-118-95686.
9. Kozulia Tatiana, Sharonova Natalia, Kozulia Mariia. Knowledge-based information support formation for complex systems research // Системні дослідження та інформаційні технології. 2017. No 3. P. 63-72.
10. Солонская, С.В., Жирнов, В.В. Предикатная модель процессных знаний при обнаружении и распознавании протяженных объектов типа облака, тучи, «ангел-эхо» в обзорных РЛС // Радиотехника. 2020. № 202. С 164-172.
11. Bendich P., Bubenik P., Wagner A. Algorithms and complexity for Turaev–Viro invariants // Journal of Applied and Computational Topology, vol. 2.1, pp.33-53, 2018.
12. Zhyrnov V., Solonska S. (2020). Intelligent system for detection of low-visible air objects in surveillance radars // Telecommunications and Radio Engineering. 2020. Vol. 79, Issue 17. pp. 1513-1519.
13. Advanced Methods and Deep Learning in Computer Vision.1st Edition / Editors: E. R. Davies, Matthew Turk. Academic Press. 2021. Page Count: 586. ISBN: 9780128221099.
14. Zubkov O., Sheiko S.. Oleynikov M., Kartashov V., Babkin S. INVESTIGATION OF EFFICIENCY OF DETECTION AND RECOGNITION OF DRONE IMAGES FROM VIDEO STREAM OF STATIONARY VIDEO CAMERA // Telecommunications and Radio Engineering. 2021. Vol. 80, Issue 3. pp. 23-37.
15. Sytnik, Igor Vyzmitinov. ADAPTIVE APPROACH TO FILTERING OF STOCHASTIC PROCESSES IN RESCUER RADAR // Telecommunications and Radio Engineering. 2021. Vol. 80, Issue 3. pp. 1513-1519.

Поступила в редколлегию 11.11.2021

Сведения об авторах:

Жирнов Владимир Витальевич – канд. техн. наук, Харьковский национальный университет радиоэлектроники, в.н.с. НИЦ интегрированных радиоэлектронных систем и технологий, Украина; e-mail: nauka123@ukr.net; ORCID: http://orcid.org/0000-0002-2397-3126

Солонская Светлана Владимировна – канд. техн. наук, Харьковский национальный автомобильно-дорожный университет, доцент кафедры естественных и гуманитарных наук, Украина; e-mail: solonskaya@ukr.net, ORCID: https://orcid.org/0000-0002-8841-7825

Шубин Игорь Юрьевич – канд. техн. наук, Харьковский национальный университет радиоэлектроники, доцент кафедры программной инженерии, Украина, e-mail: igor.shubin@nure.ua; ORCID: https://orcid.org/0000-0002-1073-023X

УДК 007.51 **DOI:10.30837/rt.2021.4.207.10**

В.М. КАНЦЕДАЛ, канд. техн. наук, А.А. МОГИЛА, канд. физ.-мат. наук

ОСОБЕННОСТИ УПРАВЛЕНИЯ ПОМЕХОЗАЩИЩЕННОСТЬЮ ОБЗОРНОЙ РЛС ПРИ ЕЕ ПОДАВЛЕНИИ АКТИВНЫМИ ПОМЕХАМИ И МЕШАЮЩИМИ ИНФОРМАЦИОННЫМИ ВОЗДЕЙСТВИЯМИ

Введение

Рассматриваются особенности кризисного управления информационной устойчивостью режимов зондирования обзорной РЛС в условиях их радиоэлектронного подавления (РЭП) воздушным комплексом РЭП с применением управляемых активных помех и мешающих информационных воздействий. Помехозащищенность режимов зондирования РЛС при этом существенно зависит не только от качества применяемых конкретных способов и средств радиоэлектронной защиты (РЭЗ), условий их применения, но и от свойств управления их применением. Поскольку с течением времени состав и содержания конфликтных ситуаций (КС) изменяется, уточняется знание о стратегии комплекса РЭП в рамках двусторонней модели динамического конфликта между комплексом РЭП и РЛС, то это делает необходимым синтез закона управления процессами РЭЗ и координации действий в ходе конфликта. Особенностью динамической модели конфликтного взаимодействия является то, что стратегии подавления РЛС активными помехами и ее РЭЗ от их угроз воздействия сопровождаются информационным противоборством, а также возможностью изменения динамического состояния КС внутренним и внешним управлением [1 – 7, 13].

Информационная устойчивость является объектом управления (ОУ) в структуре специализированной системы автоматизированного управления $САУ_{уст}$ [5 – 7]. На практике описание стратегии РЭЗ ограничиваются возможностями контура стратегий внутреннего реактивного управления средствами РЭЗ от угроз воздействия активных помех [2, 8]. Эти стратегии характеризуются как ресурс затратные, когда каждой угрозе противопоставляется средство или набор средств РЭЗ. Управление осуществляется субъектом управления по данным системы анализа только сигнально-помеховой обстановки (САПО), используя правило «если …, то …». При этом управлении доминируют информационные данные, в том числе мешающие информационные воздействия. Требуется совершенствование ее структуру, чтобы она могла синтезировать в динамике конфликта адекватные угрозам стратегии управления средствами РЭЗ с желательными свойствами, вырабатывать более обоснованные и оперативные управляющие решения при временном дефиците на принятие решения и субъектности кризисного управления.

Информационные воздействия, связанные со скрытым и активным изменением динамического состояния КС для получения конфликтного преимущества, реализуется в контуре стратегий внешнего управления предлагаемой структуры $САУ_{уст}$. Они направлены на нарушение функционирования систем радиотехнической разведки и управления (СРТР – $САУ_{РЭП}$), управления и радиоэлектронного подавления ($САУ_{РЭП}$ – СРЭП) комплекса РЭП. Это достигается введением субъекта их управления, алгоритмов принятия решения в заблуждение ложными информационными воздействиями и психологическим давлением, навязыванием системам поведения, нужного для повышения эффективности $САУ_{уст}$. То есть, специфика стратегий внешнего управления состоит в постановке нестандартных целей определенной направленности и выделении соответствующего ресурса для их достижения. Это требует системно-процессного, когнитивного подхода к управлению и применении рефлексивной формы управления, опирающейся на знания о стратегиях управления РЭП и РЭЗ, высокий уровень профессиональных компетенций субъекта управления, а также наличия в структуре $САУ_{уст}$ контура интеллектуального управления в составе контуров внутреннего и внешнего управлений.

Заметим, что кризисное управление информационной устойчивостью режимов зондирования характеризуется:

- борьбой с опасными угрозами стратегии РЭП, которая в основном опирается на опыт применения способов и средств РЭЗ и его обобщение при внутреннем управлении в $САУ_{уст}$;

- возможностью получения конфликтного преимущества за счет создания условий не только для нормальной работы режимов РЛС, но и для более эффективной работы средств радиоэлектронной маскировки (РЭМ), РЭЗ, информационного противоборства и нестандартных процедур управления ими.

То есть, одним из важных направлений совершенствования САУуст является управление целеполаганием процессов РЭЗ с минимизацией ошибок целеполагания. Просчеты целеполагания, выявляемые на этапе реализации управленческих решений, не позволяют [10, 11] достичь выдвинутых целей, решить поставленные задачи управления, влекут дополнительные затраты ресурсов на достижение не своевременно осознаваемых ложных целей. Причиной является сложность конфликтных процессов, частичная формализация процесса целеполагания, ряд этапов которого основывается на субъективных моделях, интуитивных методах и здравом смысле субъекта управления. Фрагментарность и автономность формализаций при системном характере процессов целеполагания, существенный вес субъективного компонента являются предпосылками недостаточной обоснованности и согласованности результатов отдельных этапов целеполагания, сказываясь на качестве принимаемых, на их основе решений. Поэтому важно для повышения эффективности САУ $_{уст}$ рассмотреть особенности процессов анализа полагания и синтеза достижения целей, а также логики последовательности их применения при построении стратегии управления процессами РЭЗ.

Вопросам частичной формализации и интеллектуализации процессов управления, в частности целеполагания для повышения обоснованности и оперативности управляющих решений, снижения влияния субъектности целеполагания посвящены ряд работ в различных предметных областях, например [10, 11, 18, 20]. Вместе с тем, существует потребность в результатах системного анализа особенностей процессов целеполагания при обеспечении информационной устойчивости режимов зондирования обзорной РЛС в указанных условиях ее РЭП.

Все это делает актуальным совершенствование структуры САУ$_{уст}$, моделей и средств процессов целеполагания при выработке решений кризисного управления и оценке их результатов, что является важной не только научной, но и практической задачей.

Цель работы – выявить основные особенности способов и средств управления процессами целеполагания в специализированной системе управления (САУ$_{уст}$), способствующие повышению и обеспечению информационной устойчивости режимов зондирования обзорной РЛС в условиях ее подавления управляемыми активными помехами и мешающими информационными воздействиями, которые позволяют придать, синтезируемым в ходе конфликта стратегиям и закону управления РЭЗ и координации действий, желаемые свойства.

Постановка задачи

Под информационной устойчивостью режимов зондирования РЛС в проблемных областях (секторах наблюдения) зоны обзора РЛС для различных этапов радиолокационной разведки воздушных целей понимается [2, 8, 9] их свойство осуществлять требуемые преобразования эхосигналов, радиолокационной информации (РЛИ) при воздействии факторов нестабильности, сохраняя выходные реакции в пределах допусков, установленных тактико-техническими требованиями.

Проблемные области – это области в зоне обзора РЛС, для которых характерны устойчивые особенности протекания конфликтного взаимодействия, связанными с конкретным режимом зондирования на этапах разведки воздушной цели и динамическим состоянием КС.

Факторы нестабильности порождаются: комплексом РЭП; сменой: проблемных областей зоны обзора РЛС, отличающихся динамическим состоянием КС, разнообразием видов и параметров мешающих воздействий; КС; режимов зондирования РЛС на этапах разведки воздушных целей, сменой целей; критериев эффективности управления; принятием субъектом управления неправильных управляющих решений. При смене режимов зондирования требуется, чтобы время переходного процесса, вызванного управляющим действием, было значительно меньше, чем интервал стабильной работы текущего режима зондирования. Это дает возможность не накладывать ограничения на возможность изменения режима зондирования.

Процесс целеполагания представляется как совокупность циклических поступательных действий, связанных с выявлением проблем, поиском решений и организацией их выполнения в определенных условиях при имеющихся ресурсах. Смысл целеполагания при этом заключается в обосновании и постановке целей для преодоления возникшей проблемы, а также

в выборе путей достижения поставленных целей с контролем отклонения фактических целевых показателей от требуемых [14 – 16]. Фиксирование этого смысла, дополненное требованием минимальных ресурсных затрат за допустимое время, определяет искомый закон ситуационного управления процессами РЭЗ и координации действий.

Целеполагание является основной ключевой функцией управления, которая не только в основном определяет содержание и эффективность управления, но и объединяет и определяет содержание всех остальных функций управления [14 – 16].

Цель – это образ желаемого состояния устойчивости режима зондирования РЛС в конфликтных условиях и основа для подготовки, принятия и реализации управляющих решений.

Процесс управления – это иерархический процесс выполнения функций управления, в результате которых управляемый объект приводится в желаемое состояние. Качеством целеполагания, в свою очередь, обусловлено тем, насколько в поставленных целях (оперативных, тактических, стратегических) точно и полно отражена проблема, отделяющая текущую КС от желаемой. Целеполагание задается системой целей, критериев и их показателей эффективности для иерархических уровней управления. Целеполагание должно быть адекватно угрозам конфликтных ситуаций, соразмерно с опасностями их составляющих, а также соответствовать требуемым целевым показателям.

Целеполагание зависит от многих факторов, определяющими из которых являются [3 – 7, 13]: сложность двухсторонней динамической модели рассматриваемого конфликтного взаимодействия, специфика построения и функционирования структуры $САУ_{уст}$ и участие субъекта управления – субъектность управления.

Влияние сложности целеполагания характеризуется:

- объектами и факторами внешнего и внутреннего управления: структурой, стратегией и тактиками комплекса РЭП; КС; совокупностью информационных режимов зондирования РЛС и средств их РЭЗ; исследованиями их результативности и устойчивости, а также структурой и динамикой функционирования самой $САУ_{уст}$ [1 – 8, 13];

- неопределенностью информации о возможном развитии событий при достижении поставленной цели, которая характеризуется расширением спектра возможных конфликтных ситуаций, когда становится все более трудным заранее предугадать и заложить данные в процессы целеполагания, адекватностью результатов процессов анализа состояния и динамики текущей КС;

- многообразием и изменчивостью (скачкообразной динамичностью) способов постановки, видов маскирующих и имитирующих активных помех с широкими диапазонами изменения их параметров, которые в комбинации могут вызвать различного рода уязвимости устойчивости режимов зондирования;

- тенденцией перехода от многообразия видов и параметров активных помех силового характера воздействия к низко мощным «сигналоподобным» помехам с имитирующими эффектами воздействия на системы обработки информации в РЛС, что затрудняет их выделение и дальнейшую нейтрализацию их воздействий;

- наличием скрытого обманного информационного воздействия противника, провокационного или имитационного характера с целью дезинформации и направленного на искажения алгоритмов управления информационной устойчивостью режимов зондирования; разрушением структурных связей их системы управления, а также с целью психофизического давление на субъект управления;

- комбинированием «сигналоподобных» помех и мешающих информационных воздействий;

- расширением разнообразия способов и средств РЭЗ как адекватной реакции на многообразие способов постановки активных помех [2, 8], информационных воздействий и их видов с широким диапазоном изменения их параметров, качеством и количеством комбинаций при их комплексировании в ходе противодействия стратегии РЭП и нейтрализации этих воздействий;

- трудностями формализации процессов целеполагания и оценки показателей их эффективности для различных динамических состояний КС, что требует применении дополнительно к логико-оптимальному методов для синтеза искомого закона управления процессами РЭЗ [10 – 12].

Информационное противоборство [3, 4, 13] для скрытого проникновения в автоматизированный процесс принятия противником решения на проведение РЭП с помощью обмана и

рефлексивной формы управления выполняется путем: а) технико-информационных воздействий на СРТР-САУ$_{РЭП}$, САУ$_{РЭП}$-СРЭП и систему наведения в СРЭП для затруднения или срыва процессов управления комплексом РЭП; б) психофизического давления на сознание и физическое состояние субъектов управления комплекса РЭП. Использование способов информационного противоборства таит в себе возможности получения конфликтного преимущества, несмотря на значительные интеллектуальные усилия для: маскировки своих действий (излучения зондирующего сигнала и применения средств РЭЗ); принуждения противника к нужным для РЛС действиям ведением его в заблуждение дезинформацией, манипуляцией информации, имитацией действий и др. Эффективность информационного противоборства зависит от способностей интеллекта системы управления полно учитывать цели и поведение противника. Сторона, имеющая более высокий ранг рефлексии, получит конфликтное преимущество в результате информационного противоборства.

Для построения процессов целеполагания и обеспечения эффективности его решений используется совокупность системно-процессного, целевого, ситуационного и интерпретационно-экспериментального (эвристического) подходов к управлению [14 – 16]. Получаемый при этом результат формализации процессов целеполагания позволяет видеть полный список задач, осуществлять контроль решения каждой задачи с начала и до конца, возможность видеть место трудностей и срыва процессов целеполагания. Такое представление помогает сфокусироваться на целевой и значимой информации для решения задач оптимизации процессов целеполагания. Формализация способствует разработке решений, адаптации интерфейсов субъектов управления в схемах управления структурными элементами САУ$_{уст}$ или ее базовыми объединениями функциональных элементов.

Поэтому преодоление сложности процессов целеполагания возможно при использовании адекватной структуры САУ$_{уст}$, обеспечении в ней системности процессов, повышения уровней формализации и интеллектуализации этих процессов. Это позволит существенно снизить степень влияния субъективности на вырабатываемые в САУ$_{уст}$ решения по целеполаганию и добиться их обоснованности, полноты, непротиворечивости и согласованности.

Ниже приводится рассмотрение влияния указанных факторов на процессы целеполагания.

Особенности построения и функционирования САУ$_{уст}$, влияющие на структуризацию, интеллектуализацию процессов целеполагания, повышение обоснованности и оперативности решений в условиях дефицита времени на принятие решения

Повышение конфликтной устойчивости режимов зондирования РЛС во многом определяются возможностями САУ$_{уст}$, обоснованная структура, которой представлена в работах [5 – 7] в результате многофакторного анализа. Взаимодействие структурных элементов САУ$_{уст,}$ последовательно реализующее непрерывные циклы управления целеполаганием, выполняется на трех иерархических уровнях управления контуров внутреннего и внешнего управлению с распределенными на них функциями управления. Так, целеполагание направляет их выполнение на уровнях:

- верхнем (стратегическом), где осуществляется анализ результатов оценки динамического состояния КС и вероятностных прогнозов его развития, с выявлением проблемы; постановкой и согласованием целей на иерархических уровнях управления САУ$_{уст}$, построение многоцелевой стратегии управления РЭЗ на относительно отдаленную перспективу;

- среднем (тактическом), где определяются способы ситуационного управления для: достижения поставленных целей и перестройки функциональной структуры САУ$_{уст}$ на ближнюю перспективу в соответствии с выбранным направлением РЭЗ; обоснования перестройки как этапов процессов синтеза искомого закона ситуационного управления процессами РЭЗ, осуществляющими практическое распределение ресурсов РЭЗ в зависимости от поставленной цели, степени неопределенности динамического состояния КС и формализации задач управления, так и тактической структуры средств РЭМ, РЭЗ и информационного противоборства;

- нижнем (оперативном), где выполняется: технологическая перестройка структуры САУ$_{уст}$ с регулированием режимов и параметров задействованных средств противодействия стратегии РЭП на текущий период времени; контроль на соответствие фактического результата достижения выбранной частной стратегической цели ожидаемому с последующим ини-

циированием устранения отклонения от ожидаемой цели и корректировкой структуры $САУ_{уст}$ в смысле придания ей дополнительных ресурсов РЭЗ и времени для достижения стратегической цели или ее смены.

Динамика перестройки иерархической структуры $САУ_{уст}$ определяется целеполаганием, вырабатываемым субъектом управления и контуром интеллектуального управления в различных КС с учетом ресурсных возможностей и ограничений. Динамика функционирования $САУ_{уст}$ реализуется с помощью объединения структурно-функциональной и сете-центрической схем системно-процессного, когнитивного и рефлексивного управления. Синтез стратегий и закона ситуационного управления процессами РЭЗ строится на балансе одновременного применения этих схем управления с учетом текущих условий наблюдения, принятия решений и результатов контроля их выполнения.

Объединение структурно-функциональной и сете-центрической схем управления функционированием $САУ_{уст}$ делает возможным процесс синтеза этапов целеполагания, из набора более простых процессов, выполняемых структурными элементами $САУ_{уст}$ на иерархических уровнях управления с учетом циклов управления для дальней, ближней перспектив и текущего периода времени, а также скорости изменений КС.

Структурно-функциональная схема построена с учетом аксиом и этапов рационального иерархического управления [14 – 16]. Эта схема многоканальная. Число каналов схемы определяется числом решаемых отдельных задач верхнего уровня управления. Каждый канал схемы реализует этап информационного обеспечения процессов управления (Подсистему процессов информационного обеспечения управления РЭЗ) и этапы подготовки, принятия и реализации решения на иерархических уровнях управления (Подсистему процессов подготовки, принятия и реализации конфликтно-устойчивого решений без субъекта управления, но под его контролем). Их работа базируется на применении логико-оптимальных методов анализа и синтеза в условиях определенности и рисков КС. Эта схема управления реагирует на сравнительно медленные изменения состояния КС.

Многоконтурная сете-центрическая схема обеспечивает приоритетное участие субъекта управления в процессах управления и составляет с учетом прямых и обратной связей в структуре $САУ_{уст}$ основу контура интеллектуального управления $САУ_{уст}$ в условиях сложных и непредсказуемых КС с высоким уровнем неопределенности различного рода. Субконтуры управления в контурах внешнего и внутреннего управления выполняют управление функциональными модулями в структурно-функциональной схеме на уровнях и этапах управления. Структуры этих субконтуров управления включают в свой состав специализированные информационные, управляющие и исполнительные средства, реализуемые структурными элементами $САУ_{уст}$. Схема функционирует в режиме реального времени и ориентирована на быстрые изменения состояния КС. Она отличается повышенной чувствительностью к изменениям состояния КС, быстротой реакции на эти изменения в условиях неопределенности различного рода и дополняет структурно-функциональную схему возможностью оперативного вмешательства субъекта управления на ее этапах.

Интеллектуальная платформа иерархической структуры сете-центрической схемы управления состоит из использования когнитивных и креативно-рефлексивных способностей субъекта управления, его профессиональных компетенций и возможностей специализированной интеллектуальной системы поддержки принятия решений (ИСППР). Интеллектуальное управление – это технология управления знаниями, которая играет основную роль при принятии решений. Оно дает возможность, наряду с решением или в ходе получения решения, осуществлять поиск новых знаний и накопление интеллектуальных ресурсов [18].

Субъект управления принимает участие в моделях решения задач на уровнях и этапах управления в структурно-функциональной схемы синтеза стратегий и закона ситуационного управления процессами РЭЗ, реализации ряда других функций управления на иерархических уровнях управления. Он ведет наблюдение за ходом процессов целеполагания, используя прямые и обратные связи в структуре $САУ_{уст}$ для обучения и накопления знаний на всех уровнях иерархии управления в едином с ИСППР поле управления, осуществляет координацию действий для получения синергии целеполагания.

ИСППР на основе экспертных систем интегрирована в объединение структурно-функциональной и сете-центрической схем управления. Это создает единую среду интеллектуального управления с применением формального и неформального знания о конкретных способах и средствах РЭП и РЭЗ, условиях их применения и свойствах управления их при-

менениями, сосредоточенного в этих схемах и ИСППР. ИСППР также накапливает результаты анализа информации о применяемых стратегиях РЭП и РЭЗ. Этим самым система усиливает креативно-рефлексивные способности субъекта управления и повышает уровень его профессиональных компетенций, расширяет возможности поиска эффективных решений на этапах процессов анализа, вероятностного прогноза и синтеза целей РЭЗ на временных интервалах, соответствующих уровням управления в $САУ_{уст}$ [17, 18].

Применение ИСППР осуществляется в зависимости от степени неопределенности КС и их смены, а также степени формализации процессов синтеза на основе использования знаний о сильных и слабых сторонах антагонистических стратегий сторон конфликта. Это особенно важно:

- при высокой динамике изменения КС и значений ее параметров;
- периодическом отсутствии прагматической своевременной информации, необходимой для принятия решений;
- стремлении противника сформировать заведомо ложные представления об истинных значениях параметров КС;
- жестких временных ограничениях, накладываемых на принятие решений.

ИСППР поддерживает принятие решения логико-лингвистическим или/и экспертным или эвристическими методами в объединении представленных схем управления целеполаганием.

Необходим учет влияния факторов субъективности управления целеполаганием на эффективность процессов кризисного управления в условиях повышенной напряженности во внештатных режимах и в условиях дефицита времени. Поэтому критерии, их показатели оценки степени соответствия профессиональных компетенций субъекта управления требуемой модели поведения, обеспечивающей успешное достижение стратегических и тактических целей РЭЗ, $_{т}$ должны входить в состав показателей эффективности управления в $САУ_{ус}$. Для оценки интеллектуального уровня применяется компетентностный подход и измерение профессиональных компетенций [19 – 24].

Заметим, что при целеполагании также возможны и автоматические решения в случае воздействия активных помех в простых и определенных КС.

Особенности этапов целеполагания

Основными инструментами частичной формализации процессов целеполагания, оставляя поле деятельности для субъекта управления, являются:

- постановка задачи синтеза стратегий рационального многоцелевого управления и ситуационного закона управления процессами РЭЗ динамической информационной устойчивости режимов зондирования РЛС в проблемных областях зоны обзора РЛС;
- выделение контуров внешнего и внутреннего управления, отличающихся целями управления;
- цели, критерии и их показатели эффективности целедостижения для придания желательных свойств структуре $САУ_{уст}$ и динамике ее функционирования;
- создание условий обеспечения целевого результата с учетом приоритетности действий в условиях ограничений ресурса РЭЗ;
- порядок решения задач на иерархичных уровнях в Подсистемах процессов информационного обеспечения и интеллектуального управления целеполаганием;
- базовая модель многоцелевой стратегии прогнозирующего управления процессами РЭЗ;
- использования обратной связи для придания непрерывности процессам целеполагания по результатам контроля и анализа несоответствия результата поставленной цели, а также учета результатов анализа накопленной информации о применяемых стратегиях РЭП и РЭЗ. Обратная связь дает возможность выявить признаки скрытого внешнего управления противником функционирования объекта управления и $САУ_{о}$.

Этап информационного обеспечения

Целеполагание должно учитывать отслеживаемые на этом этапе в ходе конфликта конкретные возможности стратегии РЭП относительно: изменений параметров окрестностей точек би-полифуркации процесса РЭП; опасных постановок активных помех, их видов и параметров, а также характеристик мешающих информационных воздействий; классификации

КС; вероятностных прогнозов динамик развития КС для временных циклов уровней управления и оценок опасностей прогнозируемых угроз.

Подсистема процессов информационного обеспечения $САУ_{уст}$ частично формализует эти процессы в реальном времени. Она определяет и распределяет по уровням управления условия наблюдения и принятия решений: состояние определенности КС; наличие рисков управления, когда известны вероятности событий и размеры потерь состава и качества РЛИ; состояние неопределенности КС.

Добываемая информация об угрозах и воздействующих помехах используется для оптимизации процессов решения информационных задач режимов зондирования в условиях воздействия различных видов помех и их параметров с одной стороны, а с другой – для снижения возможностей комплекса РЭП по разведке режимов зондирования РЛС и их подавлению.

Анализ осуществляется на основе знания двухсторонней динамической модели конфликтного взаимодействия составных частей комплекса РЭП и обзорной РЛС [6, 7], а также предварительно проведенной классификации КС с использованием приемов SOFT-анализа [22], когнитивных карт [23] для структурирования информационных данных.

Полнота (насыщенность знаниями, результатами критического их анализа и сопоставления), достоверность и своевременность распределения полученной информации между всеми уровнями и их этапами управления, средствами РЭЗ для трансформации результатов информационного обеспечения в процессы целеполагания и согласования связей между ними является необходимым условием эффективного целеполагания.

Обобщенным показателем эффективности информационного обеспечения может служить ее вероятность через вероятности выполнения перечисленных функциональных задач за время, не превышающее допустимое значение.

Целеполагание на верхнем уровне управления

Подсистема процессов интеллектуального управления этапами целеполагания на этом уровне частично формализует постановку иерархически связанных целей с учетом их выполнимости и ряда стратегических задач целеполагания в некоторой проблемной области зоны обзора РЛС с конкретным режимом зондирования и динамическим состоянием КС.

Формализация процессов целеполагания осуществляется с приоритетом целей и их достижением над информационным описанием конфликтных ситуаций.

Постановка задачи синтеза стратегий рационального управления процессами РЭЗ динамической информационной устойчивости режимов зондирования РЛС.

Отправной точкой построения стратегии является формулировка проблемы, которая снижает неопределенность, получая представление о том, чего можно добиться управлением. Для этого осуществляется обоснованный выбор: цели, отражающий определенный результат, которого желает достичь $САУ_{уст}$; методов и средств достижения целей; наиболее эффективного порядка их применения при достижении главной стратегической цели.

Стратегии, как последовательности решаемых частных стратегических задач (1) с учетом логики взаимосвязи между ними, синтезируются в цикле стратегического управления таким образом, чтобы каждый очередной n-й управляющий вектор **U** при смене КС наилучшим образом отвечал достижению главной цели управления процессами РЭЗ с учетом индивидуальных особенностей текущего режима зондирования и КС (проблемной области зоны обзора). Решения при этом стратегических задач должны носить взаимно усиливающий характер, а общее количество векторов **U** зависят от динамики стратегии РЭП и степени неопределенности описания динамического состояния КС.

$$\left\{\left|S^{Ц}-S^{Ф}\right|=F\left[Z,R,I,L(u),K,KC(n)\right]\right\}_{KC(n)}\to const \text{ для всех } KC(n),\ n=1,2,3,\ldots \quad (1)$$

$$\left|S^{Ц}-S^{Ф}\right|=F\left[Z,R,I,L(u),K\right]\to\min,R\to\min,T\le T_{ДОП}, \quad (2)$$

Выражение (2) отражает условие нахождения закона управления процессами РЭЗ в динамике изменения некоторой КС (в ситуационном цикле управления):

В выражениях (1), (2) используются векторы параметров модели объекта управления:

$S^{Ц}$ – вектор описания желаемого состояния информационной устойчивости режима зондирования (или КС в случае активного изменения ситуации); $S^{Ф}$ – вектор описания фактически

достигнутого на данный момент времени состояния при выборе текущего управляющего элемента (УЭ) с указанием количественных характеристик степени достижения цели РЭЗ на основе контроля результата управления и условий наблюдения и принятия решения; I – вектор индивидуальных характеристик режима зондирования (или КС); R – вектор, который характеризует виды затрат ресурсов, имеющихся в распоряжении $САУ_{уст}$ на данный момент времени; F – структура закона управления процессами РЭЗ, связывающая выход режима зондирования с мешающими воздействиями и средствами поддержки устойчивости, $L(u)$ – оператор $U \rightarrow S^{Ф}$, отображающего элементы $САУ_{уст}$ на совокупность показателей фактического состояния режима зондирования или *КС, U* – последовательность из УЭ, приводящая к поставленной цели РЭЗ; Z – база знаний, K – вектор учета предпочтений субъекта управления, как оценка полезности или качества рассматриваемой альтернативы. Он может быть задан интегрально без выделения признаков, по которым он производится, а также по различным признакам.

Закон управления процессами РЭЗ в динамике некоторой КС состоит в том, чтобы сформировать такую последовательность из УЭ, которая наиболее эффективно *приводит* к поставленной частной цели РЭЗ. При формировании каждого управляющего воздействия оценивается разность $\left|S^{Ц} - S^{Ф}\right|$, минимальное значение которой соответствует оптимальному для данной ситуации управляющему воздействию.

Базовая многоцелевая стратегия прогнозирующего управления процессами РЭЗ.

Эта стратегия, содержащая цели общих стратегических направлений РЭЗ РЭП в рамках двусторонней динамической модели рассматриваемого конфликтного взаимодействия [5 – 7] и логики их применения. Она фиксирует стратегическое видение и определяет систему координат, в которых осуществляется противодействие стратегии РЭП. Ее логики процессов принятия управленческих решений учитывают неопределенность возникновения КС, особенности функционирования обзорной РЛС в динамике конфликта и предполагают гибкий порядок изменения целей с использованием фактических результатов процессов целедостижения и прогнозов конфликтного взаимодействия. Базовая стратегия используется в качестве источника априорной информации относительно системы целей и формализации их постановки в динамике конфликта, имеющегося ресурса РЭЗ в структуре $САУ_{уст}$, необходимого для реализации каждой выбранной цели, а также начального его распределения. Она является руководством для постановки целей, обеспечивает основу для их согласования в прогнозируемых условиях конфликтного взаимодействия.

Основными принципами ее построения являются: двойное понимание КС — правильного у себя и ложного у противника; действовать при благоприятном для достижения поставленных целей стечении обстоятельств; применять сочетания возможных тактик управления состоянием и динамикой КС с использованием «несиловых» и «силовых» технических решений при наименьших затратах ресурсов. Должно также выполняться необходимое условие – минимизация времени, отведенного на принятие стратегического решения.

Методической основой целевого подхода является определение главной цели и ее дифференциации по иерархическим уровням управления и процессам управления целеполаганием на них (а также по элементам структуры $САУ_{уст}$) для задания оптимальной последовательности действий при достижении поставленных целей.

Главную цель РЭЗ можно формулировать следующим образом: обеспечить заданные вероятности устойчивого функционирования режимов зондирования РЛС и $САУ_{уст}$ путем создания условий для непрерывного и нормального функционирования режимов зондирования обзорной РЛС в конфликтном взаимодействии с комплексом РЭП, а также реализация эффективных процессов целеполагания. Другими словами, цель функционирования $САУ_{уст}$ состоит в том, чтобы показатели устойчивости режимов зондирования находилась в пределах заданной целевой области $\left|S^{Ц} - S^{Ф}\right|$ или минимизировали расстояния до заданной целевой точки или области (1),(2)..

На рис. 1 представлен вероятностный вариант базовой стратегии управления процессами РЭЗ для каждой проблемной области. Он предполагает для достижения главной цели управления несколько направлений и логик процессов принятия управленческих решений в зависимости от результата прогноза условий наблюдения и принятия решений.

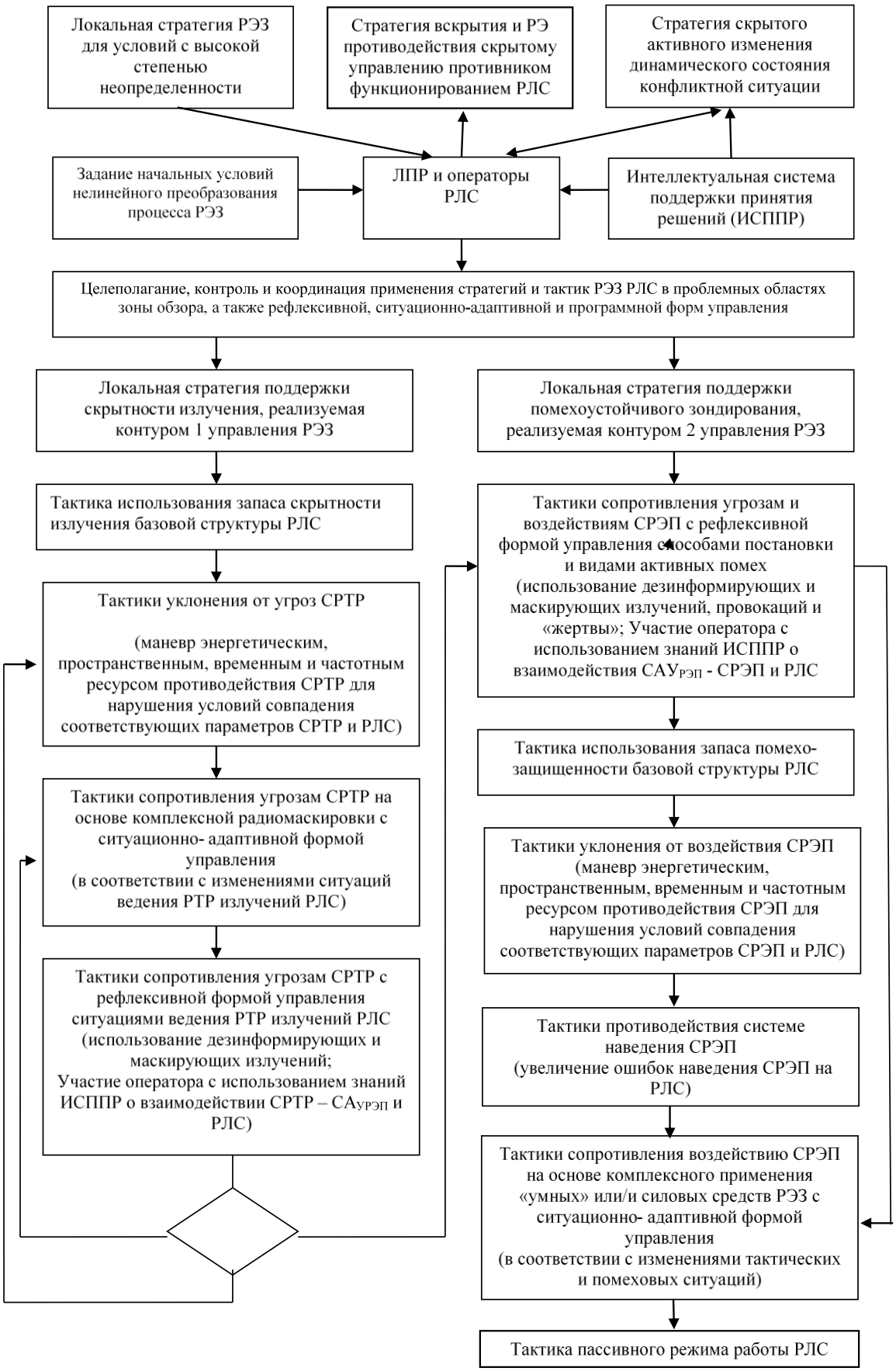


Рис. 1. Вариант базовой многоцелевой стратегии прогнозирующего управления процессами РЭЗ обзорной РЛС в условиях преднамеренных активных помех и мешающих информационных воздействий в проблемных областях ее зоны обзора

К ним относятся:

1) комбинирование частных целей стратегий внутреннего и внешнего управления в следующей последовательности:

- для создания предпосылок и условий устойчивости непрерывного и нормального функционирования текущего режима зондирования РЛС путем создания запаса помехозащищенности в его алгоритме применением модели зондирующего сигнала с повышенной скрытностью излучения и помехоустойчивостью согласованной обработки принимаемых сигналов;

- создания условий для предотвращения с упреждением потери скрытности излучения РЛС путем применения стратегии рефлексивной поддержки энергетической и структурной скрытности излучения с применением средств РЭМ;

- создания условий для предотвращения с упреждением влияния опасных активных помех после утраты скрытности излучения путем применения стратегии рефлексивной поддержки помехоустойчивого зондирования активным информационным воздействием на динамическое состояние КС и использованием средств РЭЗ;

- оказания сопротивления воздействиям активных помех путем применения реактивной стратегии внутреннего ситуативного управления, используя средства РЭЗ для их компенсации или подавления;

- выявления скрытого управления противником информационной устойчивостью режимов зондирования РЛС и $САУ_{уст}$ по результатам оценок психологического давления на субъекта управления, нарушений алгоритмов принятия управляющих решений и рассогласования, фактически достигнутых целей с ожидаемыми, а также оказание им сопротивления;

2) использование стратегии поддержки помехоустойчивого зондирования РЛС в условиях воздействия активных помех путем применения тактик: с рефлексивной формой управления способами постановки и видами активных помех в системах $САУ_{РЭП}$ – СРЭП; использования запаса помехозащищенности базовой структуры РЛС: уклонения от воздействия СРЭП; противодействия системе наведения СРЭП; оказания сопротивления воздействиям СРЭП; использования пассивного режима работы РЛС;

3) использование стратегии скрытого активного изменения динамического состояния КС путем технико-информационного и психофизического воздействия на системы СРТР – $САУ_{РЭП}$, $САУ_{РЭП}$ – СРЭП комплекса РЭП;

4) использование стратегии РЭЗ для условий высокой неопределенности КС на основе применения логико-лингвистического и/или экспертного или эвристического методов управления целеполаганием по косвенным признакам нарушения устойчивости; полученных с помощью интеллектуальных методов и средств управления.

При постановке целей также определяется то, чего нельзя делать при любых обстоятельствах.

Целеполагание на среднем уровне управления

Подсистема процессов интеллектуального управления этапами целеполагания на этом уровне частично формализует: определение, обоснование способов достижения поставленных стратегических целей; получение управляющих решений для перестройки структуры $САУ_{уст}$, связанной с рациональным распределением ресурсов РЭМ, РЭЗ и/или средств информационного противоборства, необходимых для достижения поставленных целей. Управляющими параметрами при этом являются тактики и их ресурсы. Основные тактические приемы управленческих решений состоят:

- в предотвращении риска, благодаря результатам прогноза динамического состояния КС;

- избежании риска — уклонении от воздействий, связанного с риском;

- снижении степени риска — уменьшении вероятности потерь и сокращение ожидаемого их объема;

- удержании допустимого уровня риска в условиях неопределенности различного рода путем ее оказания сопротивления деструктивным воздействиям с помощью встроенных и дополнительных средств РЭМ, РЭЗ и киберзащиты, ориентируясь на инновационные средства и их комплексирование для концентрации усилий РЭЗ соразмерно с опасностью КС и требованиям к динамической информационной устойчивости режимов зондирования РЛС;

- оказании скрытого информационного воздействия на динамическое состояние конфликтной ситуации, используя заготовки технико-информационного воздействия и психофизического давления на САУ комплекса РЭП и координацию их применения;

- выявлении признаков скрытого управления противником функционированием САУуст и радиоэлектронное противодействие ему;

- поиске субъектом управления возможных решений в условиях неопределенности высокого уровня, используя накопленные знания, опыт и свои креативно-рефлексивные способности.

При этом принимаются во внимание различия способов целедостижения для внутреннего и внешнего управлений, а также:

- особенности применения: логико-оптимального для условий определенности в случае простых КС и рисков; логико-лингвистического и/или экспертного и эвристического методов поиска решения для условий неопределенности в случае сложных и непредвиденных КС, а также трудно формализуемых задач целеполагания [10 – 12];

- интегрирование методов решения управленческих задач этого уровня управления в зависимости от условий наблюдения.

Распределение ограниченных ресурсов осуществляется по схеме «цель – действия – необходимый ресурс» с выполнением требования минимизации ресурсных затрат. Решение ресурсных задач связано с двумя основными аспектами выбором тактик, их ресурса для внутреннего или/и внешнего управлений с учетом состояния, динамики КС и распределением ресурсов РЭЗ. Трудность решения связана с тем, что на практике для достижения поставленных целей требуются различные ресурсы, количество которых ограничено. Нельзя допустить несоответствия между целями $САУ_{уст}$ и ее ресурсами, которые необходимы для их достижения. В противном случае возникает необходимость поиска ресурсного компромисса. Достичь снижения объема требуемых ресурсов возможно отбором наиболее эффективных отдельных стратегических задач РЭЗ, их тактик и комплексирования их наиболее эффективных ресурсов с учетом возможного применения одних и тех же тактик.

Специфика процессов этого уровня также состоит в зависимости процессов рационального выбора на ближнюю перспективу тактик и распределения их ресурсов от вида выбранной цели на верхнем уровне, состояния и динамики текущей КС.

Целеполагание на нижнем уровне управления

Особенности целеполагания на этом уровне связаны с обеспечением кратко временной информационной стабильности режимов зондирования РЛС:

перестройкой структуры $САУ_{уст}$, на текущий период времени, реализующей выбранных тактик с регулирование режимов и параметров назначенных средств РЭМ, РЭЗ та информационного противодействия;

контролем и анализом результатов управляющих воздействий, а также инициализации устранения отклонений их от выбранной цели путем корректировки методов выбора и распределения ресурсов, затрат ресурсов и времени принятия решения или смены стратегической цели.

Особую роль на этом этапе играет контроль фактического состояния устойчивости объекта управления в результате выполнения внешних и внутренних управляющих воздействий в перестроенной $САУ_{уст}$. Следует отметить специфику процессов перестройки структуры РЭЗ в САУуст и контроля результатов целеполагания от вида выбранной на верхнем уровне цели

По результатам последовательных оперативных сравнений рассогласований фактических состояний объекта управления с целевыми $\left| S^{Ц} - S^{Ф} \right|$, ресурсных затрат, результатов анализа накопленных данных о применяемой стратегии РЭП и прогнозов изменений КС осуществляются смены стратегических целей и строятся траектории внутреннего и внешнего управления состоянием и динамикой КС для достижения главной цели РЭЗ.

Важной особенностью оценки соответствия фактических показателей эффективности управления ожидаемым при целеполагании является применение широко распространенных на практике характерных индикаторов эффективности работы применяемых средств РЭМ и РЭЗ [2, 8, 16]. Индикаторные показатели позволяют измерить вклад этих средств (в увязке с показателями эффективности управления целеполаганием на иерархических уровнях управления) в достижение целей стратегии управления РЭЗ.

Выводы

Для повышения и обеспечения информационной устойчивости режимов зондирования обзорной РЛС в условиях ее подавления управляемыми активными помехами и мешающими информационными воздействиями системно проанализированы особенности способов и средств управления процессами целеполагания в структуре специализированной системы автоматизированного управления и на этапах ее функционировании. Они разнообразны и связаны с повышением уровней формализации и интеллектуализации ее контуров внутреннего и внешнего управлений динамическим состоянием конфликтных ситуаций. Это, в свою очередь, позволит получить большую обоснованность и оперативность принимаемых управляющих решений при дефиците времени на их принятие, уменьшение ошибок целеполагания для различных конфликтных ситуаций. При этом учитывается соответствие целей управления информационной устойчивостью текущего режима зондирования конкретным конфликтным ситуациям, складывающимся в проблемных областях зоны обзора РЛС. Представленные способы и средства будут способствовать приданию, синтезируемым в ходе конфликта многоцелевым стратегиям и ситуационному закону управления процессами РЭЗ и координации действий желательных свойств.

Важным инструментом частичной формализации управления целеполаганием является предложенный вариант базовой многоцелевой стратегии прогнозирующего управления процессами РЭЗ, при этом принимаются во внимание различия целей и процессов управления целеполаганием для внутреннего и внешнего управлений. Базовая стратегия содержит направления РЭЗ с разными логиками процессов принятия управляющих решения и достижения поставленной цели РЭЗ в зависимости от свойств динамических состояний конфликтных ситуаций Она служит источником априорной информации для обоснования выбора целей, тактик и их ресурсов.

Для полного определения критериев качества управления целеполаганием требуется задания иерархически связанной системы соответствующих показателей эффективности и методики их расчета. Полученные результаты при этом будут входить в основные положения такой методики с учетом определения зон допустимых потерь динамической устойчивости объекта управления, а также предупреждающих возникновение критических и катастрофических рассогласований фактических значений показателей эффективности управления с требуемыми.

Список литературы:

1. Конфликтно-устойчивые радиоэлектронные системы. Методы анализа и синтеза / Ю.А. Астапенко, С.Н. Вайпан, В.С. Верба [и др.]. Москва : Радиотехника, 2015. 312 с.
2. Радиоэлектронные системы: Основы построения и теория : справочник. Изд. 2-е, перераб. и доп. ; под. ред. Я.Д. Ширмана. Москва : Радиотехника, 2007. 512 с.
3. Информационное противоборство и радиоэлектронная борьба в сете-центрических войнах начала XXI века / С.И. Макаренко. СПб. : Наукоемкие технологии, 2017. 546 с.
4. Козирацкий Ю.Л. Модели информационного конфликта средств поиска обнаружения. Москва : Радиотехника, 2013. 232 с.
5. Канцедал В.М., Могила А.А.. Структура автоматизованої системи управління інформаційною стійкістю наземної оглядової РЛС в умовах активних завад // XVI міжнар. наук. конф. Харк. нац. ун-ту Повітряних Сил імені Івана Кожедуба "Новітні технології – для захисту повітряного простору" : тези доповідей, 15 – 16 квітня 2020 року. Харків : ХНУПС ім. І. Кожедуба, 2020. С. 334. Интернет ссылка http://www.hups.mil.gov.ua/assets/doc/science/conference/16/xvi-conf-hnups.pdf
6. Канцедал В.М., Могила А.А.. Структура автоматизованої системи управління інформаційною стійкістю наземної оглядової РЛС в умовах активних завад // Системи озброєння і військова техніка. 2020. № 1 (61). С. 82 – 95. Харків : ХНУПС ім. І. Кожедуба, Интернет ссылка https://journal-hnups.com.ua/index.php/soivt/article/view/245
7. Kantsedal V., Mogyla A. A Multifactorial Approach to Building a System for Automated Control of Radar Information Stability // 2020 IEEE Ukrainian Microwave Week (MRRS) Kharkov, Ukraine, September 21 – 25, Volume 2, pages 373-378. Интернет ссылка https://drive.google.com/file/d/1rnRSc1SV_I6hJ--uhjkQPhxZ6FDzlLY8/view?usp=sharing (Пароль для распаковки zip-файла сборника трудов совпадает с именем файла -«UkrMW-2020».)
8. Основы построения радиолокационных станций радиотехнических войск : учебник / В.Н. Тяпкин, А.Н. Фомин, Е.Н. [и др.] ; под общ. ред. В.Н. Тяпкина. Красноярск : Сиб. федер. ун-т. 2011. 536 с.

9. Гончаренко В.А. Концептуальные основы построения устойчивых к воздействиям автоматизированных систем специального назначения на основе адаптивных технологий // Наукоемкие технологии в космических исследованиях Земли. 2018. Т.10, № 4. С. 38– 74.

10. Лукьянова Л. М. Целеполагание, анализ и синтез целей в сложных системах, модели и методы моделирования // Известия РАИ. Теория и системы управления. 2007. № 5. С. 100-113. Источник: http://naukarus.com/tselepolaganie-analiz-i-sintez-tseley-v-slozhnyh-sistemah-modeli-i-metody-modelirovaniya

11. Лукьянова Л. М. Логико-лингвистическое моделирование целеполагания в сложных системах. Интернет-ресурс: http://ojs.philosophy.spbu.ru/index.php/lphs/article/view/233/234

12. Заде Л.А. Основы нового подхода к анализу сложных систем и процессов принятия решений // Математика сегодня. Москва : Знание, 1974.

13. Дружинин В.В., Конторов Д.С. Введение в теорию конфликта. Москва : Радио и связь, 1989. 288 с.

14. Мишин В. М. Исследование систем управления. Москва : ЮНИТИ, 2012. 527 с.

15. Теория управления (дополнительные главы) : учеб. пособие ; под. ред. Д. А. Новикова. Москва : ЛЕНАНД, 2019. 552 с.].

16. Круглова Н. Ю. Антикризисное управление : учеб. пособие. 3-е издание. Москва : КноРус, 2013. 400 с. https://www.moscowbooks.ru/book/662061/

17. Интеллектуальное ядро системы поддержки принятия решений / В.П.Осипов [и др.] // Препринты ИПМ им. М.В.Келдыша. 2018. № 205. 23 с. doi:10.20948/prepr-2018-205 URL: http://library.keldysh.ru/preprint.asp?id=2018-205

18. Розенберг И. Н. Интеллектуальное управление// Современные технологии управления. ISSN 2226-9339. №4 (76). Номер статьи: 7608. Дата публикации: 2017-04-10. Режим доступа: https://sovman.ru/article/7608/

19. Бортник Б.И., Стожко Н.Ю., Судакова Н.П. Оценка компетенций: формализация и формалистика // Современные проблемы науки и образования. 2017. № 4. URL: http://www.science-education.ru/ru/article/view?id=26693 (дата обращения: 14.07.2020).

20. Веремей Е.И. Когнитивная реализация оптимизационного подхода к синтезу законов управления подвижными объектами // Санкт-Петербургский гос. ун-т, 2016. https://cyberleninka.ru/article/n/kognitivnaya-realizatsiya-optimizatsionnogo-podhoda-k-sintezu-zakonov-upravleniya- podvizhnymi-obektami

21. Кравченко В.Н., Филипишин И.В. Целеполагание в системе управления развитием предприятия; http://dspace.nbuv.gov.ua/bitstream/handle/123456789/39651/10-Kravchenko.pdf?sequence=1

22. Коврига С.В. Методические и аналитические основы когнитивного подхода к SWOT-analysis // Проблемы управления. 2005. №5. С. 58–63.

23. Авдеева К., Коврига С. Подход к постановке задач управления на когнитивной модели ситуации для стратегического мониторинга // УБС. 2016. Вып.59, 120–146 ubs856.pdf.

24. Новиков Д.А., Чхартишвили А.Г. Рефлексия и управление: математические модели. Москва : Изд-во физ.-мат. лит., 2013. 412 с.

Поступила в редколлегию 04.11.2021

Сведения об авторах:

Канцедал Валерий Михайлович – канд. техн. наук, Институт радиофизики и электроники им. А.Я. Усикова НАН Украины, старший научный сотрудник, Харьков; Украина; e-mail: Vkantsedal9@gmail.com; ORSID: http://orcid.org/0000-0003-4008-917X

Могила Анатолий Андреевич – канд. физ.-мат. наук, Институт радиофизики и электроники им. А.Я. Усикова НАН Украины, старший научный сотрудник, заведующий отделом; Харьков; Украина; e-mail: moganat1196@gmail.com, ORSID: http://orcid.org/0000-0002-1726-6265.

УДК 621.396.96, 621.397.48:004.932.2 **DOI:10.30837/rt.2021.4.207.11**

В.М. КАРТАШОВ, д-р техн. наук, В.О. ПОСОШЕНКО, канд. техн. наук,
В.І. КОЛІСНИК, А.І. КАПУСТА, М.В. РИБНИКОВ, Є.В. ПЕРШИН, В.О. КІЗКА

КОМПЛЕКСУВАННЯ ІНФОРМАЦІЙНИХ КАНАЛІВ СИСТЕМ ВИЯВЛЕННЯ ТА СПОСТЕРЕЖЕННЯ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ З ПОЗИЦІЙ ТЕОРІЇ СТАТИСТИЧНИХ РІШЕНЬ

Вступ

В даний час безпілотні літальні апарати (БПЛА) забезпечують виконання широкого спектру корисних для людства завдань, але з іншого боку, вони представляють серйозну загрозу в господарській, військовій та інших областях діяльності людини [1]. Труднощі спостереження БПЛА з використанням сучасних технічних засобів, а також їх відносно невисока вартість призводять до розширення сфери протиправних дій з використанням БПЛА [2]. Тому захист різних об'єктів від БПЛА – серйозне науково-технічне завдання сучасності.

Останнім часом застосування БПЛА істотно збагатило та розширило методи вирішення різноманітних господарських та інших завдань, а також міцно увійшло в тактику дій військових підрозділів. Аналіз, виконаний в роботах [1, 2], показує, що найбільш складними щодо виявлення та протидії виявляються малі БПЛА – малогабаритні та нешвидкі. Природно, що літальні апарати цього класу є також найбільш складними цілями для системи виявлення та спостереження в зоні критично важливого об'єкту інфраструктури, що охороняється [3]. Дана обставина обумовлена низкою додаткових чинників, які ускладнюють виконання ефективної протидії відповідних систем по відношенню до малих БПЛА. Це, перш за все [4, 5]:

– використання в конструкції БПЛА пластикових і композитних матеріалів, що слабо відображають і розсіюють електромагнітне випромінювання (ЕМВ);

– використання «рваних» (з періодичним зависанням або різким зниженням швидкості) і високоманеврових (наприклад, «змійка») видів траєкторії переміщення та режимів польоту;

– використання для організації управління БПЛА не виділених командних радіоліній управління (КРУ), побудованих на основі окремих спеціальних засобів зв'язку, а застосування вже існуючої інфраструктури – систем зв'язку мобільних операторів і точок доступу Wi-Fi.

При вирішенні завдань виявлення, розпізнавання та вимірювання просторових координат БПЛА в даний час найбільш часто використовують радіолокаційні, акустичні, оптичні та інфрачервоні методи і засоби [10, 11].

Кожен із зазначених методів має свої переваги та недоліки, характеризується певним діапазоном дальності, але жоден з них не дозволяє вирішити задачу самостійно з достатньою ефективністю [3].

Оскільки області можливостей різних методів не збігаються, то на практиці часто реалізується передумова спільного використання систем різного виду для більш ефективного вирішення досить складного завдання виявлення та розпізнавання БПЛА [6 – 13].

Проаналізуємо відомі в літературі комплексні системи, які використовуються для виявлення БПЛА. В [14] описана мультисенсорна система, призначена для виявлення БПЛА та вимірювання їх просторових координат. Комплексна система включає активний і пасивний радіолокаційні й оптичний канали. Обробка інформації в системі реалізується шляхом зіставлення одержуваних даних – результатів виявлення та вимірювання просторових координат спостережуваних цілей. Спочатку реалізується самостійне виявлення цілей в використовуваних інформаційних каналах, далі виконується зіставлення та поєднання результатів виявлення за належністю до певної цілі. Алгоритм дозволяє виявити

які рішення відповідають корисним цілям, а які представляють собою помилкову тривогу. Визначався також внесок кожного інформаційного каналу в виявлення. У системі реалізований також алгоритм комплексування даних в процесі вимірювання просторових координат об'єктів.

Публікація [15] присвячена дослідженню об'єднання інформації радіолокаційного, акустичного й оптичного інформаційних каналів для виявлення, класифікації спостережуваних БПЛА та вимірювання їх розташування. Інтегрована система здійснює вимір кутових координат – азимута та кута місця з похибкою відповідно 1,5 і 2,5 град.

Інтегрування активного радіолокаційного та пасивного акустичного локаційних каналів дозволило забезпечити зменшення ймовірності помилкових тривог виявлення, а комплексування зображень, що формуються в видимому й інфрачервоному діапазонах (інфрачервоне зображення отримують в короткохвильовому інфрачервоному діапазоні (SWIR)), забезпечує більш швидке та достовірне виявлення БПЛА при наявності перешкод і диму на зображеннях інформаційних каналів.

В роботі [16] описано виявлення та спостереження БПЛА в межах міста. Воно реалізовано з використанням статичних і мобільних пунктів, що включають радіолокаційні, акустичні, оптичні технічні засоби, а також лідар. При пеленгації та визначенні місцезнаходження об'єктів багатоканальною акустичною системою застосовувався тріангуляційний метод. Комплексна система забезпечує впевнене виявлення БПЛА та визначення їх місця розташування із середньою помилкою в 7 м.

Процес об'єднання інформації різних інформаційних каналів, призначених для виявлення дронів, в ряді робіт реалізований з використанням засобів штучного інтелекту.

В роботі [17] для виявлення БПЛА застосовується радіолокаційна станція, а також сукупність акустичних датчиків. Отримана інформація подається на вхід попередньо навченого алгоритму глибокого навчання, який складається з трьох MLP. В описаній системі виконується виявлення БПЛА з малою вірогідністю хибних тривог, реалізоване в польових умовах.

Недороге технічне устаткування використовувалося в комплексній системі [18], яка включає радіолокаційний, акустичний, видимий і інфрачервоний канали. Для об'єднання одержуваної в зазначених каналах інформації застосовується фільтр Калмана; далі інформація подається на класифікатор найближчого сусіда для винесення рішення по завданню розпізнавання. Система забезпечує спостереження повітряних об'єктів на відстані до 800 м.

В [19] оптичний канал спостереження включає 30 відеокамер, а акустичний канал – три мікрофони. В оптичному й акустичному інформаційних каналах реалізовані класифікатори SVM, навчені відповідно за зображеннями і акустичними сигналами БПЛА. Розглянута комплексна система успішно функціонує при польотах БПЛА різних видів на висотах до 100 м і на відстанях до 200 м.

Кількість публікацій, в яких описуються методи і технічні засоби, спрямовані на виявлення БПЛА на тлі різноманітних перешкод, з кожним роком збільшується. Розглядаються різні методи прийому, обробки сигналів, їх подальшого аналізу, досліджуються комплексні системи, засновані на використанні різних мультисенсорних датчиків [5]. Але при цьому інтегральна ефективність комплексних систем виявлення БПЛА на практиці є недостатньою. Проблема ефективного спостереження та протидії БПЛА (особливо малим БПЛА), є складною, багатогранною, до теперішнього часу не має задовільного рішення і вимагає комплексного, системного підходу при її вирішенні [2].

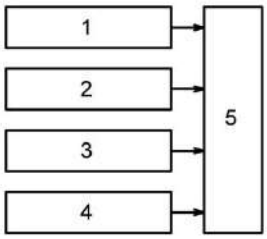
Дана стаття присвячена розгляду методів синтезу нових, більш ефективних алгоритмів комплексування радіолокаційних, акустичних, оптичних і інфрачервоних інформаційних каналів інтегральних систем виявлення та розпізнавання БПЛА, які виконуються з позицій статистичної теорії оптимізації радіосистем.

Постановка завдання комплексної обробки інформації при вимірюванні координат і параметрів руху БПЛА

Внаслідок статистичного характеру перешкод і збурюючих впливів, що надходять на вхід інформаційної системи, статистичного характеру похибок вимірювання координат об'єктів і помилкових рішень, прийнятих при виявленні і розпізнаванні цілей, в процесі комплексування інформаційних каналів систем спостереження БПЛА доцільно використовувати методи статистичної теорії оптимізації радіосистем і теорії статистичних рішень [20 – 23].

Припустимо, що комплексна система спостереження БПЛА включає l інформаційних каналів (наприклад, активний і пасивний радіолокаційні, оптичний, акустичний канали), кожен з яких містить на виході вимірювач. При цьому вимірювальний пристрій i-го каналу оцінює якийсь інформативний параметр $\lambda_{it}, i = 1,\dots,l$, або деяку функцію від нього (просторову координату або параметр руху БПЛА). Вимірювані параметри в сукупності утворюють векторний l-мірний випадковий процес $\lambda_t = (\lambda_{1t},\dots,\lambda_{lt}),\ t \geq 0$. На виході вимірників каналів отримуємо дані в вигляді оцінок інформативних параметрів і похибок їх вимірювань. Сукупності оцінок розглядаються також як реалізації деякого векторного l-мірного випадкового процесу $y_t = (y_{1t},...,y_{lt})$.

Узагальнена структурна схема системи комплексної обробки сигналів інформаційних каналів, які використовуються для спостереження БПЛА, наведена на рис.1.



1 – активний і пасивний радіолокаційні канали, 2 – акустичний канал, 3 – оптичний канал, 4 – інфрачервоний канал, 5 – пристрій обробки і прийняття рішення

Рис. 1. Узагальнена структурна схема системи комплексної обробки сигналів інформаційних каналів, які використовуються для спостереження БПЛА

Основним завданням даної комплексної системи спостереження БПЛА є формування оптимальної (в байєсовому сенсі) оцінки $\nu*_{t\tau} = (\nu*_{1t\tau},\dots,\nu*_{lt\tau})$ векторного параметру λ_τ в деякий заданий момент часу $\tau > o$ за результатами спостереження реалізацій сигналів інформаційних каналів y_t протягом відрізка часу $[0, t]$.

Між поточним моментом часу τ і тривалістю часу спостереження t можливі такі співвідношення: $\tau < t$, $\tau = t$, $\tau > t$. Вважаємо, що завдання оптимального комплексування l вимірників розглядається на етапі оцінювання, коли виконується умова $\tau = t$.

У статистичній теорії радіосистем є два основні підходи до комплексування використовуваних інформаційних засобів [21, 23]. У першому випадку завдання комплексування вирішується на етапі первинної обробки інформації, у другому – на етапі вторинної обробки одержуваної інформації (на етапі об'єднання рішень). Вторинною в теорії радіосистем називають обробку, яка здійснюється на основі результатів сформованих оцінок і рішень після виконання необхідної обробки вхідних сигналів, що поступають (сигнали фільтрації, посилення, детектування). На етапі вторинної обробки виконуються завдання зав'язування та виявлення траєкторій літальних апаратів, їх згладжування і т.д. В процесі третинної обробки за допомогою математичних методів відбуваються доповнення й уточнення отриманої раніше інформації, забезпечується підвищення стійкості супроводу

цілей і повноти даних, а також здійснюється оптимізація функціонування угруповання радіолокаційних та інших технічних засобів з метою отримання максимальної якості радіолокаційної інформації при мінімальних витратах ресурсів, з урахуванням особливостей обстановки, що спостерігається, і наявних коштів [22, 23].

Зауважимо, що при постановці і рішенні в загальному вигляді завдання оптимізації не має принципового значення як комплексуються вимірювачі інтегральної системи: на етапі первинної чи вторинної обробки. У першому випадку під вхідним коливанням y_t розуміється векторний процес, який спостерігається на входах вимірювальних пристроїв інформаційних каналів, у другому випадку – це випадковий процес на виходах вимірників каналів. Специфіка й особливості вирішення конкретного завдання комплексування будуть проявлятися при виборі адекватних математичних моделей вхідного процесу y_t. У разі комплексування на етапі первинної обробки вхідний процес y_t системи містить інформаційні сигнали й інформативні параметри λ_t, що приймаються на тлі випадкових шумів і перешкод; на етапі вторинної обробки роль адитивних шумів виконують похибки сформованих в каналах результатів вимірювань. Ефективність комплексування й оптимізації в значній мірі буде визначатися ступенем адекватності обраної математичної моделі y_t реальному векторному вхідному процесу, що спостерігається.

Функцію векторного оптимального оператора системи, або векторну вирішальну функцію, з використанням якої за вхідними реалізаціями $y_0^t = \{\gamma_{1v}, ..., \gamma_{lv}, 0 \le v \le t\}$ векторного процесу на часовому відрізку [0, t], формується в момент часу $\tau > 0$ оцінка $\nu_{t\tau} = f_\tau(y_0^t)$ параметру λ_τ, тобто $\nu_{it\tau} = f_{i\tau}(\gamma_0^t),\ i = 1, ..., l,$ уявімо вектор-функцією $f_\tau = (f_{1\tau}, \dots, f_{l\tau})$. Якщо конкретизувати функцію втрат $c(\lambda, d)$, де λ і d – l-мірні вектори, то в результаті мінімізації апостеріорного ризику

$$\min_{\delta_\tau} \mathbf{M}\{c[\lambda_\tau, f_\tau, (y_0^t)]|y_0^t\} = \mathbf{M}\{c[\lambda_\tau, f_\tau^*(y_0^t)]|y_0^t\} \tag{1}$$

може бути сформовано байєсове рішення $\nu_{t\tau}^* = f_\tau^*(y_0^t)$ – оптимальна відповідно до заданого критерію оцінка шуканого параметра λ_τ. Вираз для отримання в результаті виконаних операцій шуканої оцінки визначає, в кінцевому підсумку, загальні алгоритми оптимального комплексування вимірників інформаційних каналів.

У разі $\tau = t$ маємо поточну фільтраційну оцінку ν_{tt}^*, вираз для отримання якої визначає оптимальну структуру фільтраційної системи комплексування інформаційних каналів (ФСКІК). При $\tau \ne t$ одержувані оцінки $\nu_{t\tau}^*$ визначають структури інтерполяційної $(\tau < t)$ та екстраполяційної $(\tau > t)$ систем оптимального комплексування інформаційних каналів.

Ефективність функціонування оптимальної комплексної системи визначається отриманим баєсовим середнім ризиком:

$$\overline{r}_{t\tau}^* = \mathbf{MM}\{c[\lambda_\tau, f_\tau^*(y_0^t)]|y_0^t\} = \mathbf{M}c[\lambda_\tau, f_\tau^*(y_0^t)].$$

У разі використання квадратичної функції втрат (функції штрафів) можна записати

$$c(\lambda, \nu) = \sum_{i=1}^{l} (\lambda_i - \nu_i)^2, \tag{2}$$

а оптимальні відповідно до заданого критерію оцінки векторного параметра будуть визначатися співвідношенням

$$\nu_{t\tau}^* = \mathbf{M}(\boldsymbol{\lambda_\tau}|\boldsymbol{y_0^t}), \tau > t, \tau < t, \tag{3}$$

Якщо визначити апостеріорні щільності ймовірностей оцінюваних інформаційних параметрів $\lambda_{i\tau}, i = 1, \dots, l$ у вигляді

$$w(\lambda_{i\tau}|y_0^t) \equiv p_{t\tau}(\lambda_i),\ \tau > t, \tau < t,\ i = 1, \dots, l, \tag{4}$$

то з використанням (2) можна записати вираз для формування оцінки

$$\nu_{it\tau}^* = f_{i\tau}^*(y_0^t) = \int_{-\infty}^{\infty} \lambda_i p_{t\tau}(\lambda_i) d\lambda_i, \tau > t, \tau < t\ ,\ i = 1, \dots, l. \tag{5}$$

Для квадратичної функції втрат (2) скалярний, інтегральний баєсовий ризик буде визначатися співвідношенням

$$\overline{r}^*_{t\tau} = \sum_{i=1}^{l} \mathbf{M}[\lambda_{i\tau} - f^*_{i\tau}(y_0^t)]^2\,,\ \tau > t, \tau < t$$

у вигляді суми середніх квадратів помилок оцінювання складових векторного параметра $\lambda_{i\tau}$. Середньоквадратичні похибки оцінювання кожного скалярного параметра

$$\sigma_{it\tau} = \sqrt{\mathbf{M}[\lambda_{i\tau} - f^*_{i\tau}(y_0^t)]^2},\ \tau > t, \tau < t,\ i = 1, \ldots, l \tag{6}$$

визначають найменші помилки вимірювання, одержувані в разі оптимального комплексування інформаційних каналів. Порівнюючи похибки σ_{itt} в (6), отримані для $\tau = t$, із середньоквадратичними помилками сформованих раніше оцінок y_{it}

$$\sigma_{it} = \sqrt{\mathbf{M}(\lambda_{it} - y_{it})^2},\ i = 1, \ldots, l, \tag{7}$$

можна зробити висновки про якість функціонування оптимальної комплексної системи (про якість комплексування інформації).

Ефективність комплексної обробки інформації може бути підвищена, якщо в основу функціонування системи покласти використання інтерполяційної оцінки $v^*_{t\tau}$, $\tau<$t. Пояснюється це тим, що формування додаткової реалізації вхідного сигналу не може погіршити якості оптимальної оцінки, а може тільки поліпшити її, відповідно для середньоквадратичних похибок інтерполяції $\sigma_{it\tau}$, $\tau<$t, і фільтрації $\sigma_{it\tau}$ справедлива нерівність $\sigma_{it\tau} \le \sigma_{i\tau\tau}$, $\tau<$t, $i = 1, \ldots, l$.

Ефективність функціонування даної системи комплексування дозволяє пояснити два крайні характерні випадки. В першому випадку вимірювані параметри $\lambda_{i\tau}$, $i = 1, \ldots, l$, вважаємо статистично незалежними, як і супроводжуючі їх адитивні перешкоди, які спостерігаються в реалізаціях $\gamma^t_{i0} = \{\gamma_{iv} 0 \le v \le t\}, i = 1, \ldots, l,$ що спостерігаються в реалізаціях, які також вважаємо статистично незалежними по i. Для характерної ситуації, що розглядається, можна показати з використанням теореми Байєса, що для апостеріорного розподілів (3) мають місце співвідношення [12]

$$w(\lambda_{i\tau}|y_0^t) = w(\lambda_{i\tau}|y_{i0}^t) \equiv p_{it\tau}(\lambda_i),\ \tau > t, \tau < t, i = 1, \ldots, l.$$

Відповідно для оцінок (5) можна записати

$$v^*_{it\tau} = f^*_{i\tau}(\gamma^t_{i0}) = \int_{-\infty}^{\infty} \lambda_i p_{it\tau}(\lambda_i) d\lambda_i,\ \tau > t, \tau < t,\ i = 1, \ldots, l.$$

В даному випадку оптимальна система комплексування розпадається на l не зв'язаних між собою окремих вимірників інформаційних каналів.

В іншому характерному випадку, при

$$\lambda_{it} \equiv \lambda_t\ \ i = 1, \ldots, l, \tag{8}$$

у всіх інформаційних каналах оцінюється один і той же скалярний параметр λ_t. Внаслідок структурної та інформаційної надмірності результатів вимірювань середньоквадратична похибка σ_{tt} оцінювання параметра λ_t з використанням комплексної оптимальної системи фільтраційного типу буде задовольняти виразу

$$\sigma_{tt} \le \sigma_{jt} = \min_{i \in [1, \ldots l]} \{\sigma_{it}\},\ \ t > 0, \tag{9}$$

в якому середньоквадратичні помилки окремих вимірників σ_{it} визначаються співвідношенням (7). Рівність в співвідношенні (9) матиме місце в тому випадку, коли шуми

вимірювань для всіх каналів комплексної системи будуть однаковими, а кожен j-й вимірювач комплексної системи формує оптимальну фільтраційну оцінку параметра λ_t.

Моделі вхідних сигналів

Для більш детального розгляду загальних алгоритмів оптимального комплексування інформаційних каналів систем спостереження БПЛА необхідно визначити моделі спостереження, тобто моделі вхідних процесів для використовуваних канальних вимірників $\gamma_{1t},\dots,\gamma_{lt}$ інформативних параметрів $\lambda_{1t},\dots,\lambda_{lt}$, а також для похибок одержуваних на їх виходах результатів вимірювань, які виконують роль випадкових адитивних завадових коливань.

Зауважимо, що в загальному випадку при синтезі оптимальних пристроїв початковими є два положення: чітке математичне формулювання завдання, що враховує всі апріорні відомості (вибір моделей сигналів і перешкод); вибір математично продуктивного критерію оптимальності відповідно до фізичного змісту та цільовим змістом практичного завдання, що розв'язується [21].

Сформуємо в досить загальному вигляді рівняння спостереження для вхідних процесів інформаційних каналів

$$\gamma_{it} = F_i(\lambda_{it},\eta_{it},t) + \xi_{it},\ i = 1,\dots,l, \tag{10}$$

де η_{it},ξ_{it} – перешкоджаючі коливання, що маскують вхідні сигнали та спотворюють інформативні параметри λ_{it}, що треба знайти. Функції $F_i(\ i = 1,\dots,l)$ визначають характер взаємодії перешкоди η_{it} і спостережуваного векторного сигналу, що містить параметр λ_{it}, який може бути адитивним або мультиплікативним. Функції $F_i(\ i = 1,\dots,l)$ будемо вважати відомими. Адитивні перешкоди ξ_{it} та η_{it} в (10) в загальному випадку мають різні статистичні характеристики. Якщо перешкоди η_{it} мають адитивний характер, то функції F_i будуть мати такий вигляд

$$F_i(\lambda_{it},\eta_{it},t) = s_i(\lambda_{it},t) + \eta_{it},\ i = 1,\dots,l,$$

де $s_i(\ i = 1,\dots,l)$ – детерміновані функції. Якщо $s_i(\lambda_{it},t) \equiv \lambda_{it},\eta_{it} \equiv 0,\ i = 1,\dots,l,$ то отримуємо досить просту модель вхідних інформаційних процесів,$\gamma_{it} = \lambda_{it} + \xi_{it},\ i = 1,\dots,l,$ яка часто застосовується на практиці. Має місце також така модель

$$\gamma_{it} = \begin{cases} s(\lambda_t,t) + \xi_{it}, i = 1,\dots,m, \\ \lambda_t + \xi_{it}, i = m+1,\dots,l \end{cases}, \tag{11}$$

яка є окремим випадком розглянутої моделі (10). Модель (11) застосовується в тому випадку, коли λ_t – скалярний параметр, при цьому в частині інформаційних каналів виконується фільтрація сигналу $s(\lambda_t,t)$, а в іншій частині каналів здійснюється оцінювання його параметра.

Залежно від використовуваних технічних засобів в інформаційних каналах і типів вимірників (цифрові, аналогові) вихідні дані каналів, що формуються, надходять безперервно або дискретно в часі та мають безперервну або дискретну безліч своїх значень. У цьому випадку доцільно використовувати в якості адекватних математичних моделей інформативних параметрів і маючих місце перешкод марківські випадкові процеси. Вони адекватно описують широкий клас реальних процесів і сигналів, а також досить зручні в процесі проведення теоретичних математичних (аналітичних) досліджень. У процесі синтезу оптимальних комплексних фільтраційних, інтерполяційних і екстраполяційних систем виміру параметрів на практиці в різних областях широко застосовуються добре розроблені математичні методи теорії оцінювання векторних марківських процесів [12, 13, 23].

Співвідношення для синтезу та аналізу систем

На практиці досить широко поширений випадок, коли компоненти спостережуваного векторного процесу змінюються в часі безперервно і визначаються співвідношенням (9) при $t \geq 0$. Інформативні параметри $\lambda_{1t},\dots,\lambda_{lt}$ вхідних коливань і супроводжуючі їх перешкоди $\eta_{1t},\dots,\eta_{lt}$ (перешкоди з метою спрощення запису позначимо як $\eta_{it} \equiv \lambda_{l+i,t},\ i=1,\dots,l$) утворюють $2l$-мірний безперервний марківський процес $(\lambda_{1t},\dots,\lambda_{2lt}),\ t \geq 0,$ який характеризується в цьому випадку коефіцієнтами переносу $a_i(\lambda,t)$ і дифузії $b_{ij}(\lambda,t),\ i,j=1,\dots,2l;\ \lambda$ – $2l$-мірний вектор. Адитивні перешкоди ξ_{it} досить часто на практиці можуть бути апроксимовані білими гаусівськими шумами, для яких справедливо співвідношення

$$\mathbf{M}\xi_{it}\xi_{jt+\tau} = \begin{cases} \frac{N_{0i}}{2} f(\tau),\ i=j \\ 0,\ i \neq j. \end{cases} \tag{12}$$

Достатньою статистикою в розглянутих задачах синтезу оптимальних структур комплексних систем спостереження БПЛА може виступати апостеріорний розподіл ймовірностей спостережуваного інформаційного процесу. З використанням [21], можуть бути отримані вирази для апостеріорного розподілу параметрів

$$p_t(\lambda) = \omega(\lambda_{1t},\dots,\lambda_{2lt}|\gamma_{10}^t,\dots,\gamma_{l0}^t),$$

які представляються в симетризованій формі запису

$$p_i(\lambda) = \left[\zeta - \overline{\zeta}(p_t(\lambda))\right]p_t(\lambda), \tag{13}$$

де

$$\zeta = -\sum_{i=1}^{2l}\frac{\partial}{\partial\lambda_i}a_i(\lambda,t) + \frac{1}{2}\sum_{i,j=1}^{2l}\frac{\partial^2}{\partial\lambda_i\partial\lambda_j}b_{ij}(\lambda,t) + \sum_{i=1}^{l}\frac{2}{N_{0i}}F_i(\lambda_i,\lambda_{l+i},t)\left[y_{it} - \frac{1}{2}F_i(\lambda_i,\lambda_{l+i},t)\right];$$

$$\overline{\zeta}(p_t(\lambda)) = \sum_{i=1}^{l}\frac{2}{N_{0i}}\int_{-\infty}^{\infty}\dots\int_{-\infty}^{\infty}F_i(\lambda_i,\lambda_{l+i},t)\left[y_{it} - \frac{1}{2}F_i(\lambda_i,\lambda_{l+i},t)\right]p_t(\lambda)d\lambda_1\dots d\lambda_{2l}\,.$$

Вирази, що визначають формування оптимальних оцінок v_{itt}^* інформативних параметрів $\lambda_{it}, i=1,\dots,l,$ а також маючих місце перешкод $\lambda_{it}, i=l+1,\dots,2l,$ при використовуваних квадратичних функціях втрат мають вигляд

$$v_{itt}^* = \int_{\Theta}\lambda_i p_t(\lambda)\,d\lambda, i=1,\dots,2l. \tag{14}$$

Алгоритм формування розглянутих оцінок визначає структуру оптимальної ФСКІК і містить послідовність операцій, які в ній реалізуються.

На практиці досить широко використовується метод гаусівського наближення, що дозволяє конкретизувати вираз (13). В цьому випадку апостеріорна щільність ймовірностей інформативного параметра апроксимується багатовимірним гаусівським законом

$$p_t(\lambda) = (2\pi)^{-l}\,det^{-\frac{1}{2}}\left\|K_{ijt}\right\|\,exp\left\{-\frac{1}{2}\sum_{i,j=1}^{2l}h_{ijt}(\lambda_i - m_{it})\left(\lambda_j - m_{jt}\right)\right\}, \tag{15}$$

$$\text{де } \left\|h_{ijt}\right\| = \left\|K_{ijt}\right\|^{-1}.$$

Шляхом підстановки (15) в (13), можна отримати рівняння, що описують процедури багатовимірної нелінійної фільтрації в гаусівському наближенні [12]:

$$m_{it} = a_{it} + \sum_{n=1}^{l}\frac{2}{N_{0n}}(y_{nt} - F_{nt})\sum_{p=1}^{2l}K_{pi}\frac{\partial F_{nt}}{\partial\lambda_p}; \tag{16}$$

$$K_{ijt} = b_{ijt} + \sum_{n=1}^{2l} K_{njt} \frac{\partial a_{it}}{\partial \lambda_n} + \sum_{n=1}^{2l} K_{nit} \frac{\partial a_{jt}}{\partial \lambda_n} + \\ + \sum_{q=1}^{l} \frac{2}{N_{0q}} \left(\gamma_{qt} - F_{qt}\right) \sum_{n,p=1}^{2l} K_{njt} K_{pit} \frac{\partial^2 F_{qt}}{\partial \lambda_n \partial \lambda_p} - \\ - \sum_{q=1}^{l} \frac{2}{N_{0q}} \sum_{n,p=1}^{2l} K_{njt} K_{pit} \frac{\partial F_{qt}}{\partial \lambda_n} \frac{\partial F_{qt}}{\partial \lambda_p}, \tag{17}$$

де

$$\alpha_{it} = \alpha_i(\lambda, t)|\lambda = m_t, \ \ m_t = m_{1t}, \ldots, m_{2lt};$$

$$b_{ijt} = b_{ij}(\lambda, t)|\lambda = m_t, \ \ \mathrm{F}_{nt} = F_n\left(m_{nt}, m_{l+n,t}, t\right);$$

$$\frac{\partial^2 F_{qt}}{\partial \lambda_n \partial \lambda_p} = \frac{\partial^2 F_q(\lambda_q, \lambda_{l+q}, t)}{\partial \lambda_n \partial \lambda_p}\Bigg|_{\lambda_{l+q} = m_{l+q}, t}^{\lambda_q = m_{qt}}.$$

Апостеріорні середні m_{it}, одержувані з використанням виразів (16), (17), за умови досить великого співвідношення корисний сигнал-перешкода, що відповідає режиму роботи зі значною точністю, можна вважати приблизно рівними оптимальним оцінками (14) спостережуваних інформативних процесів: $m_{it} \approx \nu_{itt}^*, i = 1, \ldots, 2l$.

Вирази (16), (17) визначають структуру нелінійної системи ФСКІК, яка є квазіоптимальною. Якщо функції F_i в (10) є лінійними функціями марківських гаусівських процесів $\lambda_{it}, \eta_{it}, i = 1, \ldots, l$, то вирази (16), (17) визначають точне рішення задачі формування оцінок і описують оптимальну ФСКІК, в основі якої лежить використання багатовимірного лінійного фільтра Калмана.

Якість функціонування синтезованої інтегральної системи інформаційних каналів характеризується апостеріорними дисперсіями K_{iit}, які при використанні гаусівського наближення описуються виразами (16), (15). Середньоквадратичні похибки оцінювання інформативних параметрів

$$\sigma_{itt} = \sqrt{\mathbf{M}[\lambda_{it} - f_{it}^*(y_0^t)]^2} \approx \sqrt{\mathbf{M}K_{iit}}, \ \ i = 1, \ldots, l. \tag{18}$$

У приватному лінійному випадку, коли комплексна система будується на основі фільтра Калмана, апостеріорні дисперсії записуються у вигляді

$$\sigma_{itt} = \sqrt{K_{iit}}, \ \ i = 1, \ldots, l. \tag{19}$$

Співвідношення для комплексування виявлювачів

Інформаційна і структурна види надмірності сигналів, які надходять в багатоканальних системах, дозволяють при використанні комплексування підвищити не тільки точність результатів вимірювань, але й якісні показники виявлення спостережуваних об'єктів. Розглянемо загальну задачу оптимального комплексування виявлювачів БПЛА інформаційних каналів.

Вважаючи, що маємо l канальних виявлювачів, розглянемо задачу їх оптимального комплексування в інтегрованій системі на етапах первинної та вторинної обробки інформації.

При розгляді комплексування окремих виявлювачів на етапі первинної обробки необхідно математично описати спостережуваний процес γ_{it} на вході кожного з каналів $(i = 1, \ldots, l)$. Модель спостереження в цьому випадку має вигляд

$$\gamma_{it} = \theta s_{it} + \eta_{it} + \xi_{it}; \ \theta = 0{,}1; 0 \le t \le T; i = 1, \ldots, l, \tag{20}$$

де відповідно $s_{it}, \eta_{it}, \xi_{it}$ – корисні сигнали, зовнішні перешкоджаючі коливання і власні внутрішні шуми канальних виявлювачів. Вхідні сигнали можуть бути як однаковими: $s_{it} = s_t, i = 1, \ldots, l,$, так и різними. Навіть в тому випадку, якщо корисні сигнали надходять

в канали від одного сенсора, то на входах схем виявлення вони можуть мати різні значення параметрів, зокрема, як, наприклад, значення часу запізнювання в багатопозиційних системах. Крім того, сигнали в ряді каналів можуть бути відсутніми: $s_{it} \equiv 0, 0 \le t \le T$, тобто деякі канали призначені для компенсації перешкод і є «перешкоджаючими».

Якщо щільності розподілу ймовірностей перешкод, шумів і сигналів в (22) апріорі відомі, то розглянута задача виявлення зводиться до формування відношення правдоподібності. Якщо корисні сигнали s_{it} і перешкоди η_{it} стохастичні, з відомими розподілами ймовірностей, а шуми ξ_{it} є білими гаусівськими, то логарифм відношення правдоподібності записується у вигляді [21]

$$z = \sum_{i=1}^{l} \frac{1}{N_{0i}} \left[2 \int_0^T (\hat{s}_{it} + \hat{\eta}_{it1} + \hat{\eta}_{it0})(\gamma_{it} - \hat{\eta}_{it0})\, d * t - \int_0^T (\hat{s}_{it} + \hat{\eta}_{it1} - \hat{\eta}_{it0})^2 dt \right] \qquad (21)$$

Перший член у виразі (23) – інтеграл Ito, а

$$\hat{s}_{it} = \mathbf{M}[s_{it} | y_0^T, \theta = 1]; \quad \hat{\eta}_{it\theta} = \mathbf{M}[\eta_{it} | y_0^T, \theta], \ \theta = 0{,}1,$$

являють собою апостеріорні математичні очікування. Вони є баєсівськими оцінками сигналів і перешкод.

Отримані вирази визначають рішення загальної задачі синтезу оптимальної системи комплексування виявлювачів на етапі первинної обробки інформації. Аналіз якості роботи такої системи полягає в розрахунку ймовірностей правильного виявлення та помилкової тривоги.

Висновки

1. Проаналізовано відомі в літературі комплексні системи спостереження БПЛА, реалізовані у вигляді сукупності взаємопов'язаних між собою інформаційних каналів, системні і технічні рішення, що використовуються в них, апаратно-програмні засоби, методи обробки многомодальних інформаційних сигналів і зображень. Зроблено висновок, що відомі системи виявлення БПЛА і існуючі методи обробки інформації не дозволяють вирішувати актуальні для практики завдання, які полягають, наприклад, у захисті життєво важливих елементів інфраструктури з необхідною ефективністю, тож це потребує їх подальшого вдосконалення.

Завдання спостереження й ефективної протидії БПЛА (особливо малим БПЛА) до теперішнього часу не має задовільного рішення, є складною, багатогранною, та вимагає комплексного, системного підходу з використанням сучасних наукових методів при її вирішенні.

2. Статистична теорія оптимізації радіоелектронних систем, заснована на використанні марківських випадкових процесів, в гаусівському наближенні, дозволяє здійснювати оптимізацію структур обробки сигналів інтегрованих комплексних систем виявлення та спостереження безпілотних літальних апаратів, що включають інформаційні канали, побудовані з використанням різних фізичних сенсорів.

Використання теорії радіосистем дозволяє синтезувати алгоритми оптимальної обробки канальних інформаційних сигналів при вирішенні задач виявлення, вимірювання просторових координат, розпізнавання типів БПЛА. За допомогою теорії здійснюється оптимальний синтез пристроїв первинної обробки сигналів в кожному каналі, а також об'єднання інформації канальних сигналів. Такий підхід дозволяє синтезувати оптимальну (відповідно до обраного критерію якості) комплексну систему обробки інформації, що забезпечує отримання максимальної кількості інформації з векторного процесу, що спостерігається на входах інформаційних каналів.

Показана можливість побудови оптимального детектора БПЛА з використанням пізньої стратегії об'єднання інформації на рівні рішень, прийнятих в окремих каналах системи (на етапі вторинної обробки інформації).

3. Використання запропонованих підходів і методів комплексної обробки й об'єднання многомодальної інформації в інтегрованих системах спостереження БПЛА забезпечить гнучке поєднання різної інформації, одержуваної по використовуваних каналах, з урахуванням можливостей наявних технічних засобів і специфіки вирішуваних завдань.

4. Актуальні завдання даного напрямку – синтез оптимальних структур і алгоритмів комплексної обробки многомодальних сигналів із використанням математичних засобів оптимізації теорії радіосистем, евристичний синтез комплексних інтегрованих систем обробки, а також оцінка ефективності різних варіантів побудови систем і порівняння їх показників на практиці.

Список літератури:

1. Кошкин Р. Беспилотные авиационные системы. Москва : Стратегические приоритеты, 2016.
2. Макаренко С., Тимошенко А., Васильченко А. Противодействие беспилотным летательным аппаратам. Ч. 1. Беспилотный летательный аппарат как объект обнаружения и поражения // Системы управления, связи и безопасности. 2020. №1. С. 109-146, doi: 10.24411/2410-9916-2020-10105.
3. Oleynikov V., Zubkov O., Kartashov V., Koryttsev I., Sheiko S. and Babkin S. Experimental Estimation of Direction Finding to Unmanned Air Vehicles Algorithms Efficiency by Their Acoustic Emission // 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), 2019, pp. 175-178, doi: 10.1109/PICST47496.2019.9061337.
4. Sergiyenko O., Rodríguez-Quiñonez J. Developing and applying optoelectronics in machine vision // IGI Global, 2016.
5. Rivas-Lopez M., Sergiyenko O., Flores-Fuentes W. and Rodríguez-Quiñonez J. Optoelectronics in machine vision-based theories and applications // Hershey, PA: Engineering Science Reference (an imprint of IGI Global), 2019. pp. 373-391.
6. Murrieta-Rico F. et al. Pulse width influence in fast frequency measurements using rational approximations // Measurement, vol. 86. pp. 67-78, 2016, doi: 10.1016/j.measurement. 2016.02.032.
7. Avalos-Gonzalez D. et al. Constraints definition and application optimization based on geometric analysis of the frequency measurement method by pulse coincidence // Measurement. 2018. Vol. 126. P. 184-193, 2018, doi: 10.1016/j.measurement. 2018. 05. 025.
8. Ivanov M. et al. Individual Scans Fusion in Virtual Knowledge Base for Navigation of Mobile Robotic Group with 3D TVS // IECON 2018 – 44th Annual Conference of the IEEE Industrial Electronics Society. 2018. P. 3187-3192, doi: 10.1109/IECON.2018.8591442.
9. Avalos-Gonzalez D. et al. Application of Fast Frequency Shift Measurement Method for INS in Navigation of Drones // IECON 2018 – 44th Annual Conference of the IEEE Industrial Electronics Society, 2018, pp. 3159-3164, doi: 10.1109/IECON.2018.8591377.
10. Карташов В., Куля Д., Кушнир М., Толстых Ю. Выбор модели изменения скорости звука для оптимального линейного фильтра систем радиоакустического зондирования атмосферы // Радиотехника. 173. С. 63-78. Режим доступа: https://openarchive.nure.ua/handle/document/1130.
11. . Карташов В., Куля Д., Пащенко С. Алгоритм автоматического слежения за изменением параметра сигнала радиоакустических информационных систем // Восточно-Европейский журнал корпоративных технологий. 2012. Вып. 4, №. 9(58), pp. 57-61. Режим доступа: http://journals.uran.ua/eejet/article/view/5747
12. Кащеев Б., Прошкин Е., Лагутин М. Дистанционные методы и средства изучения процессов в атмосфере Земли. Харьков : Бизнес Информ, 2002.
13. Сосулин Ю.В. Теоретические основы радиолокации и радионавигации. Москва : Радио и связь, 1992.
14. W. Koch, J. Koller and M. Ulmke. Ground target tracking and road map extraction // ISPRS Journal of Photogrammetry and Remote Sensing, vol. 61, no. 3-4, pp. 197-208, 2006, doi: 10.1016/j.isprsjprs.2006.09.013.
15. F. Kloeppel et al. Multimodal UAV detection: study of various intrusion scenarios // Electro-Optical Remote Sensing XI, 2017, doi: 10.1117/12.2278212.
16. F. Giovanneschi et al. An adaptive sensing approach for the detection of small UAV: first investigation of static sensor network and moving sensor platform // Signal Processing, Sensor/Information Fusion, and Target Recognition XXVII, 2018, doi: 10.1117/12.2304758.
17. S. Park et al. Combination of radar and audio sensors for identification of rotor-type Unmanned Aerial Vehicles (UAVs) // 2015 IEEE SENSORS, 2015, pp. 1-4, doi: 10.1109/ICSENS.2015.7370533.
18. G. L. Charvat, A. J. Fenn and B. T. Perry. The MIT IAP radar course: Build a small radar system capable of sensing range, Doppler, and synthetic aperture (SAR) imaging // 2012 IEEE Radar Conference, 2012, pp. 0138-0144, doi: 10.1109/RADAR.2012.6212126.

19. H. Liu, Z. Wei, Y. Chen, J. Pan, L. Lin and Y. Ren. Drone Detection Based on an Audio-Assisted Camera Array // 2017 IEEE Third International Conference on Multimedia Big Data (BigMM), pp. 402-406, 2017, doi: 10.1109/bigmm.2017.57.

20. Басов О., Карпов А. Анализ стратегий и методов объединения многомодальной информации // Обработка информации и управления. 2015. Вып. 2. С. 7-14, , doi: 10.15217/issn1684-8853.2015.2.7.

21. Фалькович С., Хомяков Е. Статистическая теория измерительных радиосистем. Москва : Радио и связь, 1981.

22. Ширман Ю., Манжос В. Теория и методика обработки радиолокационной информации на фоне помех. Москва : Радио и связь, 1981.

Надійшла до редколегії 28.10.2021

Відомості про авторів:

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

Посошенко Віталій Олександрович – Харківський національний університет радіоелектроніки, канд. техн. наук, доцент кафедри медіаінженерії та інформаційних радіоелектронних систем, Україна, e-mail: vitalii.pososhenko@nure.ua, ORCID: https://orcid.org/0000-0003-0867-9161

Колісник Вікторія Іванівна – Харківський національний університет радіоелектроніки, асистент кафедри медіаінженерії та інформаційних радіоелектронних систем, Україна, e-mail: viktoriia.kolisnyk@nure.ua, ORCID: https://orcid.org/0000-0002-2382-9124

Капуста Анастасія Ігорівна – Харківський національний університет радіоелектроніки, аспірант кафедри медіаінженерії та інформаційних радіоелектронних систем, Україна, e-mail: anastasiia.kapusta@nure.ua, ORCID: https://orcid.org/0000-0003-2206-1552

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

Першин Євгеній Васильович – Харківський національний університет радіоелектроніки, аспірант кафедри медіаінженерії та інформаційних радіоелектронних систем, Україна, e-mail: yevhenii.pershyn@nure.ua, ORCID: https://orcid.org/0000-0002-4573-9381

Кізка Валерій Олександрович – Харківський національний університет радіоелектроніки, асистент кафедри медіаінженерії та інформаційних радіоелектронних систем, Україна, e-mail: kizkavaleri@gmail.com, ORCID: https://orcid.org/0000-0003-1007-5295

УДК 621.396.96, 621.397.48 **DOI:10.30837/rt.2021.4.207.12**

В.М. КАРТАШОВ, д-р техн. наук, В.А. ПОСОШЕНКО, канд. техн. наук,
В.И. КОЛЕСНИК, И.С. СЕЛЕЗНЕВ, Р.И. БОБНЕВ, А.И. КАПУСТА

ОБНАРУЖЕНИЕ РАДИОЛОКАЦИОННЫХ СИГНАЛОВ, РАССЕЯННЫХ НА АКУСТИЧЕСКИХ ВОЗМУЩЕНИЯХ, СОЗДАВАЕМЫХ БПЛА

Введение

В настоящее время беспилотные летательные аппараты (БПЛА) становятся важным фактором народно-хозяйственной и военной деятельности всех технологически развитых государств. Поэтому задача мониторинга окружающего воздушного пространства с целью обнаружения и оценивания характеристик БПЛА, безусловно, является актуальной.

Существующие методы (каналы) наблюдения за БПЛА [1 – 8] достаточно разнообразны и используют различные демаскирующие признаки, делающие его заметным на фоне окружающей обстановки. Среди подобных методов значительный интерес представляет активная радиолокация БПЛА, которую характеризуют всепогодность, значительная дальность обнаружения, пространственное разрешение по дальности и угловым координатам, помехоустойчивость, независимость от времени суток и т.д.

В свою очередь, существующие технологии изготовления БПЛА позволяют минимально задействовать металлические компоненты, широко использовать композитные материалы и специальные покрытия, что резко снижает ЭПР планера как радиолокационной цели. Поэтому при активной радиолокации БПЛА на первый план выходит анализ сигнала, рассеянного не конструкцией планера, а пакетом акустических волн, возникающих в процессе функционирования аппарата.

Экспериментально установлено, что БПЛА излучают акустические волны в диапазоне частот от сотен герц до 15 кГц [8, 9]. Для получения рассеянного радиосигнала от пакета акустических колебаний требуется выполнение условий Брэгга [8]:

$$\lambda_e = 2 \cdot \lambda_s \cdot \sin\theta,$$

где λ_e – длина электромагнитной волны; λ_s – длина волны акустических сигналов; θ – угол между фронтом акустической волны и направлением распространения зондирующих радиоволн.

Соответственно, диапазон рассеянных радиоволн с интенсивностью, достаточной для решения задач их обнаружения и оценивания, простирается от λ_e=6,8 м (что соответствует частоте акустического излучения f_s=100 Гц, λ_s=3,4 м) до λ_e=5,4 см (что соответствует частоте акустического сигнала f_s=15 кГц, λ_s=2,7 см).

В работах [7 – 32] показано, что структура и параметры акустических возмущений, созданных БПЛА в атмосфере, зависят от его вида, формы, количества двигателей и режимов их работы, количества и формы несущих винтов и т.д. Кроме того, экспериментальные исследования структуры и параметров звукового поля БПЛА выявили, что спектры его акустического излучения содержат ярко выраженные гармоники, имеющие частоты кратные частотам вращения винтов. Основной тон находится в полосе от 80 до 240 Гц, а количество гармоник может варьироваться от 10 до 40. При этом спектр акустического сигнала простирается до 15 кГц [8, 9].

В режиме полета спектральные линии акустического излучения размываются вследствие различия режимов работы (частоты вращения) двигателей при компенсации дестабилизирующих факторов движения в турбулентной атмосфере. По мере прохождения акустической волной определенного расстояния в атмосфере от источника излучения происходят заметные ослабления ее высокочастотных составляющих, что обусловлено дисперсионными свойства-

ми среды, а также изменчивостью характеристик направленности излучения в полосе частот [9]. Поэтому интенсивность акустических колебаний, зависящая от угла наблюдения, имеет случайный характер с неким законом распределения вероятностей.

Кроме того, анализ литературных источников, приведенных выше, позволяет предположить наличие дополнительного фактора нелинейного взаимодействия зондирующих радиоволн с динамичным звуковым полем, которое создает БПЛА, что приводит к появлению эффектов паразитной амплитудной и угловой модуляции даже в условиях излучения монохроматического и неизменного по интенсивности зондирующего радиосигнала. Эта гипотеза еще требует глубокой теоретической и экспериментальной проработки. Но уже сейчас ее необходимо учитывать в практической деятельности.

Таким образом, совокупный радиосигнал, рассеянный областью пространства, возмущенной акустическим излучением БПЛА, будет представлять собой временную последовательность колебаний с различными и случайными текущими амплитудами, частотами и временем запаздывания. Поэтому на входе приемника РЛС будет присутствовать смесь шумовых колебаний, нешумовых помех и полезного сигнала с непредсказуемой заранее комплексной огибающей. При этом полагается известной эффективная полоса частот ΔF с определенной центральной частотой f_0.

В этой связи значительный интерес представляют задачи обнаружения и оценивания сигналов с минимальной априорной информацией об их комплексной огибающей и времени существования на интервале наблюдения. Такого рода задачи помимо радиолокации распределенных целей (например, пространственно протяженных объектов) характерны для медико-биологических исследований, радиоастрономии, гидролокации и т.д.

Для решения подобных задач уже неприменимы известные процедуры оптимальной или квазиоптимальной фильтрации, а потому требуется поиск наиболее общих алгоритмов обработки, основанных на статистическом различии чистого шума и аддитивной смеси "сигнал плюс шум".

Алгоритм обнаружения

Разработку таких алгоритмов удобно проводить на основе так называемого "энергетического подхода", который базируется на анализе оценок приведенной к шумам энергии регистрируемых колебаний на интервале наблюдения в предположении гауссового характера шумов [33]. Причем это ограничение не является чрезмерным по двум причинам: во-первых, решение задачи для гауссовых шумов открывает путь для совершенствования алгоритмов обработки в условиях воздействия шумов с иными статистическими характеристиками, а во-вторых, в настоящее время получили развитие процедуры нормализации негауссовых процессов.

Рассмотрим следующую модель аддитивной смеси $\dot{Y}(t)$ полезного сигнала $\dot{S}(t)$ и шума $\dot{N}(t)$:

$$\dot{Y}(t) = \dot{S}(t) + \dot{N}(t), \text{ где } \dot{S}(t) = \sum_{i=1}^{k} \dot{S}_i(t) = \sum_{i=1}^{k} \dot{b}_i \cdot \dot{X}_i(t), \text{ где}$$

$\dot{S}_i(t) = \dot{b}_i \dot{X}_i(t)$ – i-й относительно начала пакета импульсный сигнал в пачке из K импульсов; $\dot{b}_i$ – подлежащий оцениванию произвольный амплитудный множитель i-го импульса; $\dot{X}_i(t)$ – известный с точностью до фазы φ_i опорный сигнал, соответствующий зондирующему радиоимпульсу

$$x_i(t) = \mathrm{Re}\{\dot{X}_i(t) e^{j\omega_o t}\}.$$

Корреляционная матрица шумов $\underline{\dot{\Phi}}(t_1, t_2)$, составленная для одного элемента дальности по различным периодам зондирующих радиоимпульсов, имеет вид

$$\dot{\underline{\Phi}}(t_1,t_2)=\delta(t_1-t_2)\dot{\underline{N}},$$

где $\delta(r)$ – дельта-функция.

Поскольку мгновенные значения шума на выходе приемника независимы в моменты, отстоящие на время, равное периоду зондирующих сигналов, матрица $\dot{\underline{\Phi}}'(t_1,t_2)$ размерности $(k\times k)$ – диагональная: $\dot{\underline{\Phi}}'(t_1,t_2)$=diag N_{ii}, $N_{ii}=\sigma_{ii}^2\Delta F$, где σ_{ii}^2 – дисперсия шумовых колебаний в *i*-м периоде зондирующих сигналов; ΔF – эффективная полоса пропускания узкополосного тракта принимаемых колебаний.

В матричном виде модель аддитивной смеси сигнала с шумом будет иметь вид

$$\dot{\underline{Y}}(t)=\dot{\underline{X}}(t,\dot{\underline{b}})+\dot{\underline{N}}(t),$$

где элементы матриц соответственно равны значениям аддитивной смеси "сигнал плюс шум", полезного радиосигнала с неизвестной амплитудой и начальной фазой, шумовых колебаний на фиксированном элементе дальности в каждом из *k* периодов (Тз) зондирующих сигналов на интервале наблюдения $(T2-T1)=k\cdot T_3$.

На основе этой модели в силу значительной неопределенности в представлении пакетов отражений требуемый алгоритм их совместного обнаружения и оценивания максимальных значений, регистрируемых полезных сигналов на ограниченном интервале наблюдения можно отыскивать в рамках процедур обработки в соответствии с критерием максимума отношения правдоподобия:

$$l=(p_{cn}(\dot{\underline{Y}}/\dot{\underline{b}}))/(p_n(\dot{\underline{Y}}/\dot{\underline{b}}))=\text{kexp}\{(-1/2)\int_{T1}^{T2}\int_{T1}^{T2}[\dot{\underline{Y}}^{*T}(t_1)-\dot{\underline{X}}^{*T}(t_1,\dot{\underline{b}}]\dot{\underline{\Psi}}(t_1,t_2)[\dot{\underline{Y}}(t_2)-\dot{\underline{X}}(t_2,\dot{\underline{b}})]dt_1dt_2\}/$$

$$(\text{k exp}\{(-1/2)\int_{T1}^{T2}\int_{T1}^{T2}[\dot{\underline{Y}}^{*T}(t_1)\ \dot{\underline{\Psi}}(t_1,t_2)\dot{\underline{Y}}(t_2)dt_1dt_2\})=\max$$

при $\dot{\underline{b}}=\dot{\underline{b}}_{opt}$, где p_{cn} и p_n – соответственно функционалы многомерной плотности вероятности гауссовых случайных величин для аддитивной смеси сигнала с шумом и чистого шума. Матрица $\dot{\underline{\Psi}}(t_1,t_2)$ находится путем решения интегрального уравнения

$$\int_{T1}^{T2}\dot{\underline{\Phi}}(t_1,t_2)\dot{\underline{\Psi}}(t_2,t_3)dt_2=\underline{I}\delta(t_1-t_3),$$

где $\underline{I}$ – единичная диагональная матрица; T2-T1 – временной интервал, соответствующий одному элементу дальности.

Оценки $\dot{\underline{b}}^1$ энергетических параметров $\dot{\underline{b}}$ получены в виде $\dot{\underline{b}}^1=\underline{Q}^{-1}\dot{\underline{Z}}$, где $\dot{\underline{Z}}=\{\dot{Z}_i,i=1,k\}$ – вектор приведенных к шумам результатов обработки входного колебания $\dot{Y}(t)$ в фильтре, согласованном с опорным сигналом $\dot{X}(t)$ в каждом *i*-м периоде зондов на произвольном элементе дальности на интервале наблюдения (T2 – T1):

$\dot{Z}_i=(1/N_{ii}\int_{T1}^{T2}\dot{Y}_i(t)\dot{X}_i(t)dt=\dot{Z}_{0i}/N_{ii}$, $\underline{Q}$ – диагональная матрица с элементами $q_{11},q_{22},....,q_{kk}$,

где $q_{ii}=2Э_i/N_{ii}$, $2Э=\int_{T1}^{T2}/\dot{X}_i/^2dt$ – энергия опорного сигнала $x_i(t)$ на интервале наблюдения (T2 – T1).

Подставив полученные оценки $\dot{\underline{b}}^{1}$ в выражение для ln(l), получим искомый алгоритм функционирования устройства накопления энергии нешумового сигнала $\dot{S}(t)$, представляющего собой пакет радиоотражений с флуктуирующими амплитудами импульсов, оптимальный в смысле максимума отношения правдоподобия:

$$\ln(l) = (1/2)\sum_{i=1}^{k} / \dot{Z}_i /^2 (1/q_{ii}) = (1/2)\sum_{i} / \dot{Z}_{ni} /^2, \text{ где } \dot{Z}_{ni} = \dot{Z}_{0i} / (2\,Э_i N_{ii})^{1/2}.$$

Следует отметить, что при отсутствии полезного сигнала $\dot{S}(t)$ значения математического ожидания M[ln(l)] и дисперсия D[ln(l)] – постоянны. Поэтому синтезированный алгоритм обнаружения оказывается инвариантным к интенсивности помех.

Очевидно, что случайная величина $\xi = \ln(l)$, получаемая как сумма квадратов реализаций нормально распределенной величины $\dot{Z}$ в зависимости от наличия или отсутствия полезного (нешумового) сигнала $\dot{S}(t)$, во входном случайном процессе $\dot{Y}(t)$ имеет либо центральное $P_ц(\xi)$, либо нецентральное $p_{нц}(\xi)$ распределение $\chi^2{}_{N_{св.}}$ с $N_{св.} = 2kr$ степенями свободы и параметром нецентральности $\lambda \geq 0$, где r – количество отсчетов значений $Z^2{}_i[n]$ на интервале наблюдения T2 – T1.

Известные плотности вероятности [34]:

$$p_ц(\xi) = (1/(2^{n/2}\Gamma(n/2))\xi^{n/2-1}e^{-\xi/2} \quad (1)$$

для $\xi > 0$, где n – количество степеней свободы; Γ(x) – гамма-функция Эйлера; $P_ц(\xi)$=0 для $\xi \leq 0$;

$$p_{нц}(\xi) = (e^{-0.5(\xi+\lambda)}\xi^{(n/2)-1}\sum_{j=0}^{\infty}(\lambda\xi/4)^j)/(j!\Gamma(j+n/2)))/2^{n/2} \quad (2)$$

для $\xi \geq 0$, где λ – параметр нецентральности, позволяют анализировать качественные показатели синтезированного обнаружителя для различных значений параметров λ, k, а также оценить оптимальное значение интервала наблюдения $\Delta T = kT_з$, ($T_з$ – период следования зондирующих радиоимпульсов) для малых входных соотношений сигнал/шум и определить в соответствии с выбранным критерием обнаружения пороговое значение $\ln(l)_{пор.}$, в сравнении с которым величины ln(l) выносится решение о наличии нешумового сигнала $\dot{S}(t)$ на интервале наблюдения ΔT.

Полученное выражение для ln(l) синтезированного обнаружителя пакетов радиоотражений, замаскированных шумами, позволяет применить различные способы его практической реализации. В этой связи представляется перспективным путь разделения исходного анализируемого колебания $\dot{Y}(t)$ на квадратурные составляющие $\dot{Y}_c(t)$ и $\dot{Y}_s(t)$. По цифровым отсчетам результата их согласованной фильтрации вычисляются оценки текущих значений дисперсий $\sigma^2{}_{ci}, \sigma^2{}_{si}$ в квадратурных каналах в окрестности каждой i-й текущей выборки $Z_0[i]_{c,s}$ на интервале наблюдения, после чего формируется искомая оценка вида

$$\ln(l) = S_\Sigma = \sum_{j=1}^{kr}(Z^2{}_0[j]_c/\sigma^2{}_{cj} + Z^2{}_0[j]_s/\sigma^2{}_{sj}).$$

Такой подход позволил получить оценку $(\ln(l))^1$ без детектирования огибающей узкополосного случайного процесса $\dot{Y}(t)$ (что важно при малых соотношениях сигнал/шум),

формировать фазовременную характеристику (ФВХ) пакета радиоотражений, оценить текущие значения $N_{ic,s}, \sigma^2_{ic,s}$ в квадратурных каналах по нормально распределенным отсчетам $Z_0[i]_{c,s}$, в то время как отсчеты полного вектора $Z_0[i]_{c,s}$ могут быть распределены по любому из следующих законов: Рэлея, Райса, Бэкмана или Хойта [35].

Таким образом, предложенная методика обработки на фоне гауссовых шумов принимаемого колебания $\dot{Y}(t)$ в квадратурах позволяет предложить более общий энергетический подход к задачам обнаружения и оценивания сигналов с априори неизвестной комплексной огибающей. замаскированных нестационарными, негауссовыми шумами, а также нешумовыми помехами. Во многом такой подход основан на разнообразных процедурах нормализации либо квадратурных составляющих $\dot{Y}_c(t)$ и $\dot{Y}_s(t)$ полного вектора, либо результата их согласованной фильтрации $\dot{Z}_0(t)_c, \dot{Z}_0(t)_s$ для непрерывных и для дискретных сигналов.

Известные аналитические выражения [33] для центрального и нецентрального распределения хи-квадрат (1) и (2) позволяют получить численные оценки пороговой величины $\ln(l)_{пор.}$ и вероятностные характеристики обнаружителя для текущих значений числа степеней свободы Nсв. и параметра нецентральности $\lambda \geq 0$ в зависимости от выбранного критерия обнаружения.

Рассмотрим на рис. 1 схематичное изображение дифференциальных плотностей вероятности вида (1) и (2). Пусть случайная величина ln(l)=x имеет либо центральное (кривая 1), либо нецентральное (кривая 2) распределение хи-квадрат с Nсв. степенями свободы.

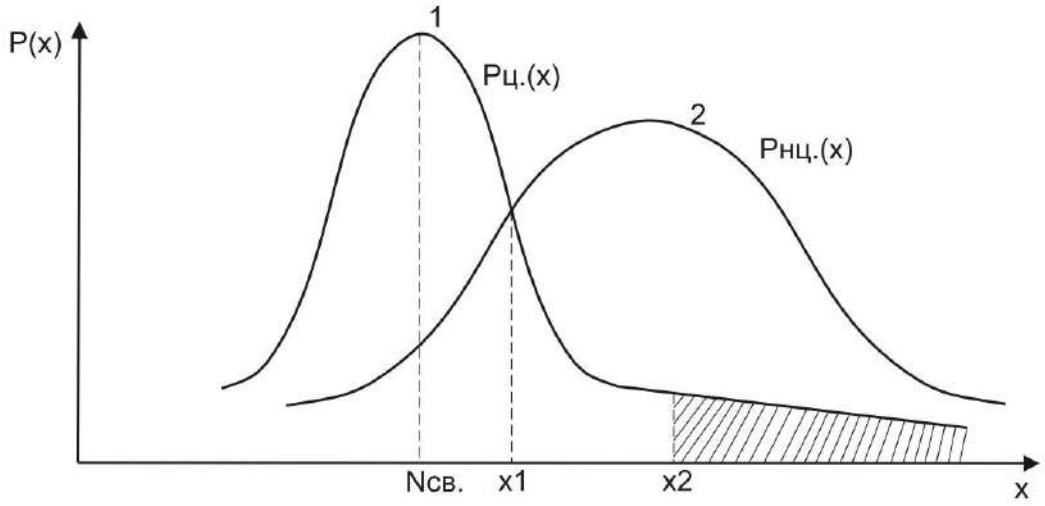


Рис. 1. Дифференциальные плотности центрального Рц(x) и нецентрального Рнц(x) распределений $\chi^2_{N_{св.}}$ с Nсв. степенями свободы

Задача выбора порогового значения ln(l)пор.=xпор. решается на основе анализа известных аналитических выражений (1) и (2), описывающих данные плотности вероятности. Выбор любой точки на оси X (например x1) в качестве порогового значения xпор. означает, что при зафиксированных значениях Nсв. и параметра нецентральности λ возможно вычислить ключевые значения вероятностей правильного обнаружения Рправ., пропусков цели Рпр.ц., ложной тревоги Рл.т. следующим образом:

$$P_{прав.} = \int_{x1}^{\infty} p_{н.ц.}(x) \cdot dx; \quad p_{пр.ц.} = \int_{0}^{x1} p_{н.ц.}(x) \cdot dx; \quad p_{л.т.} = \int_{x1}^{\infty} p_{ц}(x) \cdot dx.$$

Выбирая то или иное значение x1, можно в широких пределах изменять соотношение между численными оценками указанных вероятностей в соответствии с решаемой задачей. Например, если требуется зафиксировать максимально допустимое значение вероятности ложной тревоги (заштрихованная площадь на рис.1), то в качестве порогового значения хпор. следует выбирать точку x2.

В любом случае при приеме радиосигналов с минимально регистрируемой энергией полезных сигналов вероятность правильного обнаружения

$$P_{прав.мин.} = \int_{N_{cd\,/}+\lambda}^{\infty} p_{н.ц.}(x) \cdot dx \approx 0.5.$$

С ростом энергетики принимаемых колебаний вероятность правильного обнаружения увеличивается.

Практическая реализация алгоритма обнаружения

Структурная схема приемной части регистратора радиосигналов, рассеянных на пакетах акустических колебаний БПЛА, показана на рис.2.

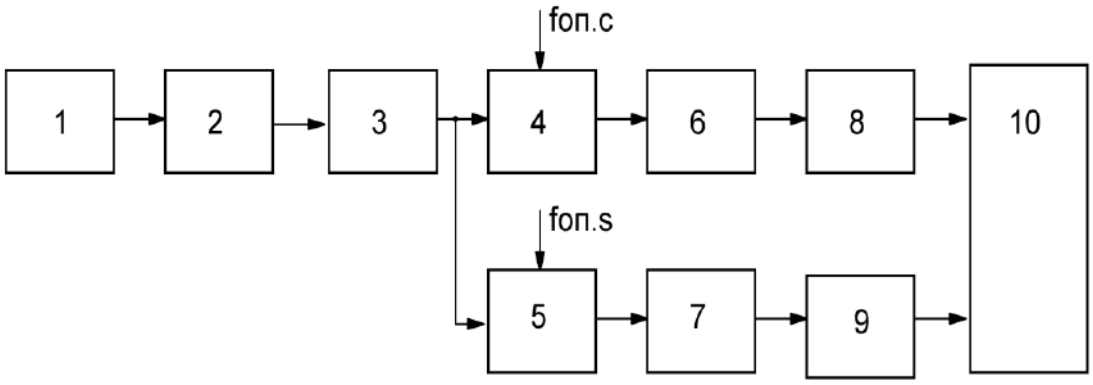


Рис. 2. Структурная схема приемной части регистратора БПЛА

На этой схеме приняты следующие обозначения:

1 – антенна;

2 – преселектор;

3 – малошумящий усилитель радиочастоты (МШУ);

4, 5 – смесители;

6, 7 – усилители низкой частоты (УНЧ);

8, 9 – АЦП;

10 – специализированное вычислительное устройство.

fоп.c, fоп.s – "косинусная" и "синусная" опорные частоты, равные несущей частоте зондирующих радиосигналов f0 и сдвинутые относительно друг друга на π/2;

Данная схема представляет собой высокочувствительный приемник прямого преобразования с двумя выходными квадратурными каналами в цифровом формате. Отсчеты с этих каналов поступают в специализированное вычислительное устройство или высокопроизводительную ЭВМ и обрабатываются в соответствии с алгоритмом, описанном выше.

В соответствии с этим алгоритмом в окрестности каждой текущей *i*-й выборки A*i* в каждом канале обработки условно "слева" и "справа" от нее (то есть, по выборкам предыстории и постистории) формируются оценки математического ожидания: $m_L = \frac{1}{k} \cdot \sum_{j=1}^{k} A_{i-j}$ и

$m_R = \frac{1}{k} \cdot \sum_{j=1}^{k} A_{i+j}$, где величина k характеризует глубину предыстории и постистории. Тогда текущую оценку дисперсии в окрестности выборки Ai получим из следующих соотношений:

$$D_L = \frac{1}{k-1} \cdot \sum_{j=1}^{k} (A_{i-j} - m_L)^2,\ D_R = \frac{1}{k-1} \cdot \sum_{j=1}^{k} (A_{i+j} \_ m_R)^2,\ D_i = \frac{D_L + D_R}{2}.$$

Теперь текущая оценка случайной величины ξ для i-й выборки получится такой: $\xi_i = \frac{A_i^2}{D_i}$.

В качестве наглядной иллюстрации на рис. 3 показана диаграмма текущих сумм $X_i = S_{\Sigma i} = (\ln l)_i$, распределенных на дискретных элементах дальности, где i – условный номер элемента на развертке дальности D.

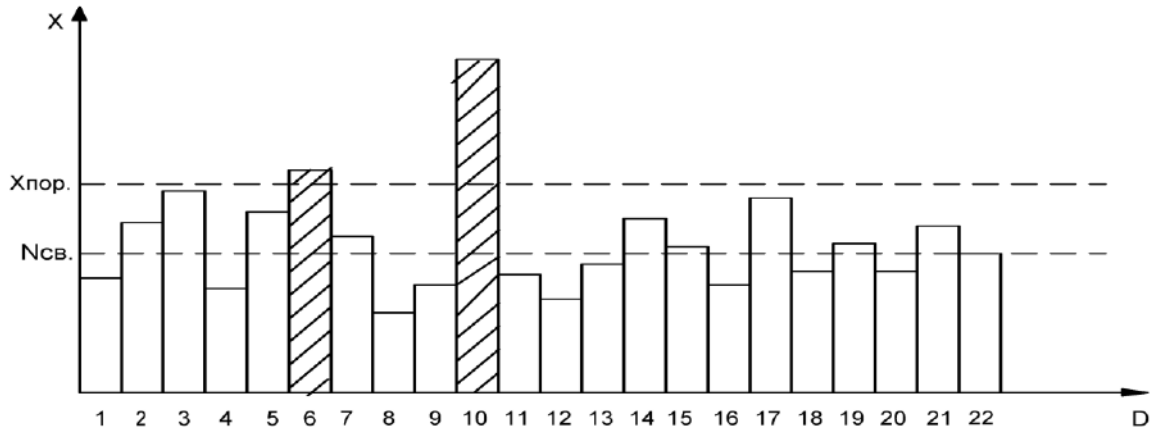


Рис. 3. Диаграмма, иллюстрирующая распределение на элементах дальности накопленной энергии, приведенной к шумам

Например, данная диаграмма показывает, что на элементах дальности с номерами (1…5), (7…9), (11…22) текущие суммы X_i не превышают пороговое значение Хпор. Поэтому принимается решение, что на этих дальностях отсутствует полезный сигнал с приемлемой энергетикой.

На элементах дальности с номерами 6 и 10 текущие значения X6 и X10 превышают пороговые значения. Следовательно, принимается решение, что на этих дальностях присутствуют интересующие нас объекты. Причем, с учетом специфики формирования оценок X_i по методу "скользящего окна", когда в каждом периоде зондирующих сигналов из суммы $S_{\Sigma i}$ вычитается первый элемент и к ней добавляется новый, ничего определенного о направленности процесса накопления сказать нельзя. Например, малое превышение порога на шестом элементе может означать либо начало полезной регистрации, либо близкое ее завершение. Значительное превышение порога на десятом элементе дальности означает, скорее всего, срединный этап процесса регистрации объекта.

Поэтому окончательный вывод о динамике процесса регистрации можно сделать лишь на этапе оценивания распределения нешумовой энергии на всем интервале наблюдения, который следует сразу за этапом обнаружения начала и окончания пакета радиоотражений на фиксированной дальности.

Выводы

Обнаружение БПЛА радиометодами представляет сложную научно-техническую задачу в силу малой эффективной поверхности рассеяния его планера. Поэтому перспективным представляется радиолокация атмосферных неоднородностей, которые создаются вследствие функционирования летательного аппарата.

В свою очередь, рассеянные на атмосферных возмущениях радиосигналы характеризуются большой априорной неопределенностью формы их комплексной огибающей. Это обстоятельство вынуждает проводить синтез алгоритма обработки принимаемых радиосигналов в рамках самых общих вероятностных подходов, основанных на статистических различиях чистого шума и аддитивной смеси "сигнал плюс шум". В этом смысле привлекательным видится так называемый "энергетический подход", заключающийся в получении текущих оценок энергии принимаемых колебаний на заданном интервале наблюдения в полосе частот, которая априори известна достаточно точно.

Для узкополосного случайного процесса подобные оценки рассматриваются как реализации случайной величины, имеющей распределение "хи-квадрат" с неким параметром нецентральности. В результате сравнения текущего значения параметра нецентральности с пороговым значением выносится решение о наличии или отсутствии нешумовой энергии на интервале наблюдения.

Синтезированный алгоритм является оптимальным в смысле максимума отношения правдоподобия, а также инвариантным к уровню шумовых колебаний. Его реализация возможна как на программном, так и преимущественно аппаратном уровнях.

Известные аналитические выражения для дифференциальной плотности вероятности распределения "хи-квадрат" позволяют получать качественные характеристики алгоритма обнаружения.

К его недостаткам следует отнести "неразборчивость" к нешумовым сигналам, попадающим в полосу пропускания узкополосного тракта радиоприемника, что является платой за наиболее общий подход к синтезу процедур обработки принимаемых радиосигналов.

Разделение обнаруженных сигналов на относящиеся к БПЛА или к сосредоточенным по спектру нешумовым помехам проводится на этапе оценивания и распознавания, который представляет отдельную задачу.

Список литературы:

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

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

3. Карташов В.М., Олейников В.Н., Леонидов В.И., Воронин В.В., Капуста А.И., Селезнев И.С., Першин Е.В. Комплексная обработка сигналов интегрированной системы наблюдения беспилотных летательных аппаратов с использованием целеуказания // Радіотехніка. 2020. Вип. 203. С. 148-161.

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

5. Макаренко С. И., Тимошенко А. В., Васильченко А. С. Анализ средств и способов противодействия беспилотным летательным аппаратам. Ч. 1. Беспилотный летательный аппарат как объект обнаружения и поражения // Системы управления, связи и безопасности. 2020. № 1. С. 109-146.

6. Molchanov P., Harmanny R.I., de Wit J.J., Egiazarian K., Astola J. Classification of small UAVs and birdsby micro-Doppler signatures // J. Microw. Wirel. Technol. 2014. 6:435–444.

7. Карташов В.М., Олейников В.Н., Шейко С.А., Бабкин С.И., Корытцев И.В., Зубков О.В., Анохин М.А. Информационные характеристики звукового излучения малых беспилотных летательных аппаратов // Радиотехника. 2017. Вып. 191. С. 181-187.

8. Красненко М.П. Акустическое зондирование атмосферы. Новосибирск : Наука СО, 1986. 167с.

9. В.М. Карташов, О.И. Харченко, В.А. Посошенко, В.И. Колесник, А.И. Капуста, А.Б. Егоров, Л.П. Тимошенко Обнаружение беспилотных летательных аппаратов с ипользованием рассеяния радиоволн на акустических возмущениях среды, создаваемых летательным аппаратом // Радіотехніка. 2021. Вип. 206.

10. Aker C., Kalkan S. Using deep networks for drone detection // Proceedings of the 2017 14th IEEEInternational Conference on Advanced Video and Signal Based Surveillance (AVSS); Lecce, Italy. 29 August–1September 2017. P. 1–6.

11.Теодорович Н.Н., Строганова С.М., Абрамов П.С. Способы обнаружения и борьбы с малогабаритными беспилотными летательными аппаратами // Интернет-журнал "Науковедение". 2017. Т.9, №1. http://naukovedenie.ru/PDF/13TVN117.pdf.

12. Даник Ю.В, Бугайов М.В. Аналіз ефективності виявлення тактичних безпілотних літальних апаратів пасивними та активними засобами спостереження // Зб. наук. праць ЖВІ ДУТ. Інформаційні системи'15. 2015. Вип.10. С.5-20.

13. Marino L. Experimental analysis of UAV-propellers noise // 16th AIAA/CEAS Aeroacoustics Conference. University «La Sapienza», Rome, Italy. American Institute of Aeronautics and Astronautics, 2010. P. 1-14.

14. Beel J. J. Anti-UAV Defense For Ground Forces and Hypervelocity Rocket Lethality Models. Monterey, California : Naval Postgr aduate School, 1992. P. 36–46.

15. .Moses A. Radar-based detection and identification for minia ture air vehicles / A. Moses, M.J.Rutherford, K.P. Valavanis // IEEE International Conference on Control Applications.

16. Даник Ю.Г., Пулеко І.В., Бугайов М.В. Виявлення безпілотник літальних апаратів на основі аналізу акустичних та радіолокаційних сигналів // Вісник ЖДТУ. 2014. № 4 (71). С.71- 80

17. Самохин В. Ф. Экспериментальное исследование источников шумности беспилотного летательного аппарата с винто-кольцевым движителем в толкающей компоновке / В.Ф. Самохин, С.П. Остроухов, .А. Мошков // Электронный журнал «Труды МАИ». 2012. Вып. № 70. С.1–24.

18. Zaslavsky Yu. M., Zaslavsky V. Yu. Acoustic noise of a low flying quadrocopter // NOUSE Theory and Practice. V.5, №3, 2019. P. 21-27.

19 Карташов В.М., Посошенко В.О., Воронин В.В., Колесник В.И., Капуста А.И., Рибников Н.В., Першин Е.В. Методы обнаружения-распознавания радиолокационных, акустических, оптических и инфракрасных сигналов беспилотных летательных аппаратов // Радиотехника. 2021. Вып. 205. С.138 – 153.

20. Sinibaldi G., Marino L. Experimental analysis on the noise of the propellers for small UAV // Applied Acoustics, 74 (2013). P. 79–88.

21. Дистанционные методы и средства исследования процессов в атмосфере Земли ; под ред. Б.Л. Кащеева, Е.Г. Прошкина, М.Ф. Лагутина. Харьков : Бизнес Информ, 2002. 426 с.

22. Saqib M., Khan S.D., Sharma N., Blumenstein M. A study on detecting drones using deep convolutional neural networks // Proceedings of the 2017 14th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS). Lecce, Italy. 29 August–1 September 2017.

23. Park S., Shin S., Kim Y., Matson E.T., Lee K., Kolodzy P.J., Slater J.C., Scherreik M., Sam M., GallagherJ.C., et al. Combination of radar and audio sensors for identification of rotor-type unmanned aerial vehicles (uavs) //Proceedings of the 2015 IEEE SENSORS; Busan, Korea. 1–4 November 2015. P. 1–4.

24. Кошкин Р.П. Беспилотные авиационные системы. Москва : Стратегические приоритеты, 2016. 676 с.

25. Harmanny R., De Wit J., Cabic G.P. Radar micro-Doppler feature extraction using the spectrogram and thecepstrogram // Proceedings of the 2014 11th European Radar Conference; Cincinnati, OH, USA. 11–13 October 2014P. 165–168.

26. De Wit J., Harmanny R., Molchanov P. Radar micro-Doppler feature extraction using the singular value decomposition// Proceedings of the 2014 International Radar Conference. Lille, France. 13–17 October 2014. P. 1–6.

27. Дистанционные методы и средства исследования процессов в атмосфере Земли ; под ред. Б.Л. Кащеева, Е.Г. Прошкина, М.Ф. Лагутина. Харьков : Бизнес Информ, 2002. 426 с.

28. Калистратова М.А., Кон А.И. Радиоакустическое зондирование атмосферы. Москва : Наука, 1985. 200 с.

29 Oh B.S., Guo X., Wan F., Toh K.A., Lin Z. Micro-Doppler mini-UAV classification using empiricalmode-decomposition features // IEEE Geosci. Remote Sens. Lett. 2017. 15:227–231.

30. Mendis G.J., Randeny T., Wei J., Madanayake A. Deep learning based doppler radar for micro UASdetection and classification // Proceedings of the MILCOM 2016-2016 IEEE Military Communications Conference.Baltimore, MD, USA. 1–3 November 2016. P. 924–929.

31 Simonyan K., Zisserman A. Very deep convolutional networks for large-scale image recognition. arXiv.20141409.1556.

32. Opromolla R., Fasano G., Accardo D. A Vision-Based Approach to UAV Detection and Trackingin Cooperative Applications. Sensors. 2018. 8:3391.

33. Урковиц. Обнаружение неизвестных детерминированных сигналов по энергии // ТИИЭР. 1967. Т.55, №4. С. 50-59.

34. В.С. Королюк, Н.И. Портенко, А.В. Скороход, А.Ф. Турбин. Справочник по теории вероятностей и математической статистике. Москва : Наука. Гл. ред. физ.-мат. лит., 1985. 640 с.

35. Куликов Е.И. Методы измерений случайных процессов. Москва : Радио и связь, 1986. 272с.

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

Посошенко Виталий Александрович – канд. техн. наук, Харьковский национальный университет радиоэлектроники, доцент кафедры медиаинженерии и информационных радиоэлектронных систем, Украина; e-mail: vitalii.pososhenko@nure.ua; ORCID: https://orcid.org/0000-0003-0867-9161

Колесник Виктория Ивановна – Харьковский национальный университет радиоэлектроники, ассистент кафедры медиаинженерии и информационных радиоэлектронных систем, Украина; e-mail: viktoriia.kolisnyk@nure.ua; ORCID: https://orcid.org/0000-0002-2382-9124

Селезнёв Иван Сергеевич – Харьковский национальный университет радиоэлектроники, аспирант кафедры медиаинженерии и информационных радиоэлектронных систем, Украина, ORCID: https://orcid.org/0000-0002-0731-7540

Бобнев Роман Александрович – Харьковский национальный университет радиоэлектроники, ст. преподаватель кафедры медиаинженерии и информационных радиоэлектронных систем, Украина; e-mail:roman.bobniev@nure.ua; ORCID: https://orcid.org/0000-0002-9322-9722

Капуста Анастасия Игоревна – Харьковский национальный университет радиоэлектроники, аспирант кафедры медиаинженерии и информационных радиоэлектронных систем, Украина; e-mail: anastasiia.kapusta@nure.ua; ORCID: https://orcid.org/0000-0003-2206-1552

УДК 621.396.96 **DOI:10.30837/rt.2021.4.207.13**

М.Г. ТКАЧ

ОЦІНКА ВІДНОСНОЇ ПРОПУСКНОЇ ЗДАТНОСТІ ЛІТАКОВИХ ВІДПОВІДАЧІВ ВТОРИННИХ РАДІОЛОКАЦІЙНИХ СИСТЕМ СПОСТЕРЕЖЕННЯ ПОВІТРЯНОГО ПРОСТОРУ

Вступ

Значну роль в інформаційному забезпеченні систем контролю повітряного простору і управління повітряним рухом відіграють вторинні радіолокаційні системи (ВРС) спостереження повітряного простору. ВРС забезпечують радіолокаційне спостереження за повітряними об'єктами (ПО), обладнаними літаковими відповідачами (ЛВ) і забезпечують двосторонній зв'язок за каналами запиту та відповіді для передачі даних між наземними радіолокаційними станціями та повітряними об’єктами. До ВРС відносяться вторинні оглядові радіолокатори [1 – 10] та системи ідентифікації за ознакою «свій-чужий» [11 – 21]. При цьому слід зазначити, що ВРС можна розглядати, як двочастотну систему передачі даних, одна частота (1030 МГц) використовується для передачі сигналів запиту, а друга (1090 МГц) – для передачі сигналів відповіді [22 – 25]. ВРС має 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 у військовій сфері, а режим 5 є беззапитальним та більш безпечним. Основні концепції режиму S були використані у режимі 5 [26 – 30], який являє собою просто криптографічно закодовану версію даних режиму S та ADS-B [31, 32].

Найбільш вразливим місцем у вторинних радіолокаційних системах, що істотно обмежує можливість ідентифікації повітряних об'єктів, є літаковий відповідач [33 – 38]. Дійсно, він побудований за принципом відкритої одноканальної системи масового обслуговування з відмовами, що викликає труднощі при роботі останніх при значній інтенсивності потоків як внутрісистемних, так і навмисних корельованих завад. Така побудова літакового відповідача викликає суттєві недоліки в безпеці як його, так і в безпеці всієї системи. Це зазначається в значній кількості робіт, зокрема в [7, 8, 15]. Використання ж єдиної частоти у каналі запиту в таких системах призводить до високої щільності сигналів запиту і, як наслідок, до внутрісистемних завад [22 – 25] значної інтенсивності. Зазначені фактори призводять до зниження якості обробки сигнальних даних, тобто до зниження пропускної здатності літакового відповідача.

При цьому слід зазначити, що основними функціями ВРС є:

- отримання польотних даних з борту повітряного об’єкта;
- ідентифікація виявленого повітряного об’єкта за ознакою «свій-чужий».

Побудова ВРС на принципах радіолокаційних систем спостереження, що передбачає оцінку координат ПО на запитувачі, суттєвим чином впливає на можливість отримання польотних даних, що передаються з літакового відповідача.

Метою роботи є оцінка відносної пропускної здатності літакових відповідачів вторинних радіолокаційних систем спостереження повітряного простору при дії в каналі запиту корельованих та некорельованих завад.

Оцінка відносної пропускної здатності літакових відповідачів вторинних радіолокаційних систем спостереження повітряного простору

Відомо, що вторинні радіолокаційні системи оцінюють виявлений повітряний об’єкт за ознакою «свій-чужий», тобто являються системами ідентифікації (IFF) [1, 5, 11 – 14] та отримують польотні дані з борту виявленого ПО. Однак, як показано в значній кількості робіт [1, 4, 15 – 18], вторинні радіолокаційні системи, побудовані так, що зацікавлена сторона може несанкціоновано використати цей інформаційний ресурс як для дальнього визначення

координат повітряних об’єктів, з одного боку, так і для перекручування інформації цього інформаційного ресурсу, з другого боку, що призводить до непередбачуваних результатів.

ВРС здійснюють спостереження за повітряними об'єктами, обладнаними літаковими відповідачами і забезпечують двосторонній зв'язок за каналом передачі даних між наземними станціями і повітряними об’єктами. ВРС відноситься до основних інформаційних джерел як системи контролю повітряного простору, так і системи управління повітряним рухом. ВРС повинна вирішувати завдання ідентифікації повітряного об'єкта за ознакою «свій-чужий» як в інтересах визначення ступеня небезпеки виявленого повітряного об'єкта, так і при безпосередньому застосуванні зброї. Рішення завдання ВРС за ознакою «свій-чужий» полягає в ухваленні рішення про виявлення повітряного об'єкта зазначеною інформаційною системою. Імітостійка (криптографічна) ідентифікація повітряних об'єктів, що реалізована в існуючих ВРС, дозволяє однозначно вирішити питання за ознакою «свій-чужий» і є важливою умовою функціонування єдиного інформаційно-комунікаційного простору. Найбільш вразливим місцем в ВРС, що суттєво обмежує пропускну здатність вторинних радіолокаційних систем спостереження, в цілому, є літаковий відповідач [17, 18]. Він побудований за принципом відкритої одноканальної системи масового обслуговування з відмовами, що викликає труднощі при роботі останніх при значних щільностях потоків як внутрісистемних завад [19], так і навмисних корельованих завад. Така побудова літакового відповідача викликає суттєві недоліки в безпеці як його, так і всієї ВРС. Використання ж єдиної частоти у каналі запиту системи, що розглядається, призводить до високої щільності сигналів запиту і, як наслідок, – до внутрісистемних завад [20] значної інтенсивності. Зазначені фактори призводять до зниження якості обробки сигнальних даних та зниження пропускної здатності ЛВ. Так, в роботі [21] наводиться характеристика середовища щодо оцінки характеристик сучасних вторинних радіолокаційних приймачів спостереження. Основна увага приділяється параметрам, що дають точну характеристику явищ завад, які суттєво обмежують продуктивність даної системи. В роботах [22 – 25] розглядаються питання оптимального виявлення сигналів запиту при однакових рівнях як сигналів запиту, так і завад, які надходять на літаковий відповідач, що представляє собою ідеальний випадок.

Побудова літакового відповідача за принципом одноканальної системи обслуговування сигналів запиту з відмовами визначила значну часову паралізацію літакового відповідача на час обслуговування попереднього сигналу відповіді, що призводить до суттєвих обмежень як відносної пропускної здатності літакового відповідача, так і до суттєвого зниження пропускної здатності усієї вторинної радіолокаційної системи.

Слід зазначити, що основними найбільш ефективними завадами для відповідачів є ненавмисні та навмисних корельовані завади (КЗ). Це обумовлено тим, що існуюча мережа запитувачів та літакових відповідачів (ЛВ) побудована на принципі несинхронній мережі, а сам ЛВ – на принципі одноканальної системи масового обслуговування з відмовами. Вплив потоку сигналів запиту (ПСЗ) призводить до паралізації ЛВ на час, який визначається режимом запиту. Зазначимо, що при прийомі сигналів запиту (СЗ) за основною пелюсткою діаграми спрямованості антени (ДСА) запитувача ЛВ повністю паралізується на час обслуговування, при прийомі СЗ по бічним пелюсткам ДСА ЛВ паралізується на час між імпульсом СЗ (амплітуда якого запам’ятовується) та імпульсом подавлення бічних пелюсток (ПБП) навмисних корельованих завад (навмисна або ненавмисна). Це впливає на роботу ЛВ двояко:

- по-перше, пригнічує окремі імпульси СЗ, що робить неможливим обслуговування даного СЗ;
- по-друге, паралізує ЛВ через утворення хибних СЗ (хибна тривога першого і другого роду).

Оцінимо пропускну здатність ЛВ при впливі вказаних завад. При надходженні на вхід ЛВ потоків СЗ і навмисних корельованих завад відповідач не сформує СВ, якщо станеться хоча б одна з таких несприятливих ситуацій:

- СЗ запитувача, що розглядається, подавиться через утворення з навмисних корельова-

них завад випереджаючих хибних СЗ (хибна тривога першого роду), які призводять до випромінювання СВ або спрацьовування схеми ПБП (імовірність P_1);

- СЗ запитувача, що розглядається, подавиться через випереджаючі СЗ сусідніх запитувачів або КЗ (імовірність P_2);

- окремі імпульси СЗ запитувача, що розглядається, подавляться на високій частоті через збіг за часом імпульсів різних СЗ при несприятливих фазових співвідношеннях (імовірність P_3);

- СЗ запитувача, що розглядається, подавиться через випереджаючі хибні СЗ, що утворюються при взаємодії першого імпульсу СЗ даного запитувача з випереджаючими (на базу коду) імпульсами навмисних корельованих завад або СЗ (хибна тривога другого роду) і призводять до випромінювання СВ або спрацьовування схеми ПБП (імовірність P_4);

- СЗ запитувача, що розглядається, подавиться через появу на позиції сигналу хибного імпульсу подавлення, який утворився з завад (імовірність P_5);

- СЗ запитувача, що розглядається, подавиться через спрацьовування схеми часової селекції відповідачів (імовірність P_6);

- СЗ запитувача, що розглядається, подавиться через інерційність схем вхідних формувачів дешифратора і обмеження завантаження відповідача (імовірність P_7).

Визначимо імовірності цих подій в припущенні, що потоки СЗ і навмисних корельованих завад впливають на СЗ розглядаємого запитувача незалежно один від одного та кількості джерел, що формують загальний потік СЗ, достатньо велика для загальної характеристики потоку як пуасонівського.

Будемо вважати, що на вхід літакового відповідача поступають:

- потік навмисних корельованих завад інтенсивністю λ_0;
- потік СЗ інтенсивністю λ_1, який включає ПСЗ сусідніх запитувачів і потік КЗ;
- потік СЗ, які викликають спрацьовування схеми ПБП, інтенсивністю λ_2.

Припустимо, що тривалість імпульсів потоку СЗ однакова, незмінна за часом і збігається з тривалістю імпульсів корисного сигналу. Припустимо також, що загальні потоки СЗ складаються з k частин неімітостійкого режиму та $(1 - k)$ частин імітостійкого режиму.

Сумісна дія навмисних корельованих завад і ПСЗ призводить до високочастотного подавлення окремих імпульсів ПСЗ при несприятливих фазових співвідношеннях, внаслідок чого інтенсивність ПСЗ зменшується.

Імовірність того, що хоча б один імпульс навмисних корельованих завад збіжиться за часом з імпульсом ПСЗ та подавить його, становить

$$P_n = \gamma\left[1 - \exp\left(-\lambda_0 \tau_{0`}\right)\right],$$

де γ – коефіцієнт інтерференційного подавлення, який визначає імовірність інтерференційного подавлення імпульсу прийнятого СЗ при його збіжності за часом з імпульсом завади.

Через високочастотне подавлення зменшується інтенсивність потоку СЗ, які викликають випромінювання СВ:

$$\lambda_1^1 = \lambda_1 \left(1 - P_n\right)^n,$$

та інтенсивність ПСЗ, які викликають спрацьовування схеми ПБП:

$$\lambda_2^1 = \lambda_2 \left(1 - P_n\right)^n,$$

де n – кількість імпульсів у СЗ.

Імовірність того, що хоча б один СЗ потрапить в випереджаючий інтервал та подавить СЗ ВРС, що розглядається, за рахунок часу паралізації t_1 ЛВ у неімітостійкому режимі при

випромінюванні СВ, визначається для навмисних корельованих завад та ПСЗ відповідно:

$$P_1^1 = 1 - \exp(-\lambda_x t_1) \quad \text{та} \quad P_1^2 = 1 - \exp(-k\lambda_1 t_1),$$

де λ_x – середня кількість хибних n-імпульсних кодів, що призводять до випромінювання СВ; $k = \lambda_н / \lambda_1$ – відносна частка неімітостійкого режиму в загальній інтенсивності потоку СЗ; $\lambda_н$ – інтенсивність потоку СЗ неімітостійкого режиму.

Середню кількість хибних n-імпульсних кодів, які призводять до випромінювання СВ, можна визначити за формулою

$$\lambda_x = n\tau_0^n \lambda_0^{n-1}(1 - \tau_c / \tau_0),$$

де τ_c – тривалість селекції імпульсів за часом.

Імовірність того, що хоча б один СЗ потрапить в випереджаючий інтервал і подавить СЗ розглядаємої ВРС за рахунок часу паралізації t_2 ЛВ в імітостійкому режимі при випромінюванні СВ, від навмисних корельованих завад та ПСЗ визначається за виразами:

$$P_1^3 = 1 - \exp(-\lambda_x t_2), \quad P_1^4 = 1 - \exp[-(1-k)\lambda_1 t_2].$$

Результуюча імовірність подавлення СЗ даного запитувача системи через паралізацію відповідача при випромінюванні СВ складає

$$P_1 = 1 - \prod_{i=1}^{4}\left(1 - P_1^i\right).$$

Імовірність P_2 того, що хоча б один СЗ попаде в випереджаючий інтервал і подавить СЗ, що розглядається, за рахунок часу паралізації t_3 ЛВ при спрацьовуванні схеми ПБП від навмисних корельованих завад чи від ПСЗ в неімітостійкому режимі, визначається відповідно:

$$P_2^1 = 1 - \exp(-\lambda_x t_3), \quad P_2^2 = 1 - \exp(-k\lambda_2 t_3).$$

Імовірність того, що хоча б один СЗ попаде в випереджаючий інтервал і подавить СЗ ВРС, що розглядається, за рахунок часу паралізації t_4 ЛВ при спрацьовуванні схеми ПБП в імітостійкому режимі від навмисних корельованих завад та від ПСЗ, визначається відповідно:

$$P_2^3 = 1 - \exp(-\lambda_x t_4), \quad P_2^4 = 1 - \exp[-(1-k)\lambda_2 t_4].$$

Результуюча імовірність подавлення СЗ даного запитувача ВРС, що розглядається, через паралізацію відповідача при прийманні СЗ по бічних пелюстках ДСА запитувача становить

$$P_2 = 1 - \prod_{i=1}^{4}\left(1 - P_2^i\right).$$

Імовірність подавлення одного будь-якого імпульсу СЗ даного запитувача через збіжність з імпульсами потоків навмисних корельованих завад і СЗ становить

$$P_{10} = \gamma[1 - \exp(-\lambda_c \tau_{0`})],$$

де $\lambda_c = \lambda_0 + \lambda_1^1 + \lambda_2^1$ – інтенсивність сумарного потоку завад та СЗ.

З урахуванням n імпульсів СЗ імовірність подавлення сигналу запиту складає

$$P_3 = 1 - (1 - P_{10})^n$$

Імовірність P_4 подавлення СЗ ВРС, що розглядається, через появу випереджаючих хибних кодів запиту, що утворюються в результаті взаємодії першого імпульсу коду запиту з випереджаючими імпульсами ПСЗ і призводять до випромінювання СВ або спрацьовування схеми подавлення бічних пелюсток, визначається співвідношенням

$$P_4 = (1 - P_{01})^n \left[1 - (1 - P_{10})^{n+1}\right].$$

Інший співмножник враховує можливі ситуації утворення хибних випереджаючих кодів запиту: n кодів запиту, що призводять до випромінювання коду відповіді, і одного коду сигналу подавлення, який призводить до спрацьовування схеми ПБП.

Імовірність хибної тривоги другого роду P_{01} визначається за формулою

$$P_{01} = 1 - \exp(-\lambda_c \tau_{0`}).$$

Імовірність P_5 подавлення запиту запитувача, що розглядається, через появу на позиції сигналу хибного імпульсу подавлення, який утворився з завад, визначається за формулою

$$P_5 = (1 - P_{10})^n P_{01}^{n-1}.$$

Імовірність P_6 подавлення СЗ в результаті спрацьовування схем часової селекції відповідачів визначається співвідношенням

$$P_6 = 1 - \exp(-2\lambda_c \tau_{0`}).$$

Імовірність P_7 подавлення кодів запиту через інерційність вхідних формувачів ЛВ визначається за формулою

$$P_7 = 1 - (1 - P_f)^n,$$

де $P_f = 1 - \exp(-\lambda_c \tau_f)$ – імовірність подавлення одного імпульсу коду через інерційність формувача.

Якщо середня кількість СЗ перевищує припустиму величину завантаження ЛВ λ_M, то імовірність відповіді при роботі схеми обмеження завантаження ЛВ зменшується і становить $P_{лв} = \lambda_M / \lambda_3$, де $\lambda_3 = \lambda_1 + \lambda_2$.

Імовірність випромінювання СВ ЛВ на запит запитувача, що розглядається, яка і є ВПЗ становить:

при $\lambda_3 < \lambda_M$ $$C_0 = \prod_{i=1}^{7} (1 - P_i),$$

при $\lambda_3 > \lambda_M$ $$C_0 = P_{лв} \prod_{i=1}^{7} (1 - P_i).$$

Розрахунки за наведеними виразами наведені на рис. 1 – 3. При цьому вважали, що інтенсивність потоку навмисних корельованих завад $\lambda_0 = 0; 2 \cdot 10^4; 4 \cdot 10^4$, а інтенсивність λ_1 ПСЗ, які призводять до випромінювання сигналу відповіді, в п’ять разів менше інтенсивності λ_2 потоку СЗ, які викликають спрацьовування схеми ПБП. Розрахунки наведено для коефіцієнтів $k = 0{,}5; 0{,}25; 0{,}1$.

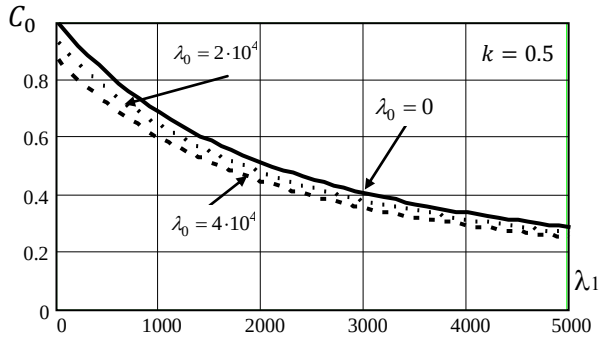


Рис. 1. Оцінка пропускної здатності літакового відповідача

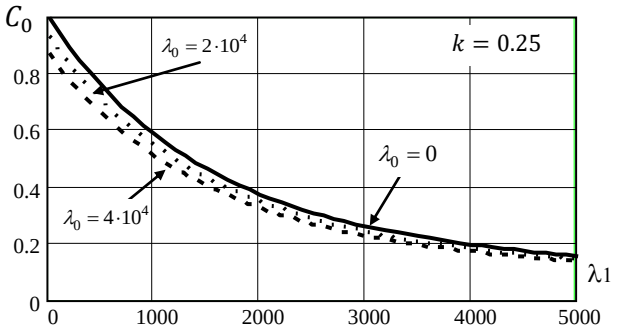


Рис. 2. Оцінка пропускної здатності літакового відповідача

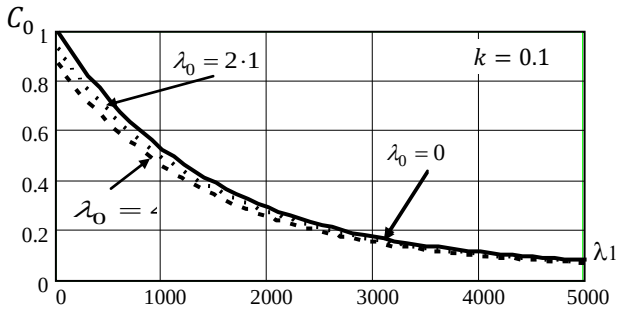


Рис.3. Оцінка пропускної здатності літакового відповідача

З наведених результатів можна зробити наступні висновки:

Збільшення інтенсивності потоку сигналів запиту призводить до різкого зниження коефіцієнта готовності літакового відповідача, що вказує на низьку пропускну здатність ЛВ (і вторинних радіолокаційних систем в цілому). Дійсно, з рис. 1 – 3 видно, що постановка навмисних корельованих завад інтенсивністю 5000 призводить до зниження відносної пропускної здатності літакового відповідача з 1 до 0,3.

Некорельовані завади порівняно слабко впливають на пропускну здатність ЛВ. Так, при $k = 0{,}5$ і наявності ПСЗ $\lambda_1 = 5000$ вплив інтенсивних некорельованих завад ($\lambda_0 = 40000$) призводить до порівняно незначного зниження пропускної здатності ЛВ з 0,3 до 0,27. Це означає, що найбільш небезпечною для вторинних радіолокаційних систем є навмисна корельована завада. Ця обставина дозволяє стверджувати, що основним видом завад при подавлені вторинних радіолокаційних систем у системному плані є постановка навмисних корельованих завад. З розрахунку виходить, що інтенсивність потоку СЗ, яка дорівнює 5000, що потребує випромінюванню 10000 імпульсів більш ніж на порядок ефективніше за випромінювання 40000 імпульсів некорельованої завади.

Збільшення частки імітостійкого режиму в загальному ПСЗ призводить до суттєвого зниження пропускної здатності ЛВ. Так, при відсутності некорельованих завад ($\lambda_0 = 0$) та при інтенсивності ПСЗ $\lambda_1 = 4000$ збільшення частки імітостійкого режиму з 0,5 до 0,9 призводить до зменшення пропускної здатності ЛВ майже втричі – з 0,35 до 0,12.

Проведена оцінка пропускної здатності ЛВ показує, що ЛВ не досягає максимального завантаження, яке закладено в діючу систему ідентифікації при дії навмисних корельованих завад. Розрахунки показують, що кількість відповідей ЛВ ніколи не досягає такого значення. Це вказує на неправильне визначення коефіцієнта завантаження, через що ЛВ існуючої ВРС не буде відсіювати СЗ малої потужності. Неправильне визначення максимального завантаження ЛВ призводить до зниження завадостійкості як ЛВ, так і всієї ВРС. При цьому слід зазначити, що зацікавлена сторона буде несанкціоновано використовувати ЛВ і отримувати від нього інформацію або паралізувати його застосуванням завад потрібної інтенсивності за допомогою одного запитувача, розташованого на значній відстані.

Висновки

Збільшення інтенсивності потоку сигналів запиту призводить до різкого зниження відносної пропускної здатності ЛВ, що вказує на низьку пропускну здатність існуючих літакових відповідачів.

Некорельовані завади порівняно слабко впливають на відносну пропускну здатність. При цьому цей вплив значно зменшується при досягнення ЛВ припустимої величини завантаження.

Збільшення частки імітостійкого режиму ідентифікації за ознакою «свій-чужий» в загальному потоку сигналів запиту призводить до зниження відносної пропускної здатності ЛВ.

Невірний вибір максимального завантаження ЛВ призвів до зниження характеристик як ЛВ, так і всієї вторинної радіолокаційної системи за рахунок відсутності виключення з обслуговування СЗ запитувачів котрі находяться значній дальності від ЛВ.

Список литературы:

1. Маляренко А.С. Системы вторичной радиолокации для управления воздушным движением и государственного радиолокационного опознавания [Справочник]. Харьков : ХУПС, 2007. 78 с.
2. Kim E. and Sivits K. Blended secondary surveillance radar solutions to improve air traffic surveillance // Aerospace Science and Technology, vol. 45, 2015, pp. 203-208.
3. Guofeng Jiang; Yangyu Fan; Hongbo Yuan. Assessing the Capacity of Air Traffic Control Secondary Surveillance Radar System // 2019 Cross Strait Quad-Regional Radio Science and Wireless Technology Conference (CSQRWC). doi: 10.1109/CSQRWC.2019.8799146.
4. Semenets V., Svyd I., Obod I., Maltsev O. Tkach M. Quality Assessment of Measuring the Coordinates of Airborne Objects with a Secondary Surveillance Radar // Ageyev D., Radivilova T., Kryvinska N. (eds) Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies, vol 69. Springer, Cham, pp. 105-125, 2021. doi: 10.1007/978-3-030-71892-3_5.
5. Svyd I., Maltsev O., Obod I. and Zavolodko G. Fusion Method of Primary Surveillance Radar Data and IFF systems Data // 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kyiv, Ukraine, 2020, pp. 336-340, doi: 10.1109/DESSERT50317.2020.9125040.
6. Обод І.І., Свид І.В. Порівняльний аналіз якості виявлення повітряних об’єктів запитальними системами спостереження // Тематичний збірник «Системи обробки інформації». Вип. 9 (90). Харків : ХУПС, 2010. С. 74-76.
7. Obod I., Svyd I., Maltsev O., Vorgul O., Maistrenko G. Zavolodko G. Optimization of the Quality of Information Support for Consumers of Cooperative Surveillance Systems // Radivilova T., Ageyev D., Kryvinska N. (eds) Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies, vol 48. Springer, Cham, pp. 133-155, 2020. doi: 10.1007/978-3-030-43070-2_8.
8. Obod I., Svyd I., Maltsev O., Zavolodko G., Pavlova D. Maistrenko G. Fusion the Coordinate Data of Airborne Objects in the Networks of Surveillance Radar Observation Systems // Radivilova T., Ageyev D., Kryvinska N. (eds) Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies, vol 48. Springer, Cham, pp. 731-746, 2020. doi: 10.1007/978-3-030-43070-2_31.

9. Черних О.П., Обод І.І., Свид І.В. Інформаційне забезпечення на основі мереж спостереження повітряного простору // Eastern-European Journal of Enterprise Technologies, 2/9(50) 2011. Харків, 2011. С. 23-25. doi: 10.15587/1729-4061.2011.1850.

10. Takuya Otsuyama; Junichi Honda; Kakuichi Shiomi; Gaku Minorikawa; Yusuke Hamanaka. Performance evaluation of Passive Secondary Surveillance Radar for small aircraft surveillance // European Radar Conference (EuRAD), 2015. doi: 10.1109/EuRAD.2015.7346348.

11. STANAG 4193 Document, Technical Characteristics of IFF Mk X and Mk XII Interrogators and Transponders (Part V). Technical Description of the MkXII System, NATO Standard, 2016.

12. Sharifi-Tehrani O., Sadeghi A. and Razavi S. M. J. Design and Simulation of IFF/ATC Antenna for Unmanned Aerial Vehicle // Majlesi Journal of Mechatronic Systems, vol. 6, no. 1, Jun. 2017.

13. Poornima P., Roja Reddy B. and Anantha Murthy B. G. Design and Simulation of Two-Chain Monopulse Receiver for IFF Radar Application // 2018 3rd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), Bangalore, India, 2018, pp. 1114-1118, doi: 10.1109/RTEICT42901.2018.9012646.9

14. Svyd I., Obod I., Maltsev O., Tkachova T. and Zavolodko G. Improving Noise Immunity in Identification Friend or Foe Systems // 2019 IEEE 2nd Ukraine Conference on Electrical and Computer Engineering (UKRCON), Lviv, Ukraine, 2019, pp. 73-77, doi: 10.1109/UKRCON.2019.8879812.

15. Pollack J. and Ranganathan P. Aviation Navigation Systems Security: ADS-B, GPS, IFF // International Conference on Security & Management, SAM'18, International Conference on Security & Management, SAM'18, Las Vegas, Nevada, USA, 2018, pp. 129-135.

16. Obod I., Svyd I., Maltsev O. and Bakumenko B. Comparative Analysis of Noise Immunity Systems Identification Friend or Foe // 2020 IEEE 40th International Conference on Electronics and Nanotechnology (ELNANO), Kyiv, Ukraine, 2020, pp. 751-756, doi: 10.1109/ELNANO50318.2020.9088856.

17. Svyd I., I. Obod I. Maltsev O. Interference Immunity Assessment Identification Friend or Foe Systems // Ageyev D., Radivilova T., Kryvinska N. (eds) Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies, vol 69. Springer, Cham, pp. 287-306, 2021. doi: 10.1007/978-3-030-71892-3_12.

18. Strelnytskyi O., Svyd I., Obod I., Maltsev O., Voloshchuk O. and Zavolodko G. Assessment Reliability of Data in the Identification Friend or Foe Systems // 2019 IEEE 39th International Conference on Electronics and Nanotechnology (ELNANO), Kyiv, Ukraine, 2019, pp. 728-731, doi: 10.1109/ELNANO.2019.8783397.

19. Svyd I., Obod I., Maltsev O., Strelnytskyi O., Zubkov O. and Zavolodko G. Method of Increasing the Identification Friend or Foe Systems Information Security // 2019 3rd International Conference on Advanced Information and Communications Technologies (AICT). Lviv, Ukraine, 2019, pp. 434-438, doi: 10.1109/AIACT.2019.8847853.

20. Schuck T.M.; Shoemaker B.; Willey J. Identification friend-or-foe (IFF) sensor uncertainties, ambiguities, deception and their application to the multi-source fusion process // Proceedings of the IEEE 2000 National Aerospace and Electronics Conference. NAECON 2000. Engineering Tomorrow (Cat. No.00CH37093). doi: 10.1109/NAECON.2000.894896

21. Svyd I., Obod I., Maltsev O., Shtykh I. and Zavolodko G. Model and Method for Detecting Request Signals in Identification Friend or Foe Systems // 2019 IEEE 15th International Conference on the Experience of Designing and Application of CAD Systems (CADSM), Polyana, Ukraine, 2019, pp. 1-4, doi: 10.1109/CADSM.2019.8779322.

22. Poornima P., Roja Reddy B. and Anantha Murthy B. G. Design and Simulation of Two-Chain Monopulse Receiver for IFF Radar Application // 2018 3rd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), Bangalore, India, 2018, pp. 1114-1118. doi: 10.1109/RTEICT42901.2018.9012646.

23. Otsuyama T., Honda J., Naganawa J. and Miyazaki H. Analysis of signal environment on 1030/1090MHz aeronautical surveillance systems // 2018 IEEE International Symposium on Electromagnetic Compatibility and 2018 IEEE Asia-Pacific Symposium on Electromagnetic Compatibility (EMC/APEMC), Singapore, 2018, pp. 71-71, doi: 10.1109/ISEMC.2018.8394048.

24. Ozeki Sh., Otsuyama T., Koga T., Sumiya Ya. Error Compensations for 1030 MHz Signal Environment Estimation: The format of Technical Report.

25. Yu Hsuan Chen; Sherman Lo; Per Enge; Shau Shiun Jan. Evaluation & comparison of ranging using Universal Access Transceiver (UAT) and 1090 MHz Mode S Extended Squitter (Mode S ES). 2014 IEEE/ION Position, Location and Navigation Symposium. doi: 10.1109/PLANS.2014.6851456.

26. Obod I., Svyd I., Vorgul O., Maltsev O., Datsenko O., Boiko N. Optimization of Data Processing Structure for Multi-Position Radar Surveillance Systems // 2021 IEEE 3rd Ukraine Conference on Electrical and Computer Engineering (UKRCON), 2021, pp. 133-137, doi: 10.1109/UKRCON53503.2021.9575286.

27. Li Huan, Zhao Feng, Li Yu Bai, Wang Jian. One Joint Demodulation and Despreading Algorithm for MOD5 // The Open Automation and Control Systems Journal 2015 7(1):386-397. doi: 10.2174/1874444301507010386

28. P. Finocchio. Future radars procurement for the Italian Ministry of Defense // 2009 European Radar Conference (EuRAD), 2009, pp. 326-329.

29. Yang Guo; Jianbo Yang; Chunjian Guan. A Mode 5 signal detection method based on phase and amplitude correlation // 2013 Ninth International Conference on Natural Computation (ICNC). doi: 10.1109/ICNC.2013.6818164.

30. E.A. El-Badawy; W.A. EL-Masry; M. A. Mokhtar; Alaa S. Hafez. A secured chaos encrypted mode-S aircraft identification friend or foe (IFF) system // 2010 4th International Conference on Signal Processing and Communication Systems. doi: 10.1109/ICSPCS.2010.5709756.

31. Edward Ted Lester. Military position source challenges for worldwide ADS-B out compliance // 2013 Integrated Communications, Navigation and Surveillance Conference (ICNS). doi: 10.1109/ICNSurv.2013.6548530.

32. Martin Strohmeier. Large-Scale Analysis of Aircraft Transponder Data // IEEE Aerospace and Electronic Systems Magazine (Volume: 32, Issue: 1, January 2017). pp. 42 – 44. doi: 10.1109/MAES.2017.160149.

33. United States Navy. Navy Programs: Mark XIIA Identification Friend or Foe (IFF) Mode 5. 2012. Available: http://www. dote. osd. mil/pub/reports/FY2012/pdf/nav y/2012mkxiiaiffmode5. pdf.

34. David S. and Vitolo A. J. Airborne IFF transponder antenna system with Omni and steerable cardioid patterns, Aug. 1970, pp. 279-283.

35. Метод підвищення завадозахищеності радіолокаційних систем ідентифікації «свій-чужий» при дії навмисних корельованих завад / І.В. Свид, І.І. Обод, О.С. Мальцев, М.Г. Ткач, С.В. Старокожев, А.О. Глущенко, В.С. Чумак // Радіотехніка. 2021. Вип. 205. С. 154-160. doi:10.30837/rt.2021.2.205.16.

36. Svyd I., Obod I., Maltsev O., Andrusevich, Bakumenko B., Vorgul O. Optimal Measurement of Signal Data Parameters of Requesting Radar Systems // 2021 IEEE 3rd Ukraine Conference on Electrical and Computer Engineering (UKRCON), 2021, pp. 138-141, doi: 10.1109/UKRCON53503.2021.9575235.

37. Свид І.В., Обод І.І., Заволодько Г.Е. Оптимізація обробки даних в літакових відповідачах системи ідентифікації «свій-чужий» // Радіотехніка. 2020. Вип. 203. С. 162-169. doi: 10.30837/rt.2020.4.203.16.

38. Evaluation the Quality of Measuring the Coordinates of Air Objects in the Synchronous Information Network of Surveillance Systems / V. Semenets, I. Svyd, I. Obod, O. Maltsev, O. Vorgul, M. Tkach, V. Chumak // Information systems and technologies IST-2021: Proceedings of the 10-th International Scientific and Technical Conference, Kharkiv – Odesa, Ukraine, 2021, pp. 23-27.

Надійшла до редколегії 03.11.2021

Відомості про автора:

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

СИСТЕМИ І МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ
СИСТЕМЫ И МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ
SYSTEMS AND METHODS OF INFORMATION SECURITY

УДК 621.37: 004.056.5 **DOI:10.30837/rt.2021.4.207.14**

С.П. СЕРГІЄНКО, канд. фіз.-мат. наук, В.Г. КРИЖАНОВСЬКИЙ, д-р техн. наук,
Д.В. ЧЕРНОВ, канд. техн. наук, Л.В. ЗАГОРУЙКО, канд. техн. наук

ВИКОРИСТАННЯ НЕСТАЦІОНАРНИХ ШУМОВИХ ЗАВАД ДЛЯ ПРОТИДІЇ ПАСИВНИМ РАДІОЗАКЛАДКАМ

Вступ

В даний час інформаційна безпека розвивається в динамічній рівновазі між технологіями несанкціонованого зняття інформації і технологіями, що створюються для протидії такій діяльності. Для захисту від підслуховуючих пристроїв (радіозакладок) зазвичай використовуються системи радіопротидії, які встановлюють перешкоди в потенційно небезпечних для передачі інформації радіочастотних діапазонах або на частотах сигналів які щойно з'явилися [1, 2]. Такі перешкоди є шумовими сигналами, які іноді використовують ще й для потайної передачі інформації, для маскування переходу сигналу на іншу частоту [3 – 6], для прихованої передачі інформації шумові сигнали включаються між інформаційними пакетами [7]. Було показано, що застосування радіочастотного зашумлення не гарантує захисту приміщення від несанкціонованого зняття інформації при використанні пасивних радіозакладок [8 – 10]. Включення радіочастотного зашумлення може бути сигналом про те, що на території, яка захищається, відбуваються інформаційно цікаві події. Радіозакладка може використовувати енергію випромінювання генератора шуму для своєї активної роботи. До того ж такі радіозакладки можна зробити невидимими для існуючих в даний час таких засобів виявлення цих пристроїв, як нелінійні радіолокатори [11 – 14]. Екранування електронної схеми, а у відсутності радіозашумлення, відключення зв'язку електронної частини від антени – унеможливить виявлення радіозакладок. У той же час, включення радіо зашумлення створюватиме перешкоди для роботи нелінійного радіолокатора.

Для забезпечення скритності несанкціонованого підслуховування сигнали, які передаються радіозакладками, повинні мати малу потужність. Радіозакладки, що використовують для своєї роботи енергію зовнішнього радіочастотного випромінювання, принципово не мають достатнього потужного джерела енергії. Цим пояснюється мала відстань упевненого прийому сигналів радіозакладок. Забезпечити високу чутливість прийому слабких сигналів можна за допомогою приймачів, що накопичують енергію сигналу. Кореляційні приймачі мають перевагу в чутливості при прийомі сигналів, що передають малі обсяги інформації в одиницю часу. Накопичення енергії за час передачі біта інформації цифрового сигналу або за період часу максимальної частоти інформаційного аналогового сигналу забезпечує високу чутливість кореляційних приймачів.

В роботі [10] було отримано оптимальні режими роботи і розраховано параметри елементів схеми, які забезпечують ефективний режим роботи радіозакладки з використанням енергії радіочастотного зашумлення. В даній статті розглядається спосіб протидії радіозакладкам, які використовують для своєї роботи радіошумові сигнали, призначені для протидії підслуховуванню, за допомогою нестаціонарних шумів. Цей аналіз проводиться на прикладі використання кореляційних приймачів для реєстрації слабких сигналів. Вибір кореляційного приймача обумовлений тим, що для прийому випадкового радіочастотного сигналу кореляційний прийом є єдиним способом забезпечити прийнятну дальність впевненого прийому слабкого сигналу.

Основна частина

Модуляція радіочастотного зашумлення аналоговим акустичним або цифровим сигналом дозволяє налагодити канал витоку інформації [10]. Такий засіб підслуховування не потребує зовнішнього джерела енергії. Але інформаційний сигнал, що випромінює радіозакладка, має малу потужність, тому в якості приймача розглядаємо кореляційний приймач.

На схемі рис. 1 показана модель підслуховування з використанням енергії сигналу радіочастотного зашумлення, де 1 – генератор постановки радіочастотних завад, 2 – радіозакладка, 3 – антена прийому сигналу, який несе інформацію від радіозакладки, 4 – підсилювач інформаційного сигналу, 5 – антена опорного сигналу, направлена на генератор шумових завад, 6 – підсилювач опорного сигналу, 7 – блок нелінійного перетворення опорного сигналу, аналогічний тому, якому підвергається сигнал в радіозакладці, 8 – смуговий фільтр, смуга пропускання якого співпадає зі смугою випромінювання радіозакладки, 9 – перемножувач інформаційного та опорного сигналів, 10 – інтегратор. Сигнал, що надходить з радіозакладки, можна представити у вигляді: $U_1(t) = \mathrm{A}(t)U_0(t)$, де $\mathrm{A}(t)$ – інформаційний сигнал, спектр якого лежить в акустичному діапазоні, що модулює шумовий сигнал $U_0(t)$ спектр якого на багато порядків вище спектра сигналу $\mathrm{A}(t)$. У відсутності інформаційного сигналу при $\mathrm{A}(t) = 1$ на виході кореляційного приймача буде постійна напруга пропорційна потужності шумового сигналу. Сигнал, що надходить в опорний канал після проходження блоку нелінійного перетворення піддається аналогічному нелінійному перетворенню що і шумовий сигнал в радіозакладці. На виході з блоку 8 напруга $U_0(t)$ буде така ж, як і напруга в інформаційному каналі.

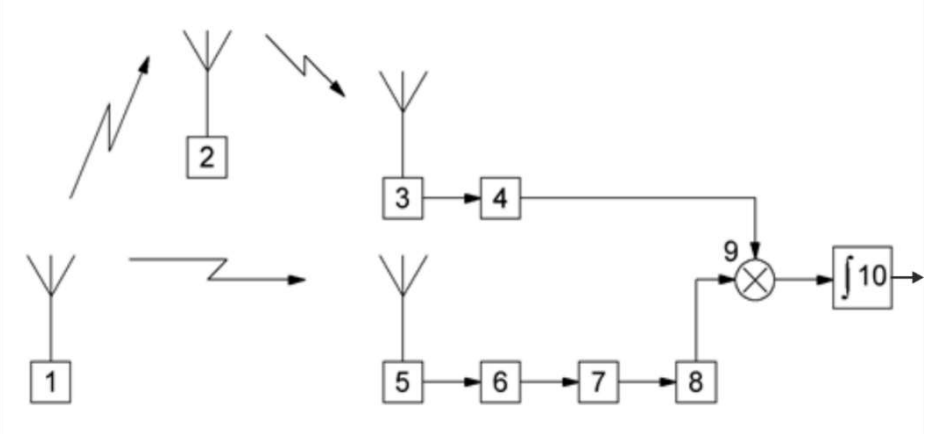


Рис. 1. Схема підслуховування з використанням енергії сигналу радіочастотного зашумлення

Сигнал на виході з кореляційного приймача (після перемножувача і інтегратора) визначається виразом $U(t) = \int_t^{t+\Delta t} U_1(t)U_0(t)^2 dt$, де $U_1(t) = \mathrm{A}(t)U_0(t)$. Інформаційний сигнал $\mathrm{A}(t)$ – функція, що повільно змінюється. За час інтегрування Δt, який визначається постійною часу інтегратора, можна вважати $\mathrm{A}(t)$ = const. При появі інформаційного сигналу він модулює шумовий сигнал. При передачі інформації сигнал на виході кореляційного приймача буде визначатися виразом

$$U(t) = \int_t^{t+\Delta t} \mathrm{A}(t)U_0(t)U_0(t)dt \cong \mathrm{A}(t) \int_t^{t+\Delta t} U_0(t)^2 dt. \quad (1)$$

Інтеграл $\int_t^{t+\Delta t} U_0(t)^2 dt$ (при відсутності амплітудної модуляції) буде константою, що не залежить від поточного часу t, якщо $U_0(t)$ буде стаціонарним випадковим сигналом, а $\Delta t >> \tau_0$, де τ_0 – час кореляції стаціонарного смугового випадкового сигналу. Цей інтеграл буде залежати від Δt. При модуляції шуму випадковий смуговий сигнал перестає бути стаціонарним і на виході перемножувача напруга буде змінюватися пропорційно інформаційному сигналу $\mathrm{A}(t) \int_t^{t+\Delta t} U_0(t)^2 dt$. Для часу інтегрування також повинна виконуватися друга умова

– $\Delta t < 1/f_m$, де f_m – максимальна частота в спектрі сигналу модуляції, або $\Delta t < T_b$, де T_b – час передачі одного біта інформації. Друга умова обмежує чутливість кореляційного приймача (збільшення Δt приведе к збільшенню інтеграла $\int_t^{t+\Delta t} U_0(t)^2 dt$ в виразі для вихідного сигналу (1)). Якщо час накопичування сигналу збільшити порівняно з умовою $\Delta t < 1/f_m$, при передачі аналогового сигналу буде втрачена частина спектральних складових інформаційного сигналу і інформаційний сигнал буде спотворений або, якщо не буде виконуватися умова $\Delta t < T_b$ при передачі цифрового сигналу, буде усереднена напруга логічної одиниці і логічного нуля і логічний перепад буде менше допустимого.

Спектр сигналу генератора перешкод для протидії роботі пасивних радіозакладок має вигляд, представлений на рис. 2. Розрахунки проводилися у відносних одиницях. Крива (a) – спектр потужності сигналу радіочастотних перешкод, (b) – спектр сигналу перешкод, який відбився від нелінійного елементу в підслуховуючому пристрої. Для активізації пасивної радіозакладки необхідне її опромінення електромагнітним випромінюванням досить великої амплітуди, здатної створити на нелінійному елементі напругу, амплітуда якої перевищує напругу термічного потенціалу $U = kT/q$. Тому пасивна радіозакладка буде більш ефективно працювати в безпосередній близькості джерела шумових перешкод і тому розташування генератора шумових перешкод біля радіопідслуховуючого пристрою не заважає його роботі, а, навпаки, збільшує дальність впевненого прийому інформації, що передається. Вузька смуга спектру радіочастотних перешкод обумовлена потребою уникнути негативного впливу на легальні радіопристрої. Зашумленню піддається частотний діапазон, в якому існує потенційна загроза несанкціонованого знімання інформації.

Для підвищення чутливості кореляційного приймача опорний сигнал повинен мати достатньо велику амплітуду. Для цього підсилювач 6 підвищує амплітуду опорного сигналу. Слід зазначити, рівень опорного сигналу, який надходить на антену 5, спрямовану на випромінюючу антену системи радіопротидії, набагато більший від інформаційного сигналу, який приходить на антену 3. Це обумовлено тим, що антену 5 кореляційного приймача можна зробити більш ефективною в порівнянні з антеною радіопідслуховуючого пристрою. Її габаритні розміри і конструкція не обмежені вимогами забезпечення скритності. На відміну від антени для підслуховування антена кореляційного приймача може мати вузьку діаграму спрямованості і у неї буде великий коефіцієнт посилення. Антена для підслуховування 2 менш ефективна в порівнянні з антеною 5, а перетворений сигнал буде ослаблений на нелінійному елементі радіопідслуховуючого пристрою. Тому, можна зробити висновок, що інформаційний сигнал на вході кореляційного приймача завжди буде значно слабше від опорного сигналу, прийнятого антеною 5. В інформаційному каналі сигнал набагато слабше в силу вище зазначених причин, тому він і визначає максимальну дальність прийому сигналу радіозакладки, обмежену шумами підсилювача, в нашому випадку це підсилювач 4 [10].

Розглянемо ефективність використання нестаціонарних шумових завад для протидії пасивним підслуховуючим пристроям. Можливість прийому сигналів в умовах присутності шумів з співпадаючим спектром аналізується за допомогою теорії [15], яка розроблена для аналізу забезпечення якісного прийняття шумоподібних радіосигналів в умовах присутності шумів, що заважають. Умови, щоб сигнал можна було розглядати як шумоподібний, визначаються співвідношенням, яке визначає базу шумоподібного сигналу $B = \Delta F \cdot T$, де ΔF – ширина смуги спектра сигнал. За умови, що $B > 1$ інформаційний сигнал можна вважати шумоподібним. У нашому випадку шумовий сигнал, модульований інформаційним сигналом, завідомо є випадковим і для нього також виконується співвідношення $B > 1$, тому ми можемо застосовувати, вищевказану теорію, для аналізу умови придушення каналу передачі інформації з радіозакладки, яка використовує шумові сигнали для передачі інформації. Завадостійкість прийому сигналу кореляційним приймачем залежить від співвідношення сигнал-шум на вході і бази сигналу B:

$$q^2 = 2B\rho^2, \tag{2}$$

де $\rho^2 = P_c/P_v$ – відношення потужностей сигналу і перешкоди. Завадостійкість зростає з ростом бази сигналу, інформація завжди передається сигналами відомої часової залежності, а завада носить випадкову залежність від часу. Тому збільшення часу накопичування або розширення спектру сигналу дозволяє виділити інформаційний сигнал змішаний с завадою. Оцінка завадостійкості береться виходячи з максимальності бази сигналу. Збільшити базу сигналу можна за рахунок збільшення ширини спектра і за рахунок збільшення тривалості сигналу. Змінити ширину спектру неможливо внаслідок того, що параметри шумового сигналу задаються системою захисту і зловмисники не можуть впливати на параметри системи радіопротидії. Збільшення база сигналу B за рахунок збільшення тривалості сигналу T призведе до зменшення швидкості передачі цифрової інформації, що часто неприпустимо через обмеженість часу, протягом якого актуальна передача інформації. Кількість біт інформації, переданої сигналом, у якого база сигналу була збільшена в T/T_0 разів, буде зменшена в стільки же разів. Тут T_0 – мінімальна тривалість часу передачі цифрової одиниці, яка пов'язана з максимальною частотою спектра сигналу згідно с теоремою Котельникова формулою $T_0 = 1/f_m$, f_m – максимальна частота спектра сигналу модуляції. Тому максимальна швидкість передачі інформації в одну секунду становить $1/T_0$.

Максимальна дальність прийому інформаційного сигналу визначається співвідношенням сигнал/шум в інформаційному каналі, що складається з шумів підсилювача і ефірних шумів. Рівність потужності шуму в спектральної смузі інформаційного сигналу і потужності інформаційного сигналу визначає максимальну дальність впевненого прийому сигналу. На вході перемножувача шум, присутній в опорному сигналі, набагато менше шуму в інформаційному сигналі і їм можна знехтувати. Сигнал на виході підсилювача 4 міститиме крім інформаційного сигналу ще й сигнал шуму підсилювача $V(t)$. Спектр шуму вважатимемо білим, пересічним зі спектром інформаційного сигналу.

$$U(t) = \int_t^{t+\Delta t}\{\mathrm{A}(t) + V(t)\}U_0(t)U_0(t)dt \cong \{\mathrm{A}(t) + V(t)\}\int_t^{t+\Delta t} U_0(t)U_0(t)dt. \tag{3}$$

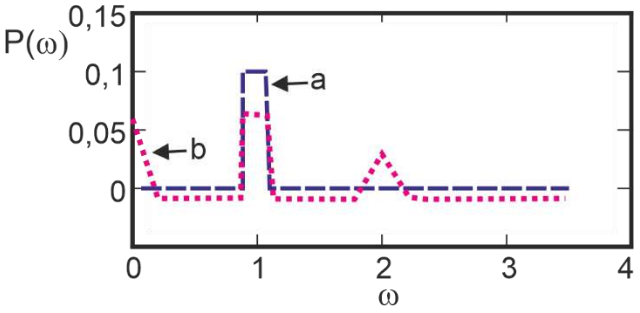
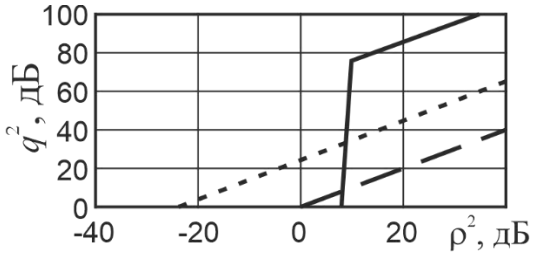


Рис. 2. Спектр сигналу генератора перешкод для протидії роботі пасивних радіозакладок (а) і спектр відбитого сигналу генератора перешкод від *p/n* переходу (b)



– – Амплітудна модуляція, – – – частотна модуляція, ── широкосмуговий сигнал

Рис. 3. Завадостійкість систем зв'язку за допомогою шумоподібних сигналів з різною модуляцією

Вважається що стійкість амплітудно-модульованого сигналу при однаковій базі B забезпечується при співвідношенні сигнал-шум $q^2\rho^2 = 1$ рис. 3 [15, с.7]). Рівень шуму в спектральній смузі частот інформаційного сигналу $U_0(t)$ можна зробити набагато більшим ніж спектральна потужність сигналу $A(t)$, що призведе до придушення каналу передачі інформації, який використовує енергію зашумлення в приміщенні. Для досягнення зазначеної мети необхідно провести амплітудну модуляцію шумового високочастотного сигналу (зашумлення) – шумом зі спектром акустичного діапазону. Сигнал зашумлення перестане бути стаціонар-

ним. На виході інтегратора, у якого постійна часу інтегрування $\Delta t < 1/f_m$, з'явиться шум $F_m(t)^2$, спектр якого буде перетинатися зі спектром сигналу модуляції $A(t)$. Розглянемо модуляцію випадкового високочастотного сигналу випадковим низькочастотним сигналом акустичного діапазону. Випадковий низькочастотний сигнал будемо описувати рядом Котельникова з максимальною частотою f_m. Сигнал на виході перемножувача

$$U = \int_t^{t+\Delta t} \mathrm{A}(t)F_m(t)U_0(t)F_m(t)U_0(t)dt \cong \mathrm{A}(t)F_m(t)^2 \int_t^{t+\Delta t} U_0(t)^2 dt \qquad (4)$$

де $U_0(t)$ – випадковий сигнал, що модулюється низькочастотним сигналом $F_m(t) = \sum_{-\infty}^{\infty} \xi_n \frac{\sin(t - n\frac{\pi}{\Omega})}{t - n\frac{\pi}{\Omega}}$, де ξ_n – випадкові амплітуди в відповідні моменти часу. Для забезпечення відсутності перемодуляції, випадкові амплітуди ξ_n повинні підкорятися рівномірному закону розподілу в діапазоні [-1,1]. При відсутності інформаційного сигналу $\mathrm{A}(t) = 1$ і спектр потужності сигналу на виході перемножувача описується виразом

$$P(\omega) = \int_{-\infty}^{\infty} e^{-i\omega\tau} \int_{-\infty}^{\infty} F_m(t)^2 F_m(t+\tau)^2 \, dtd\tau \qquad (5)$$

Графік спектру потужності на виході перемножувача представлений на рис. 4, крива (a). Спектр потужності на виході перемножувача ширше спектра низькочастотної обвідної модулюючого сигналу на вході перемножувача в обох каналах рис. 4, крива (b), тому можна модулювати шумовий сигнал випадковим сигналом з низькочастотним спектром, максимальна частота якого менше передбачуваного інформаційного сигналу. Спектр потужності сигналу на виході перемножувача при наявності інформаційного сигналу визначається виразом

$$P(\omega) = \int_{-T}^{T} e^{-i\omega\tau} \int_{-T}^{T} \mathrm{A}(t)F_m(t)^2 \mathrm{A}(t+\tau)F_m(t+\tau)^2 \, dtd\tau \qquad (6)$$

З огляду на те, що потужність шумової складової $|F_m(t)|^2$ значно перевищує потужність інформаційної складової $|\mathrm{A}(t)|^2$ вхідного сигналу перемножувача, неможливо відновити інформаційний сигнал (рис. 3). В якості ілюстрації було промодельовано передачу гармонійного сигналу радіозакладкою з використанням стаціонарного шуму. Спектр потужності на виході інтегратора для модуляції гармонічним сигналом $\mathrm{A}(t) = \sin\omega_0 t$ стаціонарного шуму визначається виразом

$$P_0(\omega) = \int_{-T}^{T} e^{-i\omega\tau} \int_{-T}^{T} \sin\omega_0 t \sin\omega_0(t+\tau) \, dtd\tau \qquad (7)$$

Вираз (7) є дельта функцією. Реальний сигнал проходить через інтегратор з кінцевим часом інтегрування T, рис. 5 (крива a). Час інтегрування брався рівним $200T_0$, де $T_0 = 2\pi/\omega_0$. На рис. 5 (крива b) представлено графік спектра потужності при модуляції монохроматичним сигналу нестаціонарного зашумлення при однаковому часі інтегрування. Потужність переданого монохроматичного сигналу при використанні нестаціонарного сигналу зашумлення набагато менше. Це обумовлено параметричною взаємодією корисного монохроматичного сигналу з модулюючим сигналом $F_m(t)$. Графік $N = 10log_{10}\left(\frac{P(\omega)}{P_{0(\omega)}}\right)$ на частоті $\omega = 1$ від часу усереднення T в (6) і (7) представлений на рис. 6. Завдяки використанню нестаціонарного шуму інформаційний монохроматичний сигнал послаблюється більш ніж 10 дБ порівняно з передачею такого ж сигналу стаціонарним шумом.

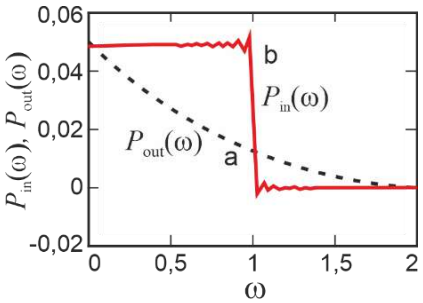


Рис. 4. Спектр потужності моделюючого сигналу на виході перемножувача (a) і на його вході (b)

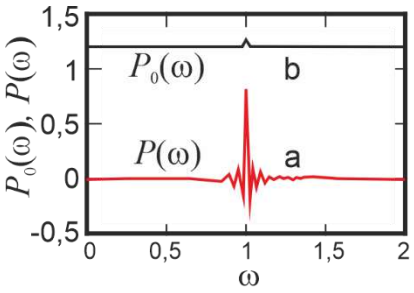


Рис. 5. Спектр потужності інформаційного гармонічного сигналу на виході корелятору при передачі сигналом зашумлення без модуляції (a) і з модуляцією (b)

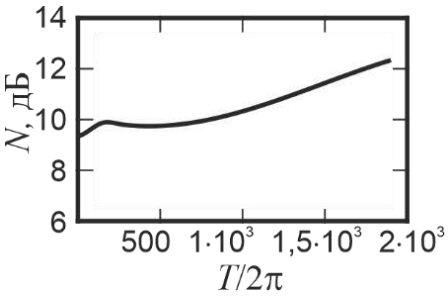


Рис. 6. Залежність послаблення інформаційного монохроматичного сигналу завдяки використанню нестаціонарного шуму від сталої часу корелятору

Висновки

Показано, що для протидії несанкціонованому зніманню інформації пасивними радіозакладками використання нестаціонарного шуму з випадковою 100 % амплітудною модуляцією в смузі частот сигналу, що передається, дозволяє подавити канал передачі інформації радіозакладок. Нестаціонарність шуму в діапазоні сигналу, що передається, призводить до його послаблення завдяки нелінійному перетворенню у перемножувачі кореляційного приймача. Використання вузькосмугових інформаційних сигналів для забезпечення прийнятного відношення сигнал/шум призведе до зниження швидкості передачі інформації, яка буде недостатня для передачі акустичної інформації в реальному масштабі часу.

Список літератури:

1. Encyclopedia of industrial espionage / Under total. ed. E. V. Kurenkova. St. Petersburg: ed. LLC "Publishing house Polygon", 1999. 515p.

2. Youhong Feng, Shihao Yan, Jinhong Yuan. User and Relay Selection With Artificial Noise to Enhance Physical Layer Security // Published 19 September 2018 Computer Science IEEE Transactions on Vehicular Technology. p. 10906-10920.

3. Xing H., Wong K., Chu, Z., Nallanathan A. To Harvest and Jam: A Paradigm of Self-Sustaining Friendly Jammers for Secure AF Relaying // IEEE Trans. Signal Process. 2015, 63, p. 6616–6631.

4. S. S. Kalamkar and A. Banerjee. Secure Communication via a Wireless Energy Harvesting Untrusted Relay // IEEE Transactions on Vehicular Technology, vol. 66, no. 3, pp. 2199-2213, March 2017.

5. Kyriakos Fytrakis, N. Kolokotronis, Konstantinos Katsanos, N. Kalouptsidis. Optimal Cooperative Strategies for PHY Security Maximization Subject to SNR Constraints Computer Science // IEEE Access 2020 DOI: 10.1109 / ACCESS.2020.3005481 Corpus ID: 220466452

6. Youhong Feng, Z. Yang, Shihao Yan, Nan Yang, Bin Lv It is shown that the JUFDRS scheme significantly outperforms the joint user and half-duplex relay selection (JUHDRS) scheme when the self-interference at the FD relay can be reasonably suppressed Computer Science // 2017 IEEE International Conference on Communications (ICC) 2017 TLDR DOI:10.1109/TVT.2018.2870280

7. C. Gong, X. Yue, Z. Zhang, X. Wang and X. Dai. Enhancing Physical Layer Security With Artificial Noise in Large-Scale NOMA Networks // IEEE Transactions on Vehicular Technology, vol. 70, no. 3, pp. 2349-2361, March 2021, doi: 10.1109/TVT.2021.3057661.

8. Serhiienko Sergey, Krizhanovski Vladimir, Chernov Dmitry. Transmission of Information by a Passive Radio Device in the Field of Radio Noise Interference with Transmission on Terrestrial Radio Frequency // Multidisciplinary Research. Abstracts of XIV International Scientific and Practical Conference Bilbao, Spain. December 21–24, 2020. P. 470–474. DOI – 10.46299/ISG.2020.II.XIV

9. Serhiienko S., Krizhanovski V. Modeling of the potential threat of unauth. orized removal of information by a passive radio tab in the rooms protected by noise field // The Fourth International Conference on Information and Telecommunication Technologies and Radio Electronic (UkrMiCo'2019) 09–13 September 2019 Odessa, Ukraine.

10. Serhiienko S.P., Kryzhanovsky V.G., Chernov D.V., Zagoruyko L.V. Effective modes of operation of radiocharging devices for secret recording of information in the field of noise interference // Radio Engineering. 2021. Vip. 205. S. 169-174. DOI:10.30837/rt.2021.2.205.18

11. A. S. Luchinin, I. V. Malygin, A. G. Dolmatov and A. A. Yazovsky. Synchronization and Noise Immunity of Communication Systems Using Signals with Multi-position Modulation // 2018Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO), 2018, pp. 1-5, doi: 10.1109/SYNCHROINFO.2018.8456963.

12. Kyriakos Fytrakis, N. Kolokotronis, Konstantinos Katsanos, N. Kalouptsidis. Optimal Cooperative Strategies for PHY Security Maximization Subject to SNR Constraints Computer Science IEEE Access 2020 DOI: 10.1109 / ACCESS.2020.3005481 Corpus ID: 220466452

13. G. V. Kulikov, A. A. Lelyukh, E. V. Batalov, P. I. Kuzelenkov. Immunity of reception QAM signals in the presence of phase-shift keying interference // Radio electronics journal [electronic journal]. 2019. №7. Access mode: http://jre.cplire.ru/jre/jul19/10/text.pdf DOI 10.30898 / 1684-1719.2019.7.10

14. Alshammari A.S., Sobhy M.I., Lee P. (2018) Digital Communication System with High Security and High Noise Immunity: Security Analysis and Simulation. In: Barolli L., Xhafa F., Conesa J. (eds) Advances on Broad-Band Wireless Computing, Communication and Applications. BWCCA 2017. Lecture Notes on Data Engineering and Communications Technologies, vol 12. Springer, Cham. doi.org/10.1007/978-3-319-69811-3_43

15. Varakin L.E. Communication systems with noise-like signals, Moscow, P.384. https://www.studmed.ru/varakin-le-sistemy-svyazi-sshumopodobnymisignalami_7cfcca93721.html(accessed 14 May, 2019).

Надійшла до редколегії 10.10.2021

Відомості про авторів:

Сергієнко Сергій Петрович – канд. фіз.-мат. наук, доцент, Донецький національний університет імені Василя Стуса (м. Вінниця), доцент кафедри інформаційних технологій; Україна; email: s.serhiienko@donnu.edu.ua; ORCID: https://orcid.org/0000-0001-5515-8946

Крижановський Володимир Григорович – д-р техн. наук, професор, Донецький національний університет імені Василя Стуса (м. Вінниця), професор кафедри інформаційних технологій; Україна; email: v.krizhanovski@donnu.edu.ua; ORCID: https://orcid.org/0000-0002-2685-9740

Чернов Дмитро Вікторович – канд. техн. наук, Донецький національний університет імені Василя Стуса (м. Вінниця), доцент кафедри інформаційних технологій; Україна; email: d.chernov@donnu.edu.ua; ORCID: https://orcid.org/0000-0001-7173-0842

Загоруйко Любов Василівна – канд. техн. наук, Донецький національний університет імені Василя Стуса (м. Вінниця), доцент кафедри інформаційних технологій; Україна; email: l.zahoruiko@donnu.edu.ua; ORCID: https://orcid.org/0000-0002-6958-8696

УДК 621.369:534 **DOI:10.30837/rt.2021.4.207.15**

Д.Ю. ГОРЕЛОВ, канд. техн. наук, Е.А. ИВАНОВА канд. техн. наук,
А.В. ЛИТВИНЕНКО, А.А. ДОВБНЯ, Д.А. МИНИН

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТЕЙ ИСПОЛЬЗОВАНИЯ КЛАВИАТУРНОГО ПОЧЕРКА ДЛЯ ЗАДАЧ ИДЕНТИФИКАЦИИ СТУДЕНТОВ В СИСТЕМАХ ДИСТАНЦИОННОГО ОБРАЗОВАНИЯ

Введение

При использовании систем дистанционного образования (СДО) возникает проблема информационной безопасности учебного процесса, которая, кроме внешних, подразумевает также и внутренние угрозы. Одной из таких угроз может стать студент СДО, который заплатил мошеннику за сдачу тестов и создал видимость учебной деятельности под своим именем. Таким образом, нелегальное получение диплома или сертификата получает удобный механизм реализации.

Использование традиционных методов идентификации в СДО имеет два существенных недостатка: во-первых, неоднозначность идентифицируемого пользователя, поскольку в данном случае установление личности пользователя происходит по введенной парольной фразе; во-вторых, отсутствие возможности обнаружения подмены идентифицированного пользователя в процессе работы с системой (пользователь, заинтересованный в завышении результата оценки знаний, может авторизоваться и передать управление компьютером постороннему лицу). Указанные недостатки устраняются при использовании биометрических методов скрытного мониторинга.

В связи с пандемией коронавируса, начавшейся в 2019 году, актуальность задачи [1 – 7], решаемой в данной статье, резко возросла, поскольку СДО стали использоваться в многих странах вместо традиционного очного обучения.

Обзор методов скрытного биометрического мониторинга

Для решения проблемы распознавания пользователей в СДО необходимо проводить идентификацию не только при входе пользователя в систему, но и регулярно с некоторой периодичностью в течение всего пользовательского сеанса. Таким образом, следует использовать биометрические методы скрытного мониторинга, которые удовлетворяют следующим требованиям: отсутствие необходимости в дополнительном аппаратном оснащении компьютера (ноутбука); простота сбора и анализа биометрических признаков в процессе работы в СДО; возможность идентификации незаметно для пользователя.

Указанным требованиям соответствуют методы идентификации по геометрии лица, по голосу и по клавиатурному почерку [8].

Преимущества идентификации по геометрии лица:

− имеющиеся в личных делах студентов фотографии могут быть использованы в качестве биометрических эталонов;

− бесконтактный и ненавязчивый процесс идентификации;

– идентификацию можно осуществлять в процессе любой деятельности пользователя в СДО: при изучении учебно-методических материалов, сдаче тестов, общении с преподавателем.

Недостатки идентификации по геометрии лица:

– нарушается право на частную жизнь (в процессе идентификации важно именно незаметное использование фронтальной камеры монитора – в противном случае злоумышленникам будут известны промежутки времени, когда у экрана должен находиться студент, а когда – злоумышленник);

– высокая чувствительность алгоритмов распознавания к изменениям положения головы или ракурса, освещения (если студент предпочитает обучаться вечером при выключенном свете в комнате, то его идентификация становится затруднительной).

Преимущества идентификации по голосу – надежность, гибкость и высокие показатели точности. Технология развивается достаточно продолжительное время и сегодня существует большое количество алгоритмов [9], устойчивых к изменяющимся условиям применения – уровню шума, фонемам речи конкретного человека, техническим характеристикам микрофона и т.д.

Недостатки идентификации по голосу:

– возможное отсутствие микрофона у студента СДО;

– голос человека может кардинально измениться из-за болезней, например во время сезонной эпидемии гриппа;

– специфика контрольных тестов: идентификация применима только в случае, если проверка знаний осуществляется при помощи устных ответов на вопрос.

Клавиатурный почерк – уникальный стиль работы на клавиатуре [10], зависящий от таких параметров как: количество пальцев, задействованных во время набора текста; длительность нажатия клавиш; время между нажатиями клавиш; использование основной или дополнительной части клавиатуры; характер сдвоенных или строенных нажатий; излюбленные сочетания горячих клавиш и т.д.

Преимущества идентификации по клавиатурному почерку:

– простота реализации и внедрения (реализация исключительно программная, ввод осуществляется со стандартного устройства ввода – клавиатуры. Это самый дешевый способ аутентификации по биометрическим характеристикам);

– возможность полностью легальной скрытой аутентификации на протяжении всего пользовательского сеанса;

– простота интеграции в мультимодальные биометрические системы (клавиатурный почерк плюс динамика мыши, клавиатурный почерк плюс геометрия лица и т.д.).

Недостатки идентификации по клавиатурному почерку:

– на корректность работы алгоритма аутентификации достаточно сильно влияет психофизическое состояние пользователя;

– для корректной работы алгоритма аутентификации необходим стабильный клавиатурный почерк, который вырабатывается у пользователей, давно работающих на компьютере, следовательно, данный метод нельзя использовать для новичков.

Таким образом, с учетом того, что оценка знаний, как правило, проходит в форме тестирования, наиболее предпочтительным методом идентификации пользователей в системах дистанционного обучения является использование алгоритмов скрытного клавиатурного мониторинга.

Информативные параметры клавиатурного почерка и специфика дистанционного контроля знаний

В задаче идентификации пользователя по клавиатурному почерку основным этапом является анализ и обработка первичных данных. После данной операции входной информативный поток делится на ряд характеристик, которые отражают те или иные динамические признаки набора текста пользователем, который проходит идентификацию. Далее данные признаки позволяют получить ряд уникальных характеристик пользователя.

В настоящее время можно выделить три класса информативных параметров клавиатурного почерка [11, 12].

1. Временные характеристики отдельных событий клавиатуры (монографов), например, абсолютная длительность удержания клавиши, абсолютная длительность паузы перед клавишей, абсолютная длительность паузы после клавиши, отношение длительности паузы перед клавишей к длительности удержания клавиши, отношение среднего значения длитель-

ности удержания конкретной клавиши к среднему значению длительности удержания всех клавиш и т.д.

Информативные параметры монографов клавиатуры формируются для каждой клавиши отдельно, следовательно, обладают важным недостатком: исследуемые интервалы времени всегда связаны с конкретной клавишей и рассчитываются независимо от клавиш, которые нажимались до и после, т.е. не несут информации о динамике набора текста.

2. Временные характеристики последовательных событий клавиатуры (на рис.1 два последовательных события клавиатуры образуют дограф, три последовательных события – триграф, n последовательных событий клавиатуры – n-граф), например, абсолютное значение и распределение длительности всех диграфов в заданном тексте (параметры $t_{A_D B_U}$, $t_{B_D C_U}$ на рис. 2), абсолютные значения и распределения времен между нажатиями (параметры $t_{A_D B_D}$, $t_{B_D C_D}$ на рис. 2) и времен между отпусканиями (параметры $t_{A_U B_U}$, $t_{B_U C_U}$ на рис. 2) клавиш всех диграфов в заданном тексте и т.д.

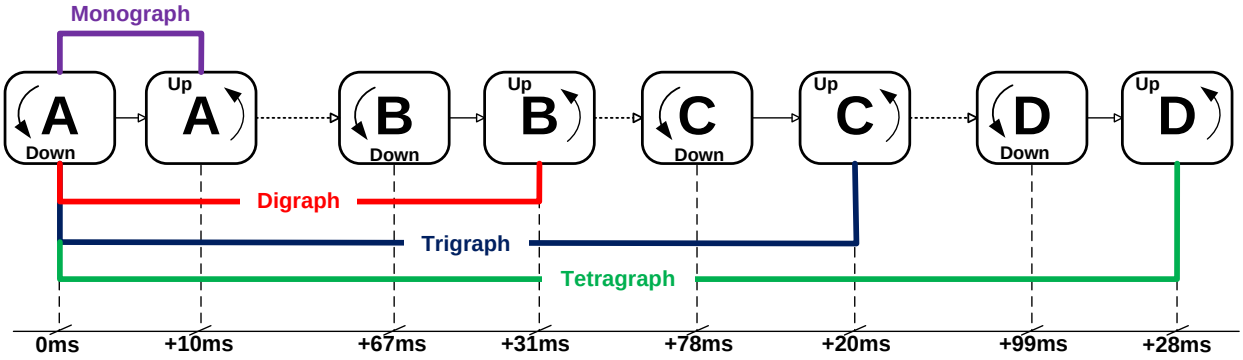


Рис. 1. *N*–графы клавиатуры

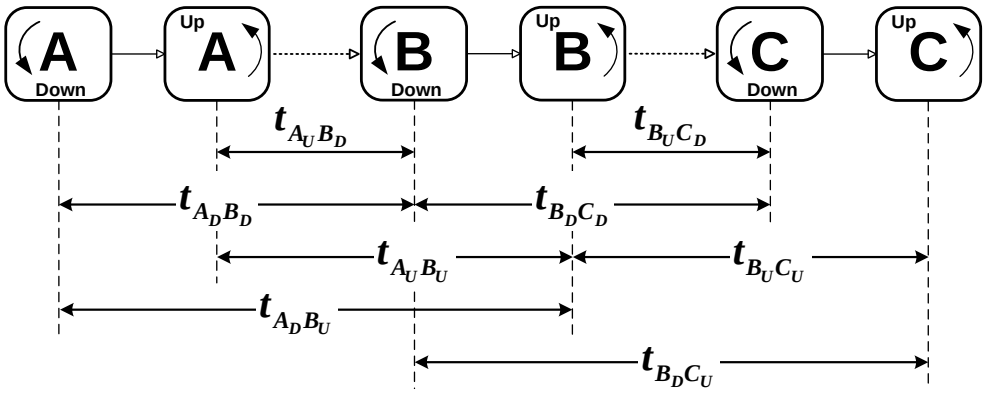


Рис. 2. Временные параметры диграфов клавиатуры

Информативные признаки последовательных событий клавиатуры точнее передают особенности клавиатурного почерка, но также имеют недостаток: для их получения необходимо иметь в несколько раз больший набор данных, чем для получения предыдущей группы характеристик. Также следует отметить, что согласно [13 – 15] переход к анализу отношений временных параметров диграфов, например, $\frac{t_{A_D B_D}}{t_{A_U B_D}}$ и $\frac{t_{A_D B_D}}{t_{A_U B_U}}$, приводит к «нормализации» закона распределения исследуемых признаков, то есть «случайность» изменения параметров клавиатурного почерка уменьшается.

3. Интегральные характеристики набора текста, например, скорость набора символов, скорость набора слов, степень аритмичности набора, количество исправлений, количество и особенности перекрытий (случай нажатия второй клавиши, когда еще не отпущена первая),

распределение частот использования клавиш изменения регистра, пропуск определенных букв в определенных буквосочетаниях/словах, опечатки определенных букв в определенных буквосочетаниях/словах и тому подобное.

Класс интегральных информативных характеристик клавиатурного почерка в сочетании с любым из первых двух классов дает максимальную точность, однако требует значительных затрат на разработку, внедрение и поддержку подобных систем.

В технологиях дистанционного обучения, которые использует мировая педагогическая практика, тестированию уделяется значительное внимание. Хотя тестирование как форма аттестации не является идеальной, однако в дистанционном обучении именно тесты чаще всего представляют собой залог качества полученных знаний.

В настоящее время используется много разновидностей тестов. Условно их можно поделить на две группы [16].

Первая группа – тесты с выбираемыми ответами, их разновидности: 1) тесты опознания – это задания, требующие альтернативного ответа: «согласен» или «не согласен», «да» или «нет» и т.п.; 2) тесты различения – содержат варианты ответов, из которых надо выбрать один или несколько; 3) тесты соотнесения – в них предлагается найти общее или отличное в объектах, соотнося их по свойствам, параметрам, классам и т.д.; 4) тесты-задачи – дается условие задачи, нужные данные и варианты ответов в цифровой или буквенной форме. Студенту нужно выбрать правильный вариант. Задача также может быть сформулирована таким образом, что студенту нужно выбрать правильную последовательность действий и операций или определить зависимость каких-то факторов.

Все эти тесты рассчитаны на проверку знаний-представлений и, отчасти, понимания материала. Такие тесты в наибольшей степени подходят для текущего контроля, а также для самоконтроля.

Вторая группа тестов не содержит вариантов ответов. Такие тесты используются для проверки понимания материала, а также некоторых умений. К ним относятся: 1) тесты-подстановки – в таких заданиях пропущены некоторые составляющие – слова, элементы схем, графиков, и студент должен заполнить пропуски; 2) конструктивные тесты не содержат подсказок и вариантов ответов и требуют от студента самостоятельного конструирования ответа: написания формулы, формулировки свойств, операционной последовательности, выполнения схемы и т.д. Эти тесты, в свою очередь, делятся на два подвида: 1) тесты-задачи – отличие от подобной разновидности первой группы в том, что в нем не предлагаются варианты ответов; тесты-процессы – предназначаются для проверки подготовленности студентов к разработке содержания и последовательности различных процессов.

Таким образом, для использования алгоритмов скрытного клавиатурного мониторинга в задаче идентификации пользователей СДО необходимо:

1) использовать тесты, не содержащие вариантов ответов;

2) использовать тесты при текущем контроле знаний, т.е. в конце каждой лекции или практического занятия (поскольку для формирования биометрического эталона нужно несколько сеансов);

3) использовать тесты с большим количеством вопросов, т.к. объемы текстов, которые вводятся при ответе на каждый вопрос весьма незначительны;

4) использовать тесты с численными ответами. В данном случае анализируются только десять клавиш (цифры от 0 до 9) и 100 возможных диграфов, следовательно, получить необходимую для расчетов «статистику» достаточно легко.

Статическая и динамическая идентификация пользователей по клавиатурному почерку

Идентификация по клавиатурному почерку может быть разделена на два типа: статическая (парольная) и динамическая (непрерывная). Статическая идентификация – это проверка и сопоставление характеристик почерка в процессе набора определенной текстовой последо-

вательности, например логина и пароля пользователя. Непрерывная идентификация направлена на постоянный анализ почерка пользователя во время работы за клавиатурой с целью выявления и сопоставления особенностей почерка.

Парольной идентификации характерен ограниченный набор данных и, как следствие, худшая по сравнению с динамической идентификацией точность. В СДО парольную идентификацию следует использовать как вспомогательное средство в двух случаях, во-первых, когда основной модуль скрытного мониторинга не дал точного идентификационного решения; во-вторых, когда факт сдачи теста третьим лицом уже установлен и по динамике набора парольной фразы проводится идентификация этого лица с целью добавления его в черный список.

Можно выделить два этапа скрытой идентификации пользователя: качественный и количественный. Первый обнаруживает различия в заранее выявленных индивидуальных особенностях работы с клавиатурой легального пользователя. Это использование альтернативных служебных клавиш (например, клавиши Backspace и Delete, CapsLock и правый/левый Shift) использование клавиш дополнительной клавиатуры и др. Эти особенности проявляются на подсознательном уровне, и попытка контролировать их неизбежно отразится на изменении динамики почерка. Второй этап предусматривает продление сбора и анализа ключевых временных характеристик клавиатурного почерка после того, как пользователь уже вошел в систему. Таким образом, мониторинг характера клавиатурной активности выполняется в течение всей рабочей сессии под конкретным аккаунтом. По мере накопления статистических данных происходит уточнение сходства эталона по вновь сформированной совокупности параметров.

Описание алгоритма формирования профиля пользователя и его идентификации

1. Сочетанием качественного и количественного подходов является анализ диграфов ответов-чисел вида «клавиша А – десятичный разделитель», «десятичный разделить – клавиша А» и «клавиша А – клавиша В».

К качественному подходу относятся:

1) распределение частот использования групп цифровых клавиш, а также знаков «плюс» и «минус» – основная или вспомогательная клавиатура (рис. 3);

2) распределение частот использования клавиш-разделителей целой и дробной части – клавиши «,» и «.» в английской раскладке, клавиши «б», «ю» и «.» в украинской раскладке, клавиша «,» на вспомогательной клавиатуре в английской/украинский раскладке.

Рис. 3. Разделение клавиш клавиатуры на функциональные блоки

1. Количественный подход начинается с формирования профиля пользователя путем накопления данных о временных интервалах каждого диграфа введенных пользователем ответов-чисел:

$$T_1 = \begin{vmatrix} t_{1A_DB_D} \\ t_{2A_DB_D} \\ \dots \\ t_{N_{AB}A_DB_D} \end{vmatrix}, \quad T_2 = \begin{vmatrix} t_{1A_UB_D} \\ t_{2A_UB_D} \\ \dots \\ t_{N_{AB}A_UB_D} \end{vmatrix}, \quad T_3 = \begin{vmatrix} t_{1A_UB_U} \\ t_{2A_UB_U} \\ \dots \\ t_{N_{AB}A_UB_U} \end{vmatrix}, \quad T_4 = \begin{vmatrix} t_{1A_DB_U} \\ t_{2A_DB_U} \\ \dots \\ t_{N_{AB}A_DB_U} \end{vmatrix}, \qquad (1)$$

где N_{AB} – количество повторений диграфа «AB».

2. Пять процентов самых быстрых и пять процентов медленных диграфов изымаются из анализа. Таким образом, можно исключить случайные хаотичные нажатия клавиш – быстрые диграфы и случаи, когда пользователь отвлекся на длительное время и нажал одну кнопку – медленные диграфы.

3. ***Подалгоритм 1.*** Построение профиля и правило идентификации пользователя на основе девиации Δt_{AB} длительности диграфов (клавиши «A» и «B» принимают значения «.», «0», «1», … «9»).

3.1. Для каждого диграфа рассчитывается значение относительной девиации длительности:

$$\Delta t_{AB} = \frac{1}{N_{AB} \cdot \Delta t} \sum_{i=1}^{N_{AB}} t_{A_DB_U\,i}, \qquad (2)$$

где средняя длительность по всем возможным диграфам равна:

$$\Delta t = \frac{1}{L} \sum_{j=1}^{L} t_{X_DY_U\,j}, \qquad (3)$$

L – общее количество диграфов; клавиши «X» и «Y» принимают значения «.», «0», «1», … «9».

3.2. По результатам п. 3.1 строится табличный профиль пользователя (табл. 1), причем значения относительной девиации записываются в таком формате:

если $\Delta t_{AB} \geq 1$, то $\Delta t_{AB} = 1$;

если $\Delta t_{AB} < 1$, то $\Delta t_{AB} = -1$.

Таблица 1

Пример формирования профиля пользователя

Первая клавиша диграфа	Вторая клавиша диграфа	Параметр Δt_{AB}
.	0	1
.	1	-1
.	2	1
.	3	1
.	4	-1
.	5	-1
.	6	1
.	7	-1
.	8	1
.	9	1
0	.	-1
0	0	1
0	1	1
0	2	-1
…	…	…
9	7	-1
9	8	1
9	9	-1

3.3. На втором шаге (по окончании второго текущего контроля знаний) уточняется профиль пользователя:

1) рассчитывается новое среднее значение длительности диграфов Δt;
2) рассчитываются новые значения относительной девиации Δt_{AB};
3) строится новый табличный профиль пользователя;
4) профили объединяются по формуле (табл. 2):

$$\Delta t_{AB} = \Delta t_{AB1} + \Delta t_{AB2} = \begin{cases} 2, & \textit{если} \;\; \Delta t_{AB1} = \Delta t_{AB2} = 1, \\ -2, & \textit{если} \;\; \Delta t_{AB1} = \Delta t_{AB2} = -1, \\ 0, & \textit{ели} \;\; \Delta t_{AB1} \neq \Delta t_{AB2}. \end{cases} \qquad (4)$$

3.4. На третьем шаге (по окончании третьего текущего контроля знаний) уточняется профиль пользователя:

1) рассчитывается новое среднее значение длительности диграфов Δt;
2) рассчитываются новые значения относительной девиации Δt_{AB};
3) строится новый табличный профиль пользователя;
4) профили объединяются по формуле

$$\Delta t_{AB} = \Delta t_{AB1} + \Delta t_{AB2} + \Delta t_{AB3} = \begin{cases} \pm 3, & если \ \ \Delta t_{AB1} = \Delta t_{AB2} = \Delta t_{AB3}, \\ \pm 1, & если \ \ \Delta t_{AB1} \neq \Delta t_{AB2} \neq \Delta t_{AB3}. \end{cases} \quad (5)$$

3.5. На шестом шаге (по окончании шестого текущего контроля знаний) формируется табличный профиль пользователя. Значения параметров Δt_{AB} после объединения становятся равными $\{-6;\ -4;\ -2;\ 0;\ 2;\ 4;\ 6;\}$. Сформированный профиль графически (рис. 4) удобно представлять в виде двух 3D диаграмм.

Таблица 2

Пример формирования уточненного профиля пользователя

Первая клавиша диграфа	Вторая клавиша диграфа	Параметр Δt_{AB1}	Параметр Δt_{AB2}	Параметр Δt_{AB}
.	0	1	1	2
.	1	-1	1	0
.	2	1	-1	0
.	3	1	1	2
.	4	-1	-1	-2
.	5	-1	1	0
.	6	1	1	2
.	7	-1	-1	-2
.	8	1	-1	0
9	7	-1	-1	-2
9	8	1	-1	0
9	9	-1	-1	-2

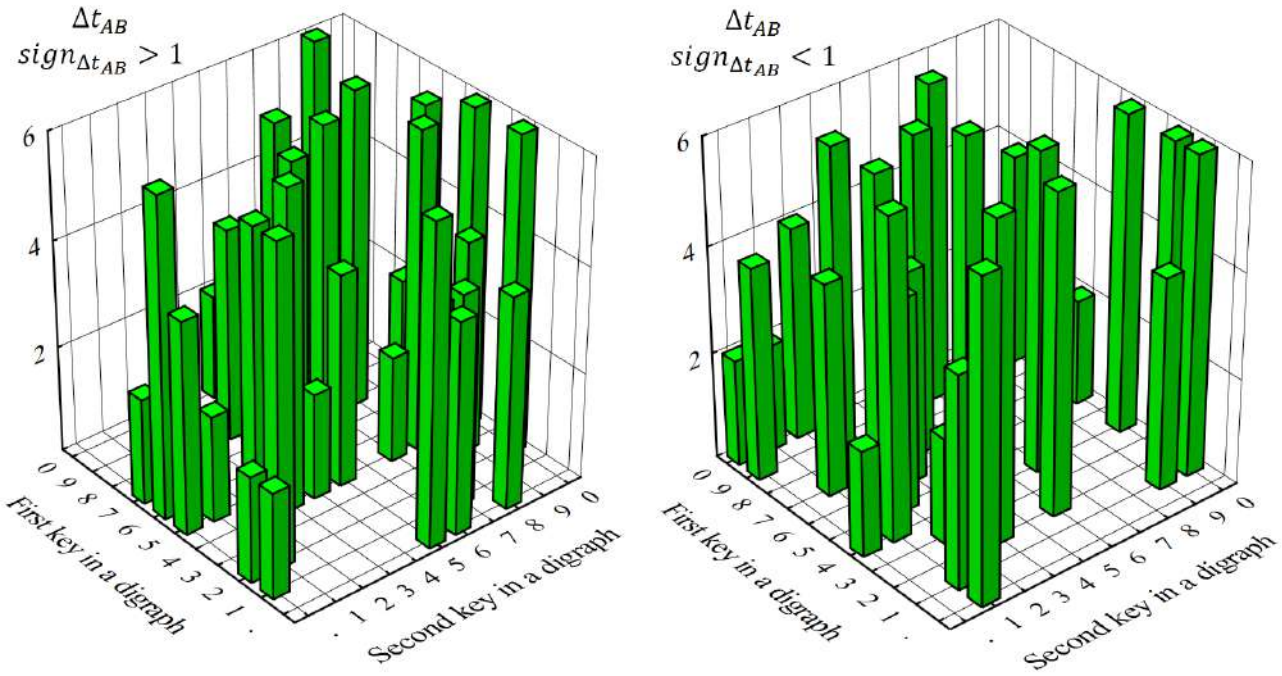


Рис. 4. Пример представления профиля пользователя в виде 3D диаграмм

3.6. Формируется вектор биометрического профиля пользователя:

$$V_{\Delta t_{AB}} = \begin{vmatrix} \Delta t_{.0} \\ \Delta t_{.1} \\ \Delta t_{.2} \\ \dots \\ \Delta t_{99} \end{vmatrix} \quad (6)$$

и рассчитывается его норма

$$n_{\Delta t_{AB}} = \sqrt{\sum_{i=1}^{119} \Delta t_{AB_i}^{\ 2}}. \quad (7)$$

Как видно из (7), все диграфы с нулевым значением Δt_{AB} не участвуют в формировании профиля пользователя.

3.7. На этапе идентификации пользователя выполняются следующие шаги.

3.7.1. Рассчитываются значения относительной девиации длительности диграфов δt_{AB} и приводятся к виду $\delta t_{AB} = \pm 1$.

3.7.2. Рассчитывается вектор идентификации:

$$V_{\delta t_{AB}} = \begin{vmatrix} v_{.0} \\ v_{.1} \\ v_{.2} \\ \dots \\ v_{99} \end{vmatrix}, \quad v_i = \begin{cases} \Delta t_{AB_i}, & \textit{если } \Delta t_{AB_i} \cdot \delta t_{AB_i} > 0, \\ 0, & \textit{если } \Delta t_{AB_i} \cdot \delta t_{AB_i} < 0; \end{cases} \quad (8)$$

и рассчитывается его норма:

$$n_{\delta t_{AB}} = \sqrt{\sum_{i=1}^{119} v_i^2}. \quad (9)$$

3.7.3. В соответствии со значениями нормы вектора идентификации $n_{\delta t_{AB}}$ и нормы вектора биометрического профиля пользователя $n_{\Delta t_{AB}}$ принимается решение о подлинности пользователя:

$$Rule_{\Delta t_{AB}} = \begin{cases} 1, & \textit{если } n_{\delta t_{AB}} \geq 0.7 n_{\Delta t_{AB}}, \\ 0, & \textit{иначе.} \end{cases} \quad (10)$$

4. Аналогично п. 3 формируются профиль (вектор $V_{\Delta t_{AB}^{pause}}$) и правило идентификации $Rule_{\Delta t_{AB}^{pause}}$ на основе относительной девиации длительности паузы в диграфах.

5. Аналогично п. 3 формируются профиль (вектор $V_{\Delta t_{AB}^{A/DD}}$) и правило идентификации $Rule_{\Delta t_{AB}^{A/DD}}$ на основе относительной девиации отношения времени нажатия первой клавиши диграфов ко времени между нажатиями клавиш в диграфах.

6. Аналогично п. 3 формируются профиль (вектор $V_{\Delta t_{AB}^{B/UU}}$) и правило идентификации $Rule_{\Delta t_{AB}^{B/UU}}$ на основе относительной девиации отношения времени нажатия второй клавиши диграфов ко времени между отжатиями клавиш в диграфах.

7. Общее решение о подлинности пользователя принимается на основе частных:

$$Rule = \begin{cases} Rule_{\Delta t_{AB}} + Rule_{\Delta t_{AB}^{pause}} + Rule_{\Delta t_{AB}^{A/DD}} + Rule_{\Delta t_{AB}^{B/UU}} \geq 3 \; - \; \text{пользователь подлинный,} \\ Rule_{\Delta t_{AB}} + Rule_{\Delta t_{AB}^{pause}} + Rule_{\Delta t_{AB}^{A/DD}} + Rule_{\Delta t_{AB}^{B/UU}} < 2 \; - \; \text{пользователь не подлинный,} \\ RA_{\Delta t_{AB}} + RA_{\Delta t_{AB}^{A}} + RA_{\Delta t_{AB}^{B}} + RA_{\Delta t_{AB}^{P}} = 2 \; - \; \text{использование качественого подхода.} \end{cases} \quad (11)$$

В третьем случае, когда $Rule = 2$, подлинность пользователя проверяется с использованием качественного подхода. Если частоты использования групп цифровых клавиш, клавиш «плюс», «минус» и клавиш разделителей целой и дробной части для более чем 75 % диграфов совпадают с эталоном, то принимается решение о положительной идентификации.

Результаты исследований и выводы

Тестовую группу составили восемь студентов и аспирантов в возрасте от 20 до 30 лет, каждый из которых ежедневно работает за компьютером и имеет стабильный клавиатурный почерк.

За время эксперимента каждый пользователь сделал по восемь подходов в привычной для него обстановке, на своей клавиатуре, что позволило снизить влияние внешних факторов на почерк и собрать более точные данные. Каждый из подходов состоял из ввода 200 цифровых диграфов, таким образом, в течение каждого подхода пользователь находился в разных психофизических состояниях: медлительность и неуверенность в первых попытках, стабильность в середине, усталость и путаность ближе к концу подхода.

В результате было собрано базу, состоящую из 51200 записей о временных параметрах $t_{A_D B_U}$, $t_{A_U B_D}$, $\frac{t_{A_D A_U}}{t_{A_D B_D}}$, $\frac{t_{B_D B_U}}{t_{A_U B_U}}$. Далее данные были разделены на две части: первую, учебную, выборку составили 38400 записей (восемь пользователей, шесть подходов, 200 диграфов в подходе); вторую, тестовую, составили 12800 записей (восемь пользователей, два подхода, 200 диграфов в подходе).

Ошибка FRR рассчитывалась следующим образом. Для каждого пользователя был сформирован эталон, который сравнивался с двумя тестовыми профилями этого же пользователя. Таким образом, было проведено 8×2=16 аутентификационных тестов. Одно аутентификационное решение было неверным, то есть ошибка FRR составила 6,25 %.

Ошибка FAR рассчитывалась следующим образом. Для каждого пользователя был сформирован эталон, который сравнивался с двумя тестовыми профилями последних семи пользователей. Таким образом, было проведено 8×2×7=112 идентификационных тестов. Пять идентификационных решений были неверными, то есть ошибка FAR составила 4,64 %.

Полученные ошибки классификации пользователей близки к таковым, например, из [1, 6, 7]. Конечно, в реальных условиях объемы данных о временных параметрах диграфов для формирования эталонных и тестовых профилей могут оказаться значительно меньшими, а следовательно, и ошибки FRR и FAR будут иметь более высокие значения. Однако на самый главный вопрос этих исследований – о принципиальной возможности использовать предложенную методику для скрытного мониторинга клавиатурного почерка слушателей СДО – проведенные исследования дали положительный ответ.

Сохранить точность предложенного метода идентификации и уменьшить необходимый объем данных о диграфах клавиатуры можно с помощью мультимодальных систем идентификации. Например, одновременно с клавиатурным почерком отслеживать динамику курсора компьютерной мыши или анализировать совокупность данных, которые сервер СДО может получить о компьютере и браузере пользователя, запросив эту информацию при загрузке веб-страницы (параметры Browser Fingerprints).

Список литературы:

1. Zamfiroiu, Alin, Diana Constantinescu, Mădălina Zurini, and Cristian Toma. Secure Learning Management System Based on User Behavior. Applied Sciences 10, no. 21 (October 2020): 7730. DOI:10.3390/app10217730.

2. Marcela Hernández de Menéndez, Ruben Morales-Menendez, Carlos A. Escobar, Jorge Arinez. Biometric applications in education. International Journal on Interactive Design and Manufacturing (IJIDeM) 15(5). September 2021 DOI:10.1007/s12008-021-00760-6.

3. Rajamanogaran, M.; Subha, S.; Baghavathi Priya, S. Contactless Attendance Management System using Artificial Intelligence. Journal of Physics: Conference Series, Volume 1714, Issue 1, article id. 012006 (2021). DOI: 10.1088/1742-6596/1714/1/012006.

4. Jack Curran, Kevin Curran. Biometric Authentication Techniques in Online Learning Environments. In book: Biometric Authentication in Online Learning Environments (pp.266-278). January 2019. DOI:10.4018/978-1-5225-7724-9.ch011.

5. Aeri Leea, Jin-young Hanb. Effective User Authentication System in an E-Learning Platform. International Journal of Innovation, Creativity and Change (pp. 1101-1113). Volume 13, Issue 3, 2020.

6. Adetoba B.T., Awodele O., Kuyoro S.O., Nwaocha O. An Improved Authentication and Monitoring System for E-Learning Examination Using Supervised Machine Learning Algorithms (pp. 235-242). International Journal of Scientific & Engineering Research Volume 11, Issue 3, March-2020.

7. Amr Jadi. New Detection Cheating Method of Online-Exams during COVID-19 Pandemic (pp. 123-130).International Journal of Computer Science and Network Security. VOL.21 No.4, April 2021. https://doi.org/10.22937/IJCSNS.2021.21.4.17

8. A.V.S. Kumar, Biometric authentication in online learning environments. IGI Global, Information Science Reference, an imprint of IGI Global, 2019.

9. Homayoon Beigi. Fundamentals of Speaker Recognition. Springer Science + Business Media; 2011.

10. Teh P S, Teoh A B J, Yue S. A Survey of Keystroke Dynamics Biometrics, The Scientific World Journal, vol. 2013, Article ID 408280, 2013, 24 pages.

11. Заяць В.М., Уліцький О.О. Алгоритмічне та програмне забезпечення системи розпізнавання людини за її рукомоторними реакціями // Вісник Держ. ун-ту «Львівська політехніка» «Комп'ютерна інженерія та інформаційні технології». 2000. № 392. С.73 – 76.

12. Тушканов Е.В. Разработка методов и алгоритмов повышения защищенности информации на основе анализа клавиатурного почерка : дис. канд. техн. наук / Санкт-Петербург. нац. исслед. ун-т информационных технологий, механики и оптики, Санкт-Петербург, 2016. 118 с.

13. Vasyl Alieksieiev, Aleksey Strelnitskiy, Dmitry Gavva, Denis Gorelov, Yuliia Synytsia. Studying of keystroke dynamics statistical properties for biometric user authentication. Proceedings of 14th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), Pages 559-563, 2018.

14. Дослідження статистичних властивостей клавіатурного почерку для вирішення задач аутентифікації користувачів комп'ютерних мереж / Д. Ю. Горелов, В. О. Алєксєєв, В. М. Бублик, Д. В. Маслій // Радиотехника. 2019. Вып. 197. С. 78-85.

15. Дослідження інформативних параметрів диграфів клавіатурного почерку для задач ідентифікації користувачів комп'ютерних мереж / Д. Ю. Горелов, О. О. Іванова, О. В. Кокорін, Д. В. Маслій, О. В. Литвиненко // Радіотехніка. 2020. Вип. 201. С. 194-200.

16. Калмыков А.А., Орчаков О.А., Попов В.В Дистанционное обучение. Введение в педагогическую технологию : учеб. пособие / МГТУ МИРЭА. Москва, 2005. 196 с.

Поступила в редколлегию 07.11.2021

Сведения об авторах:

Горелов Денис Юрьевич – кандидат технических наук, доцент, Харьковский национальный университет радиоэлектроники, доцент кафедры компьютерной радиоинженерии и систем технической защиты информации, Украина; email: denis.gorelov@nure.ua; ORCID: https://orcid.org/0000-0002-0845-8070.

Иванова Елена Александровна – кандидат технических наук, доцент, Харьковский национальный университет радиоэлектроники, доцент кафедры компьютерной радиоинженерии и систем технической защиты информации, Украина; email: olena.ivanova1@nure.ua; ORCID: https://orcid.org/0000-0001-9970-7951.

Литвиненко Александр Викторович – аспирант кафедры безопасности информационных технологий, Харьковский национальный университет радиоэлектроники, Украина; email: oleksandr.lytvynenko@nure.ua.

Довбня Андрей Анатольевич – аспирант кафедры безопасности информационных технологий, Харьковский национальный университет радиоэлектроники, Украина; email: andrii.dovbnia@nure.ua.

Минин Дмитрий Александрович – аспирант кафедры безопасности информационных технологий, Харьковский национальный университет радиоэлектроники, Украина; email: dmytro.minin@nure.ua.

УДК 537.868 **DOI:10.30837/rt.2021.4.207.16**

Г.Л. КОМАРОВА, канд. техн. наук

ВЛИЯНИЕ ФЕРРИМАГНИТНОГО РЕЗОНАНСА НА ПРЕОБРАЗОВАНИЕ ЭНЕРГИИ ЭЛЕКТРОМАГНИТНОЙ ВОЛНЫ ЖИГ-РЕЗОНАТОРОМ В МЕХАНИЧЕСКУЮ ЭНЕРГИЮ

Постановка проблемы

Известные научные разработки, направленные на создание преобразователей электромагнитной энергии СВЧ в механическую энергию, показывают, что они имеют чрезвычайно малую силу тяги, равную $4 \cdot 10^{-6}$ мН/кВт [1], 0,6 мН/кВт [2], (1,2-2) мН/кВт [3, 4], 53 мН/кВт [4]. Основными элементами таких преобразователей являются генератор СВЧ, электромагнитная волна, металлический экран, диэлектрический либо сегнетоэлектрический эллипсоид, ферритовый цилиндр либо сфера.

Этот недостаток не позволяет использовать их в промышленных условиях. Поэтому разработка новых методов преобразования электромагнитной энергии СВЧ в механическую энергию является актуальной.

Цель работы – усовершенствование метода преобразования электромагнитной энергии СВЧ в механическую энергию.

Анализ последних исследований и публикаций

Для совершенствования метода преобразования электромагнитной энергии в механическую энергию использованы результаты следующих исследований.

В работе [5] предложен метод преобразования энергии неоднородной электромагнитной волны в механическую энергию. Метод преобразования заключается в изготовлении преобразователя из ферримагнетика и воздействия на него постоянным магнитным полем и неоднородным электромагнитным полем. При этом величина напряженности постоянного магнитного поля соответствует возникновению ферримагнитного резонанса. Технический результат – увеличение коэффициента преобразования электромагнитной энергии в механическую энергию.

В работе [6] предложен метод преобразования энергии неоднородной электромагнитной волны в механическую энергию. Метод преобразования заключается в изготовлении преобразователя из сегнетоэлектрика и воздействия на него постоянным электрическим полем и неоднородным электромагнитным полем. При этом величина напряженности постоянного электрического поля соответствует возникновению сегнетоэлектрического резонанса. Технический результат – увеличение коэффициента преобразования электромагнитной энергии в механическую энергию.

В работе [2] в нулевом приближении получен алгоритм вычисления силы, с которой неоднородная электромагнитная волна, распространяющаяся в прямоугольном волноводе, действует на ферритовый шар. Результаты теоретических исследований сопоставлены с результатами эксперимента. Электромагнитная волна мощностью 10 Вт, распространяющаяся в прямоугольном волноводе с поперечным сечением $10 \cdot 23$ мм^2, действует на ферритовый шар диаметром 3,55 мм, помещенный в постоянное магнитное поле, величина которого соответствует ферримагнитному резонансу с силой, равной $(6 \pm 0{,}5) \cdot$мкН. Недостатком этих исследований является то, что они справедливы только для ферритовых шаров малых размеров и малых величин напряженности магнитного поля электромагнитной волны.

В работе [3] исследовано силовое воздействие неоднородной электромагнитной волны на диэлектрический диск, помещенный во внутренней части замкнутого несимметричного металлического объема. Уровень силового воздействия неоднородной волны составляет 1,2 мН/кВт. В качестве преобразователя электромагнитной энергии в механическую используется диэлектрический диск. Не исследовано влияние на силовое воздействие энергии СВЧ: геометрических размеров диска, геометрической формы преобразователя (цилиндр, шар), материала из которого он изготовлен.

В работе [4] исследовано силовое действие стоячей электромагнитной волны на ферритовый цилиндр произвольного диаметра, помещенный в постоянное магнитное поле. Применение пространственного резонанса (совпадение размера диаметра цилиндра с размером длины электромагнитной волны в цилиндре) и стоячей электромагнитной волны позволило увеличить до 53 мН/кВт силу тяги ферритового преобразователя. Не исследовано силовое действие стоячей электромагнитной волны на ферритовый шар произвольного диаметра.

В работе [7] исследовано распространение электромагнитных волн в 3D-решетках магнитных цилиндрических нанопроволок в условиях магнитного резонанса. Исследования подтверждают влияние взаимной ориентации постоянного и высокочастотных магнитных полей на коэффициент распространения. Силовое действие электромагнитных волн на магнитные материалы в области магнитного резонанса не исследовано.

В работах [8, 9] разработана аналитическая теория электромагнитных явлений в резонансных сложных пространственных системах малых резонансных однородных изотропных магнитодиэлектрических сферах. Исследовано влияние явления пространственного резонанса на рассеянное электромагнитное поле. Недостаток: исследование проведено в рамках квазистационарного приближения (электромагнитное поле вдоль сечения сферы предполагается постоянным).

Из анализа известных работ следует, что для увеличения силового воздействия электромагнитной волны на ферритовый преобразователь в качестве преобразователя необходимо использовать ферритовую сферу. Поместить ее в стоячую электромагнитную волну. Создать условия, во-первых, для возникновения резонанса между движением магнитных моментов доменов феррита и движением вектора напряженности неоднородного магнитного поля электромагнитной волны и, во-вторых, – для возникновения пространственного резонанса.

Для достижения поставленной в этой работе цели необходимо:

– исследовать связь между напряженностью магнитного поля в стоячей электромагнитной волне и в середине ферритовой сферы произвольного диаметра;

– разработать алгоритм вычисления влияния ферримагнитного и пространственного резонансов на преобразование энергии стоячей электромагнитной волны ферритовой сферою в механическую энергию;

– исследовать преобразование электромагнитной энергии СВЧ ферритовой сферой произвольного радиуса в механическую энергию.

Разработка алгоритма вычисления переменного магнитного поля внутри ферритовой сфере

Рассмотрим падение плоской поляризованной электромагнитной волны 1, на ферритовую сферу 2, что находится в постоянном магнитном поле 3 и металлический экран 4. Физическая модель этого процесса представлена на рис. 1.

Радиус сферы равен R. Металлический экран расположен в точке с координатой z равной L, а центр сферы размещен в точке с координатой z равной 0. Вектор электрической напряженности электромагнитной волны имеет направление параллельное направлению оси y, а вектор магнитной напряженности параллельный оси x.

Среда в середине ферритовой сферы характеризуется параметрами: диэлектрическая проницательность – $\varepsilon\cdot\varepsilon_o$, магнитная проницательность – $\mu\cdot\mu_o$, постоянная распространения электромагнитной волны – $k = \omega\cdot(\varepsilon\cdot\varepsilon_o\ \mu\cdot\mu_o)^{1/2}$, волновое сопротивление –

$\rho = (\mu \cdot \mu_o / \varepsilon \cdot \varepsilon_o)^{1/2}$, длина волны – $\lambda = 2\pi/k$. Внешняя среда характеризуется параметрами: диэлектрическая проницательность – ε_o, магнитная проницательность – μ_o, постоянная распространения электромагнитной волны – $k_o = \omega \cdot (\varepsilon_o \cdot \mu_o)^{1/2}$, волновое сопротивление – $\rho_o = (\mu_o / \varepsilon_o)^{1/2}$, длина волны – $\lambda_o = 2\pi/k_o$.

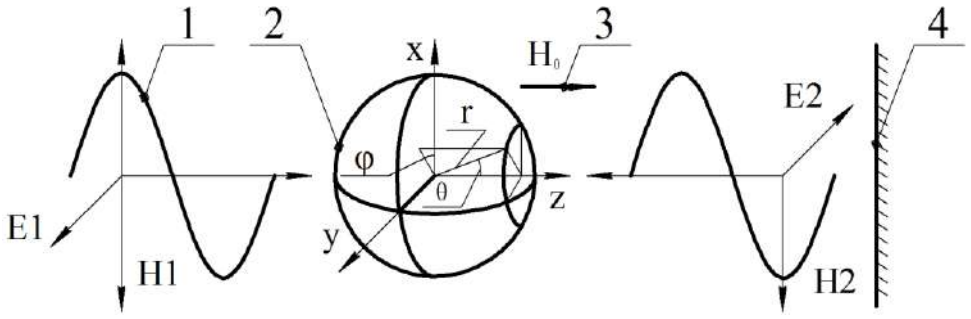


Рис. 1. Физическая модель объекта исследования

Плоско поляризованная электромагнитная волна в соответствии с принципом суперпозиции может быть представлена в виде суммы двух волн [11]:

$$H1 = H1^{л} + H1^{п}, \tag{1}$$

где $\boldsymbol{H1^{л}}$ – вектор магнитной напряженности электромагнитной волны, которая имеет левую круговую поляризацию, $\boldsymbol{H1^{п}}$ – правую круговую поляризацию.

После размещения ферритовой сферы в постоянном магнитном поле $\boldsymbol{B_o}$ магнитные моменты $\mathbf{p_i}$ ее доменов и вектор намагниченности $\boldsymbol{J_n}$ будут вращаться вокруг вектора магнитной индукции $\boldsymbol{B_o}$. $p_i = p_i \cdot (-\mathbf{y_o} + i \cdot \mathbf{z_o}) \exp(\omega_o \cdot t + \varphi_i)$ где $\mathbf{y_o}$, $\mathbf{z_o}$ – единичные орты направлены вдоль осей $\mathbf{y_o}$, $\mathbf{z_o}$; ω_o – угловая частота, c^{-1}; i – мнимая единица, ($i^2 = -1$); t – время, с; φ_i – начальная фаза [11]:

Вектор магнитной напряженности $\boldsymbol{H1^{л}}$ электромагнитной волны, которая имеет левую круговую поляризацию, вращается в одном направлении с вектором намагниченности $\boldsymbol{J_n}$. Вектор $\boldsymbol{H1^{п}}$ и вектор $\boldsymbol{J_n}$ вращаются в противоположных направлениях. Поэтому электромагнитная волна, которая имеет правую круговую поляризацию, слабо взаимодействует с ферритовой сферою. Ее силовым воздействием на ферритовую сферу можно пренебречь.

Электромагнитную волну, которая имеет левую круговую поляризацию в соответствии с принципом суперпозиции можно представить в виде суммы двух плоско поляризованных волн:

$$\boldsymbol{H1^{л}} \cdot = \left(- \mathbf{x_o} + i \cdot \mathbf{y_o}\right) \cdot \frac{H_o}{2} \cdot e^{i \cdot (\omega \cdot t - k \cdot x)}, \tag{2}$$

$$\boldsymbol{H1^{л}} = \boldsymbol{x_o} \cdot H11 + \mathbf{y_o} \cdot H12. \tag{3}$$

Аналогичным образом отраженную электромагнитную волну, которая имеет левую круговую поляризацию, можно представить суммой двух плоско поляризованных волн:

$$\boldsymbol{H2^{л}} = \boldsymbol{x_o} \cdot H21 + \mathbf{y_o} \cdot H22. \tag{4}$$

Отраженная от металлического экрана волна и падающая создают стоячую электромагнитную волну:

$$H^{л} = H1^{л} + H2^{л}. \tag{5}$$

Стоячая электромагнитная волна индуцирует электромагнитное поле в середине ферритовой сфере $\boldsymbol{H^{ч}}$, $\boldsymbol{E^{ч}}$.

Рассмотрим случай, когда металлический экран размещен на большом расстоянии от ферритовой сферы ($|L|/\lambda_o >> 1$). В этом случае энергией отраженных от металлического экрана рассеянных электромагнитных волн сферой можно пренебречь.

Составляющие электромагнитных полей, индуцированные стоячей волной в середине ферритовой сферы можно выразить через составляющие падающей и отраженной от металлического экрана электромагнитных волн $E11_x$, $H12_y$, $E21_x$, $H22_y$. Эти составляющие можно представить следующими выражениями [13].

Для падающих волн:

$$E11_x \cdot = E_m \cdot e^{-i(\omega \cdot t + k \cdot (z+L))}, \tag{6}$$

$$H12_y = i \cdot H_m \cdot e^{-i(\omega \cdot t + k \cdot (z+L))}. \tag{7}$$

Для отраженных волн:

$$E21_x \cdot = -E_m \cdot e^{-i[\omega \cdot t - k(z+L)]}, \tag{8}$$

$$H22_y \cdot = i \cdot H_m \cdot e^{-i[\omega \cdot t - k(z+L)]}. \tag{9}$$

где E_m, H_m – амплитудные значения напряженности электрического и магнитного полей электромагнитной волны ($E_m = \rho o\, H_m$).

Падающая электромагнитная волна $E11_x$ создает внутри ферритовой сферы электромагнитную волну, которую можно представить следующим выражением [13]:

$$\boldsymbol{H11^c} = H_m \sum_{n=-1}^{\infty} i^n \frac{2 \cdot n + 1}{n \cdot (n+1)} \left[\boldsymbol{r_o} i a_n N_1^E + \boldsymbol{\theta_o} \left(b_n M_2^E + i a_n N_2^E \right) + \varphi_{\boldsymbol{o}} \left(b_n M_3^E + i a_n N_3^E \right) \right], \tag{10}$$

$$M_2^E = -\frac{1}{\sin\theta} \cdot J_n(\rho_2) \cdot P_m^1(\cos\theta) \cdot \sin\varphi; \quad M_3^E = -\cdot J_n(\rho_2) \cdot \left[\frac{d}{d\theta} P_m^1(\cos\theta) \right] \cdot \cos\varphi;$$

$$N_1^E = \frac{n \cdot (n+1)}{\rho_2} \cdot J_n(\rho_2) \cdot P_m^1(\cos\theta) \cdot \sin\varphi;$$

$$N_2^E = \frac{1}{\rho_2} \cdot \left[\frac{d}{d(\rho_2)} \rho_2 \cdot J_n(\rho_2) \right] \cdot \left[\frac{d}{d\theta} P_m^1(\cos\theta) \right] \cdot \sin\varphi$$

$$N_3^E = \frac{1}{\rho_2 \cdot \sin\theta} \cdot \left[\frac{d}{d(\rho_2)} \cdot \rho_2 \cdot J_n(\rho_2) \right] \cdot P_m^1(\cos\theta) \cdot \cos\varphi; \quad H_o = -i \cdot \frac{k_2}{\mu_2 \cdot \omega} \cdot E_m \cdot e^{-i \cdot \omega \cdot t}$$

$$a_n = \frac{H_n^1(\gamma_1)\left[\gamma_1 J_n(\gamma_1)\right]_{\gamma_1}^{\Uparrow} - J_n(\gamma_1)\left[\gamma_1 H_n^1(\gamma_1)\right]_{\gamma_1}^{\Uparrow}}{Y H_n^1(\gamma_1)\left[\gamma_2 J_n(\gamma_2)\right]_{\gamma_2}^{\Uparrow} - J_n(\gamma_2)\left[\gamma_1 H_n^1(\gamma_1)\right]_{\gamma_1}^{\Uparrow}}; \; b_n = \frac{H_n^1(\gamma_1)\left[\gamma_1 J_n(\gamma_1)\right]_{\gamma_1}^{\Uparrow} - J_n(\gamma_1)\left[\gamma_1 H_n^1(\gamma_1)\right]_{\gamma_1}^{\Uparrow}}{N H_n^1(\gamma_1)\left[\gamma_2 J_n(\gamma_2)\right]_{\gamma_2}^{\Uparrow} - G J_n(\gamma_2)\left[\gamma_1 H_n^1(\gamma_1)\right]_{\gamma_1}^{\Uparrow}}$$

где r,θ,φ – сферические координаты; $\boldsymbol{r_o},\boldsymbol{\theta_o},\boldsymbol{\varphi_o}$ – единичные орты; $P_m^1(\cos\theta)$ – полином Лежандра; $J_n(\rho_1)$ – сферическая функции Бесселя; $H_n^1(\rho_1)$ – сферическая функция Ханкеля первого рода; $\rho_1 = k_1 \cdot r$; $\rho_2 = k_2 \cdot r$; $\gamma_1 = k_1 \cdot R$; $\gamma_2 = k_2 \cdot R$; $[\gamma_1 \cdot J_n(\gamma_1)]_{\gamma}^{1}$ – первая производная от произведения γ_1 и $J_n(\gamma_1)$ по аргументу γ_1 .

Отраженная электромагнитная волна $E21_x$ создает внутри ферритовой сферы электромагнитную волну, которую можно представить выражением

$$\boldsymbol{H21^c} = H_m \sum_{n=-1}^{\infty} (-i)^n \frac{2 \cdot n + 1}{n \cdot (n+1)} \left[\boldsymbol{r_o} \left(i \cdot a_n N_1^E \right) + \boldsymbol{\theta_o} \left(-b_n M_2^E + i \cdot a_n N_2^E \right) + \varphi_{\boldsymbol{o}} \left(b_n M_3^E - i \cdot a_n N_3^E \right) \right], \tag{11}$$

Падающая электромагнитная волна $H12_y$ создает внутри ферритовой сферы электромагнитную волну, которую можно представить выражением

$$\boldsymbol{H12^c} = i \cdot H_m \sum_{n=-1}^{\infty} i^n \frac{2 \cdot n+1}{n \cdot (n+1)} \left[\boldsymbol{r_o} \left(i \cdot a_n N_1^H \right) + \boldsymbol{\theta_o} \left(b_n M_2^H - i \cdot a_n N_2^H \right) + \varphi_o \left(b_n M_3^H - i \cdot a_n N_3^H \right) \right], \quad (12)$$

$$M_2^H = -\frac{1}{\sin\theta} \cdot J_n(\rho_2) \cdot P_m^1(\cos\theta) \cdot \cos\varphi; \quad M_3^H = -\cdot J_n(\rho_2) \cdot \left[\frac{d}{d\theta} P_m^1(\cos\theta) \right] \cdot \sin\varphi;$$

$$N_1^H = \frac{n \cdot (n+1)}{\rho_2} \cdot J_n(\rho_2) \cdot P_m^1(\cos\theta) \cdot \cos\varphi \; ; \; N_2^H = \frac{1}{\rho_2} \cdot \left[\frac{d}{d(\rho_2)} \rho_2 \cdot J_n(\rho_2) \right] \cdot \left[\frac{d}{d\theta} P_m^1(\cos\theta) \right] \cdot \cos\varphi$$

$$N_3^H = \frac{1}{\rho_2 \cdot \sin\theta} \cdot \left[\frac{d}{d(\rho_2)} \cdot \rho_2 \cdot J_n(\rho_2) \right] \cdot P_m^1(\cos\theta) \cdot \sin\varphi \, .$$

Отраженная электромагнитная волна $H22_y$ создает внутри ферритовой сферы электромагнитную волну, которую можно представить следующим выражением:

$$\boldsymbol{H22^c} = i \cdot H_m \sum_{n=-1}^{\infty} \left(-i^n \right) \frac{2 \cdot n+1}{n \cdot (n+1)} \left[\boldsymbol{r_o} \left(i \cdot a_n N_1^H \right) + \boldsymbol{\theta_o} \left(b_n M_2^H + i \cdot a_n N_2^H \right) + \varphi_o \left(b_n M_3^H + i \cdot a_n N_3^H \right) \right], \quad (13)$$

Суммарное электромагнитное поле в середине ферритовой сферы можно представить уравнением:

$$H^c = H11^c + H21^c + H12^c + H22^c \, , \quad (14)$$

Выражения (9) – (13) удовлетворяют уравнениям Максвелла и граничным условиям на границе ферритовый шар – свободное пространство.

Исследование свойств напряженности переменного магнитного поля внутри ферритовой сферы

На рис. 2 приведены зависимости отношения модуля напряженности магнитного поля в центре ферритовой сферы H^c к напряженности падающей волны H_m в зависимости от величины ее радиуса.

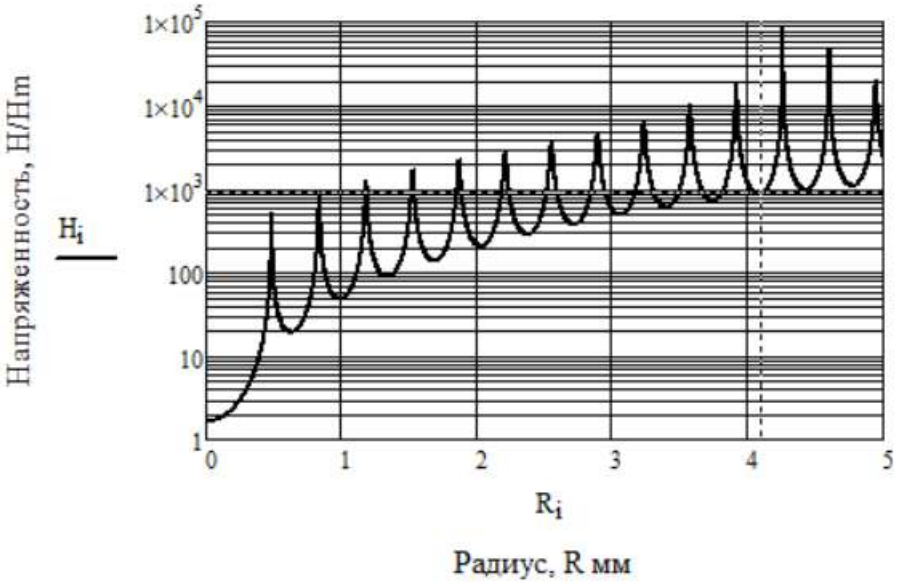


Рис. 2. Зависимость напряженности магнитного поля в середине шара от величины радиуса

Входные параметры: мощность падающей электромагнитной волны P равна 200 кВт, диаметр электромагнитного луча D равен 20 λ_o; λ_o = 3,2 см; Напряженность падающего на ферритовую сферу магнитного поля СВЧ H_m равна 28,7 А/м; феррит марки С-4256 [15]; $\varepsilon = 15{,}1\text{-}i\cdot 0{,}003$; $\mu = 143{,}5 - i\cdot 1{,}4$. Действительная часть магнитной проницаемости вычислена по методике, представленной в работе [4]. Мнимая часть вычислена методом решения уравнения движения вектора намагниченности в постоянном магнитном поле и поле СВЧ [11].

Кривая H_i построена на основании численного анализа уравнения (9) – (13). Параметры вычислений $L = \lambda_o/8$; $r = R\cdot 10^{-4}$; $\theta = 0{,}0001\cdot\pi$; $\varphi = \pi/2$. Из кривой, приведенной на рис. 2, видно, что при резонансных радиусах сферы $R1_p$, $R2_p$, … равных 0,4875 мм, 0,8406 мм, …, и так далее до $R12_p$, равного 4,2634 мм, напряженность магнитного поля в центре ферритовой сферы резко возрастает. Дальнейшее увеличение радиуса приводит к уменьшению напряженности магнитного поля.

В центре ферритовой сферы, резонансный радиус которой равен 4,2634 мм, можно достичь увеличения напряженности магнитного поля СВЧ в 83796 раз по сравнению с напряженностью магнитного поля в падающей волне. При нерезонансном радиусе равном 4,0637 мм напряженность магнитного поля СВЧ в центре ферритовой сферы будет равна $865\cdot H_m$. На рис. 2 эта точка выделена пересечением пунктирных линий.

На рис. 3 представлена зависимость отношения модуля напряженности магнитного поля H_i в середине ферритовой сферы к напряженности падающей плоской волны H_m от координаты r.

Рис. 3. Зависимость напряженности магнитного поля от сферической координаты r.

Кривые H1, H2, H3, соответствуют значениям сферических координат θ – 0, φ – π/2 и резонансным радиусам R1, R2, R3 равным соответственно 0,4875 мм, 0,8406 мм, 1,1847 мм. Кривые построены на основании численного анализа уравнения (9-13).

Ход кривых, приведенных на рис. 3, показывает, что внутри ферритовой сферы устанавливаются неоднородные электромагнитные волны.

На рис. 4 представлена зависимость отношения модуля напряженности магнитного поля H_i к напряженности падающей плоской волны H_m от координаты θ. Резонансный радиус сферы $R1_p$ равен 0,4268 мм. Точки наблюдения при сферической координате r равной $0{,}1\cdot R_p$. Кривые H1, H2, H3, H4 и H5 соответствуют координатным углам φ, равным соответственно 0^o, 30^o, 60^o, 90^o, 120^o. Кривые, представленные на рис. 4, построены на основании численного анализа уравнений (9 -13).

При увеличении сферической координаты θ от 0^o до 180^o (кривые 0^o, 30^o, 60^o, 120^o) отношение амплитуд H_i/H_m имеет максимум при (= 90). Кривые H2 и H5 совпадают.

Для координаты φ равной 90° при увеличении сферической координаты θ от 0°,до 180° отношение амплитуд H_i/H_m плавно изменяется от $5{,}6 \cdot H_m$ до $4{,}9 \cdot H_m$.

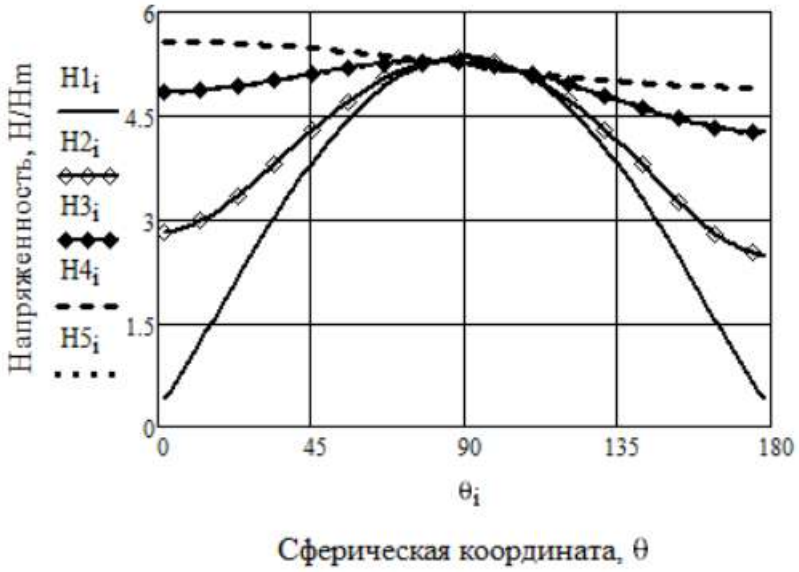


Рис.4. Зависимость напряженности магнитного поля от сферической координаты θ.

Ход кривых, приведенных на рис. 3 и 4, показывает, что внутри ферритовой сферы устанавливаются неоднородные электромагнитные волны.

Среднее квадратичное значение напряженности $H^c_{ск}$ переменного магнитного поля по объему ферритовой сферы изменяется с увеличением его резонансного радиуса. При резонансном радиусе $R1_{р,}$ равном 0,4875 мм, величина $H1^c_{ср}/H_m$ равна 1,5 и при $R12_{р,}$ равном 4,2634 мм, – $H7^c_{ср}/H_m$ равно 4,8. При нерезонансном радиусе $R_н$, равном 4,08 мм, – $H7^c_{ср}/H_m$ равно 0,54.

В таблице приведены величины коэффициента усиления амплитуды напряженности магнитного поля электромагнитной волны в середине ферритовой сферы ($\eta = H1^c_{ср}/H_m$) для всех рассматриваемых радиусов.

Исследование силового воздействия стоячей электромагнитной волны на ферритовую сферу

Средняя за период потенциальная энергия, которую получает ферритовая сфера в электромагнитном поле стоячей волны, может быть вычислена с помощью уравнения [2]:

$$U = -\frac{1}{T} \cdot \int_0^T \int_V \cdot \mathrm{Re}(J) \cdot \mathrm{Re}(B^C) dV dt, \qquad (15)$$

где $\mathrm{Re}(\boldsymbol{J})$, $\mathrm{Re}(\boldsymbol{B}^c)$ – действительные части векторов намагниченности $\boldsymbol{J}$ и магнитной индукции $\boldsymbol{B}^c$ в середине ферритовой сферы, V – объем ферритовой сферы, T – период колебаний электромагнитной волны.

В соответствии с уравнениями (14), (15) и физической моделью объекта исследования составляющую потенциальной энергии (которая превращается в кинетическую энергию поступательного движения ферритовой сферы) можно представить выражением

$$U = -\frac{1}{T} \int_0^T \int_0^R \int_0^{\pi} \int_0^{2\pi} \mathrm{Re}\left[(\mu - 1) H_x^c\right] \mathrm{Re}\left[\mu_o \mu \cdot H_x^c\right] d\varphi \cdot \sin\theta \cdot d\theta \cdot r^2 dr dt, \qquad (16)$$

где

$$\boldsymbol{H_x^c} = \sin\theta \cdot \cos\varphi \cdot H_r^c + \cos\theta \cdot \cos\varphi \cdot H_\theta + \sin\varphi \cdot H_\varphi^c, \quad (17)$$

Сила, с которой стоячая электромагнитная волна действует на ферримагнитный цилиндр, размещенный в постоянном магнитном поле, может быть вычислена с помощью уравнения

$$F = gradU. \quad (18)$$

При расстоянии от центра ферритовой сферы до металлического экрана, которое равно ($\lambda_o/8 + n\cdot\lambda_o/2$, где n = 0, 1, 2, 3…), наблюдается максимальная величина силы, направленная вдоль распространения падающей электромагнитной волны. При расстоянии – ($3\cdot\lambda_o/8+n\cdot\lambda_o/2$) направление силы противоположно направлению распространения падающей электромагнитной волны.

Результаты анализа аналитических уравнений (16) и (18) приведены в таблице.

R_p	Резонансный радиус, мм	Коэффициент усиления, η	Сила, действующая на уединенный шар, Н
R_1	0,4875	1,5	$1{,}8\cdot10^{-5}$
R_4	1,595	1,6	$6{,}3\cdot10^{-4}$
R_8	2,895	2,3	$9{,}2\cdot10^{-3}$
R_{11}	3,9616	4,7	$9{,}3\cdot10^{-2}$
R_{12}	4,2634	4,8	0,12
	Не резонансный		
$R_н$	4,08	0,54	$1{,}3\cdot10^{-3}$

Сила, действующая на ферритовую сферу, увеличивается с увеличением резонансного радиуса. Это обусловлено зависимостью величины сил от объема шара и от коэффициента усиления напряженности магнитного поля СВЧ внутри шара.

Для ферритовой сферы радиус, которой равен 4,2634 мм отношение полученной силы к плотности потока мощности СВЧ и к объему шара равно $3{,}6\cdot10^5$ Н/(Вт·м). Это же отношение, полученное в работе [5], для ферримагнитного цилиндра равно 4,3 Н/(Вт·м). Следовательно, преобразование электромагнитной энергии в механическую энергию ЖИГ-резонатором эффективнее в $8{,}6\cdot10^4$ раз по сравнению с преобразованием ферримагнитным цилиндром.

Обсуждение результатов исследований

Заменив в уравнениях (16) – (18) μ-1 и μ на Re(μ-1) и Re(μ), получим численную величину для силы, действующей на ферритовый шар $R_{12,}$ равную 0,1199. Приближенное значение силы меньше на 0,08 % от силы, вычисленной при помощи (16) – (18). Из уравнений (12) – (14) и (20) следует, что $H^c_{ск}$ пропорционально напряженности магнитного поля падающей электромагнитной волны $\eta\cdot H_m$.

С учетом сказанного выше приближенно (с погрешностью 0,08 %) сила может быть вычислена с помощью уравнений:

$$F = \mu_o \cdot \big(\mathrm{Re}(\mu-1)\big)\cdot \mathrm{Re}(\mu)\cdot grad(H_{ск}^c)^2 \cdot V, \quad (19)$$

$$(H_{ск}^c)^2 = \frac{1}{V\cdot T}\int_0^T \int_0^R \int_0^{\pi} \int_0^{2\pi} \left[\mathrm{Re}(H_x^c)\right]^2 \cdot d\varphi \cdot \sin\theta \cdot d\theta \cdot r^2 dr \cdot dt, \quad (20)$$

$$H_{ск}^c = \eta \cdot H_m, \quad (21)$$

где H_m – модуль вектора напряженности переменного магнитного поля, вращающегося вокруг оси z и подающего на ЖИГ-резонатор.

В работе [3] используются следующие параметры: P1=10 Вт, S1=2,3·10^{-4} м^2 (2,3·1 см^2), V1=2,34·10^{-8} м^3 (диаметр шара R равен 3,55 мм), μ = 143,5, F1= (6 ± 0,5)·10^{-6} Н; η1 = 0,69; $H1^{c}_{ск}$ = 12,7 cos(π·z/a) А/м, размер широкой стенки волновода a = 2,3 см, координата размещения центра шара z = a/4.

В соответствии с (19) силу, действующую на ферритовую сферу, помещенную в прямоугольном волноводе,можно представить выражением

$$F1 = -\mu_o \cdot \mu^2 \cdot \eta 1^2 \cdot V1 \cdot \frac{d}{dz}\left(12{,}7 \cdot \cos(\pi \cdot z / a)\right)^2 = 6{,}3 \cdot 10^{-6} \cdot\cdot H \,. \qquad (22)$$

Совпадение результата вычисления силы по упрощенному выражению с величиной силы, измеренной экспериментально в пределах погрешности измерения, подтверждает справедливость разработанного алгоритма для исследования силового действия неоднородной электромагнитной волны на ферритовую сферу, находящейся в состоянии ферримагнитного резонанса.

В настоящей работе используются параметры: P2=200 кВт; S2=0,32 м^2 (диаметр поперечного сечения луча, в котором распространяется падающая электромагнитная волна, равен 0,64 м); V2=3,2·10^{-7} м^3 (радиус ферритовой сферы R12 равен 4,2634 мм); μ = 143,5; F12 = 0,12 Н; η_7 = 4,8; $H2^{c}_{ск}$ = 2 H_m·cos(2·π·z/λ_o) А/м; координата размещения центра сферы z = λ_o/8;

$$F2 = -\mu_o \cdot \mu^2 \cdot \eta 2 \cdot V2 \cdot \frac{d}{dz}\left(40{,}6 \cdot \cos(2 \cdot \pi \cdot z / \lambda_o)\right)^2 = 0{,}12 \cdot H \,. \qquad (23)$$

Совпадение результатов исследований, полученных при помощи упрощенной методики, и результатов исследования, полученных на основании строгих математических расчетов, свидетельствует, что при анализе уравнений (10) – (16) отсутствуют ошибки.

Оценим величину силы, с которой стоячая электромагнитная волна может действовать на систему ферритовых сфер.

Выше было показано, что при расстоянии от центра ферритовой сферы до металлического экрана, которое равно (λ_o/8 + n·λ_o/2, где n = 0, 1, 2, 3…), наблюдается максимальная величина силы. В объеме луча, в котором распространяется падающая электромагнитная волна (длина объема равна λ_o/8 + 100·λ_o/2= 1,604 м; диаметр равен 0,64 м), можно разместить 1,257·10^5 ферритовых сфер на расстоянии, равном λ_o/2 одна от другой. На эти ферритовые сферы будет действовать стоячая электромагнитная волна с примерно одинаковою силою.

Без учета явления дифракции плоской электромагнитной волны на системе из ферритовых сфер и потерь на их нагревание можно оценить силу, с которой стоячая электромагнитная волна действует на систему сфер. Оценочная величина силы, действующей на 1,257·10^5 ферритовых сфер, составляет 1,5·10^4 Н (сила тяги равна 1,7·10^3 кг; мощность падающей электромагнитной волны равна 200 кВт). Справедливость оценочной величины силы тяги предложенного преобразователя может быть проверена после решения ряда задач:

1. Дифракция плоской электромагнитной волны на системе ферритовых сфер произвольного диаметра (до настоящего времени эта задача не решена).

2. Вычисление потерь в системе ферритовых сфер.

3. Разработка предложенного преобразователя и проведение экспериментальных исследований.

Выводы

Применение ЖИГ-резонатора, ферримагнитного и пространственного резонансов позволило разработать преобразователь электромагнитной энергии в механическую энергию, с силою тяги, равной 0,12 Н. Полученные результаты исследований могут быть использованы разработчиками преобразователей СВЧ энергии в механическую энергию. Дальнейшее усовершенствование метода преобразования электромагнитной энергии СВЧ в механиче-

скую энергию, по-видимому, заключается: в проведении экспериментальных исследований, решении задачи дифракции плоской электромагнитной волны на системе ферритовых сфер произвольного диаметра, исследовании потерь в системе ферритовых сфер.

Список литературы:

1. Пондеромоторное действие электромагнитного поля (теория и приложения) / Р. А. Валитов, Н. А. Хижняк, В. С. Жилков [и др.] ; под ред. Р. А. Валитова. Москва : Сов. радио, 1975. 232 с.
2. Мартыненко Л. Г. Влияние ферримагнитного резонанса на преобразование электромагнитной энергии в механическую. Л. Г. Мартыненко, Г. Л. Комарова, В. В. Маличенко // Известия вузов, радиоэлектроника. 2016. Т. 59. №. 10, С 30-36. DOI: 10.3103/S0735272716100046.
3. Measurement of Impulsive Thrust from a Closed Radio-Frequency Cavity in Vacuum / H. White, P March, J. Lawrence et al. // Journal of propulsion and power. Vol. 33, No. 4, July–August 2017 P. 830 – 841. DOI: 10.2514/1.B36120.
4. Мартыненко Л. Г. Влияние ферримагнитного резонанса на преобразование энергии электромагнитной стоячей волны в механическую энергию / Л. Г. Мартыненко, Г. Л. Комарова // Известия вузов, радиоэлектроника. 2020. Т. 63. №. 5. С 290-298. DOI: 10.3103/S0735272720050039
5. Мартиненко Л. Г. Спосіб перетворення електромагнітної енергії в механічну / Л.Г. Мартиненко, Г.Л. Комарова, В.В. Маличенко. Патент на винахід України. № 117748. Бюл. № 18 від 25.09.2018.
6. Мартиненко Л.Г. Спосіб перетворення електромагнітної енергії в механічну / Л.Г. Мартиненко, Г.Л. Комарова, В.В. Маліченко. Патент на корисну модель № 1129907. від 10.01.2017. Бюл. № 1.
7. Макеева Г. С. Электродинамический анализ постоянных распространения электромагнитных волн в 3D-решетках магнитных нанопроволок в условиях магнитного резонанса в микроволновом диапазоне / Г. С. Макеева, О. А. Голованов // Радиотехника и электроника. 2016. Т. 61. №. 1. С. 3 - 11. DOI:10.7868/S0033849415110145
8. Kozar A. I. Resonant degenerate crvstal made of spheres located magnetodielectric medium // International Journal of Electromagnetics and Applications, Vol. 3, No. 2, 2013, pp. 15-19. DOI: 10.5923/j.idea.20130302.02.
9. Козар А.И. Резонансные метакристаллы из малых магнитодиэлектрических сфер : монография. Харьков : ХНУРЭ, 2014. 352 с.
10. Никольский В.В. Теория электромагнитного поля. Москва : Высш. шк. 1961. 371с.
11. Гуревич А.Г. Ферриты на сверхвысоких частотах / А.Г. Гуревич. Москва : Физматгиз, 1960. 208 с.
12. Електродинаміка та поширення радіохвиль. Ч. 1. Основи теорії електромагнітного поля / В. М. Шокало, В. І. Правда, Усін [та ін.] ; за заг. ред. В. М. Шокало та В. І. Правда. Харків : Колегіум, 2009. 208 с.
13. Стреттон Дж. А. Теория электромагнетизма. Москва : Гостехиздат. 1948. 539 с.
14. Микроволновые ферриты. [Электронный ресурс] Режим доступа: https://www.domen.ru/mikrovolnovye-ferrity 07.01.2018.

Поступила в редколлегию 17.10.2021

Сведения об авторах:

Комарова Анна Леонидовна – канд. техн. наук, доцент, Украинский государственный университет железнодорожного транспорта, доцент кафедры инженерии вагонов и качества продукции, Украина; e-mail: anna.kom3793@gmail.com.ua; ORCID: https://orcid.org/0000-0001-8597-5891

ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНІ ТЕХНОЛОГІЇ
ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНЫЕ ТЕХНОЛОГИИ
INFORMATION AND MEASURING TECHNOLOGIES

УДК 004.45:004.057.02 **DOI:10.30837/rt.2021.4.207.17**

N. SHTEFAN, Cand. Sc. (Technology), O. ZAPOROZHETS, Cand. Sc. (Technology)

SOFTWARE QUALITY MODEL ON THE BASE OF SQUARE STANDARDS

Introduction

Given the rapid introduction of computer systems into almost all aspects of human life, the issue of assessing the software quality of is becoming increasingly important. While talking about a unified approach that can be achieved with the help of international standards [1].

Standardization ensures the unification of requirements for quality, its measurement and assessment. The use of standards provides many potential benefits for any organization, especially in such key areas as measuring the quality of software products and information and measurement systems. Accordingly, it is advisable to analyze modern standards as a basis for the formation of requirements for the software quality and measuring the quality of software, which will reduce risks in the development, implementation and maintenance of software. The relevance of this issue is also supported by the fact that the standards are adopted in Ukraine as national.

The first international standards in this area were adopted back in 1991, and have been revised several times since then. Today there is a set of standards ISO 25000 SQuaRE – Systems and software Quality Requirements and Evaluation – logically organized and unified series covering two main processes: software quality requirements specification and software quality evaluation supported by a quality measurement process [2].

SQuaRE Quality Model

SQuaRE standards include five core divisions [1]: quality requirement 2503n, quality model 2501n, quality measurement 2502n, quality evaluation 2504n and quality management 2500n, and also extension division 25050–25099.

The ISO 25000 SQuaRE standards are coordinated with ISO/IEC/IEEE 15939 [3] by content which define the general process and basis for systems and software measurement, as well as the relevant terminology from an engineer's point of view. Following modern ISO trends in terminology harmonization, ISO/IEC/IEEE 15939 adopts and adapts the metrological terminology established by VIM [4] for program and system engineering standards. The following concepts from ISO/IEC/IEEE 15939 fully compliant, adapted or based on definitions from VIM: base measure – based on the definition of the «base value»; derived measure – adapted from the definition of «derived value»; measurement – adapted; measurement method – based on the definition of the «measurement method»; measurement procedure – fully compliant; scale – based on the definition of the «scale»; unit of measurement – fully compliant.

SQuaRE standards define a software and systems quality models used to determine requirements, develop measures and measure quality. Quality model is the set of classes of characteristics. Characteristics can be divided into subcharacteristics and, in some cases, into subsubcharacteristics. Quality-related measurable properties are called quality properties. Quality properties are associated with the appropriate quality measures.

The quality in SQuaRE standards is described by four models: quality in use model and product quality model defined ISO/IEC 25010, as well as the data quality model defined ISO/IEC 25012 and IT-services quality model defined ISO/IEC 25011.

The product quality model reduces quality features to eight characteristics, each of them consists of a number of subcharacteristics (fig. 1) [5].

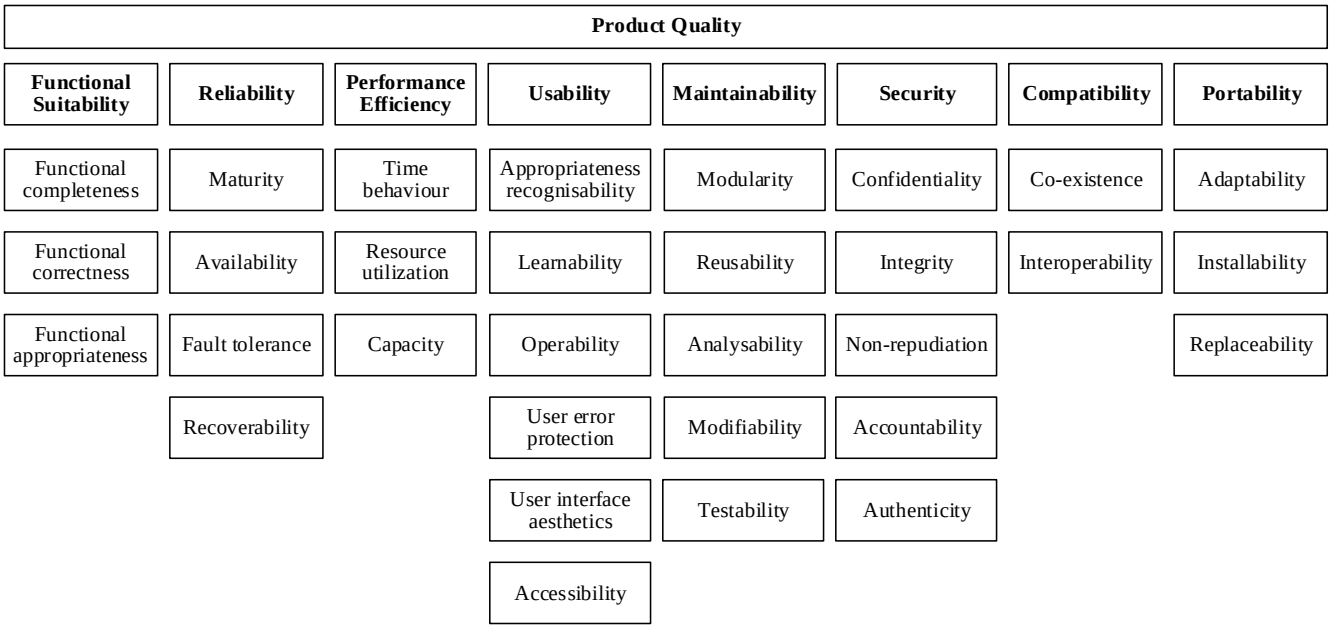


Fig. 1. The product quality model

This product quality model is complemented by a quality in use model that characterizes the impact of the product (system or software product) on the stakeholders. Quality in use is determined by the quality of the software, hardware, operating environment, as well as the characteristics of users, tasks and social environment. The quality in use model determines through five characteristics associated with the results of interaction with the system (fig. 2) [5].

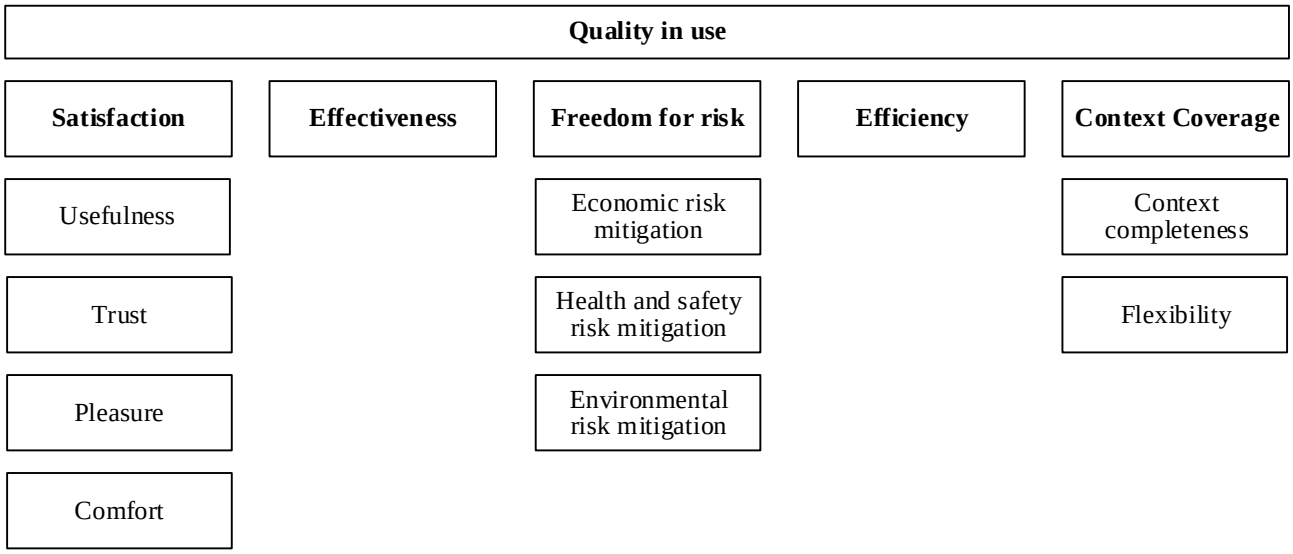


Fig. 2. The quality in use model

Models of product quality and quality in use can be used to define requirements, generate measures, and quality evaluations. The defined quality characteristics can be used as a checklist to provide a detailed study of the quality requirements, thus providing a basis for evaluating the subsequent effort and actions required in the system development process.

SQuaRE Quality Measurement Division

The Quality Measurement Division (2502n) includes six standards:

– ISO/IEC 25020 – Quality measurement framework: provides a framework for developing quality measurement;

– ISO/IEC C 25021 – Quality measure elements: provides a format for specifying QMEs (Quality Measure Elements) and a few examples of QMEs that can be used to construct software quality measures;

– ISO/IEC 25022 – Measurement of quality in use: provides measures, including associated measurement functions for the quality characteristics in the quality in use model;

– ISO/IEC 25023 – Measurement of system and software product quality: provides measures, including associated measurement functions and QMEs for the quality characteristics in the product quality model;

– ISO/IEC 25024 – Measurement of data quality: provides measures, including associated measurement functions and QMEs for the quality characteristics in the data quality model;

– ISO/IEC TS 25025 – Measurement of IT service quality: provides measures for the IT service quality model.

Figure 3 shows the Structure of SQuaRE Quality Measurement Division.

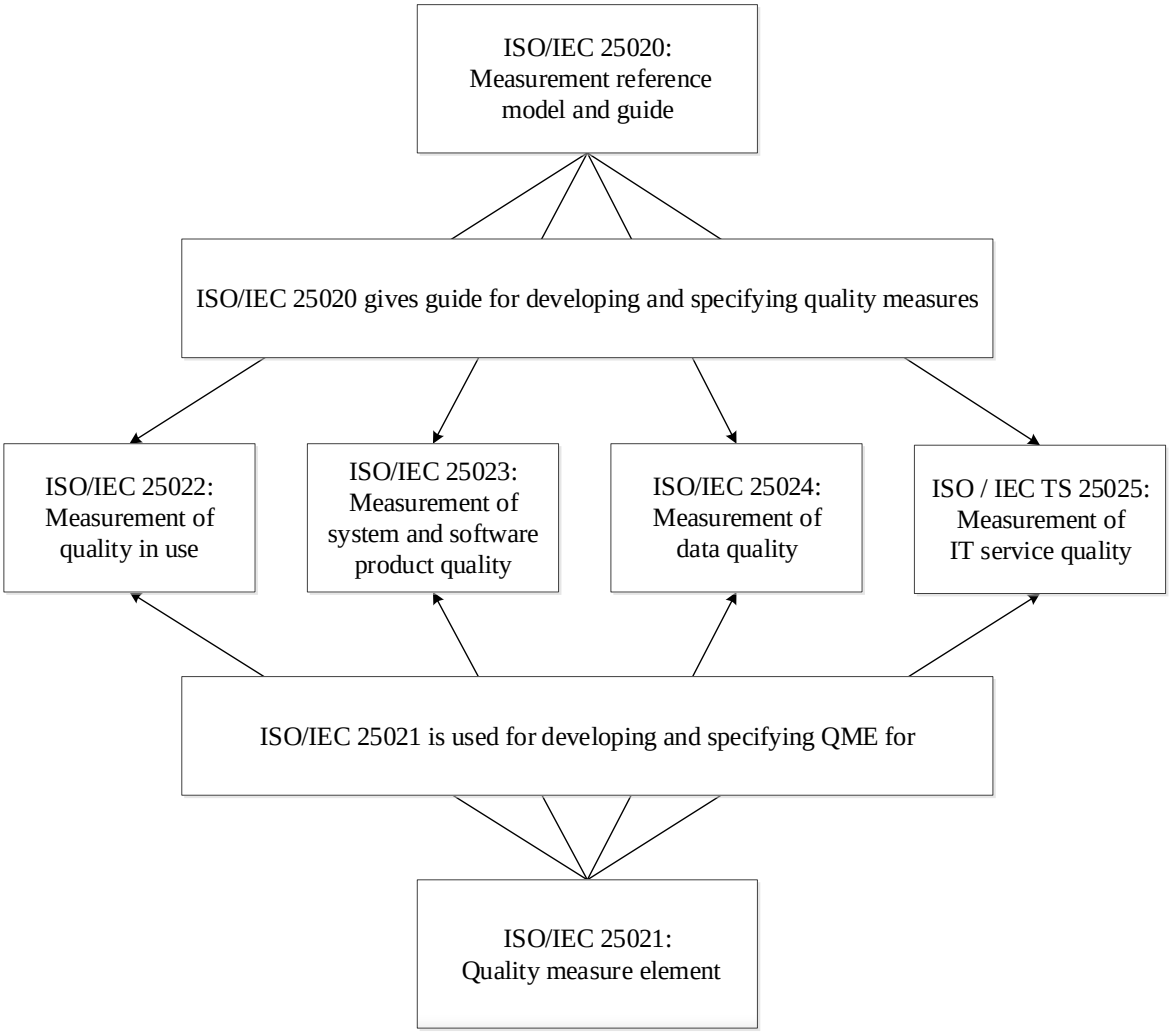


Fig. 3. Structure of SQuaRE Quality Measurement Division

Quality measure element as the basis of quality measurement

ISO/IEC 25020 provides framework for developing quality measures [6]. Measurement of software quality is based on two concepts: quality measure and quality measure element.

Quality measure element (QME) is an indicator defined in terms of a feature and a measurement method to quantify that feature, including a selective transformation using a mathematical function.

The main purposes of defining and using of QME:

1) provide guidance for organizations that develop and implement their own QME;

2) to promote the consistent application of a given QME for measuring and using product features that relate to different characteristics and sub-characteristics of product quality;

3) to help identify a set of QME's that are uniquely in demand, to obtain all the quality indicators of this set of characteristics or sub-characteristics of the product.

The quality measures and, accordingly, the QME are determined to understand and indicate the characteristics and sub-characteristics of quality. The measurement function is applied to the EPC to generate the quality measures. The measurement method must be applied to the property to establish and identify a method for quantifying QME.

The user of the measurement method must identify and collect data related to the quantification of the property (fig. 4). Depending on the context of use and the purposes of EPC, a number of properties and subproperties can be identified. They are the input data for the measurement method. These properties are defined and retrieved from artifacts, components, content, or behavior of the target object (eg, documentation, code).

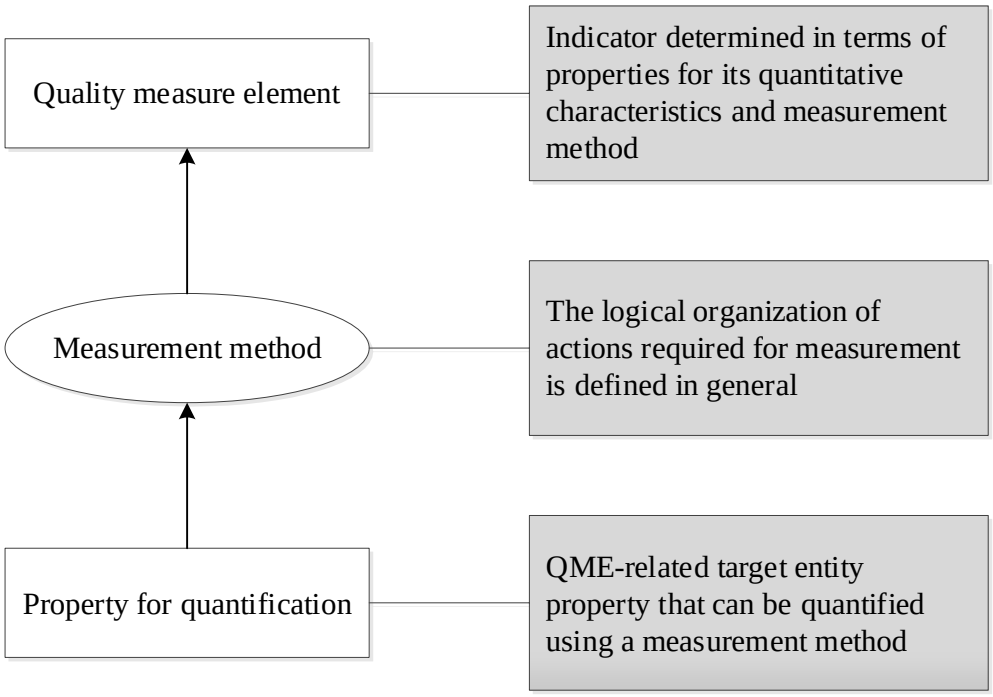


Fig. 4. Relationship between quantification property, measurement method and QME

So, the ISO / IEC 25000 defines 36 quality characteristics and over 200 quality measures and expected further multiplication of characteristics.

Practical Usage of SQuaRE Quality Measurement Model

The Quality Measurement Reference Model describes the relationship between a quality model and the construction of quality measures from quality measure elements (fig. 5).

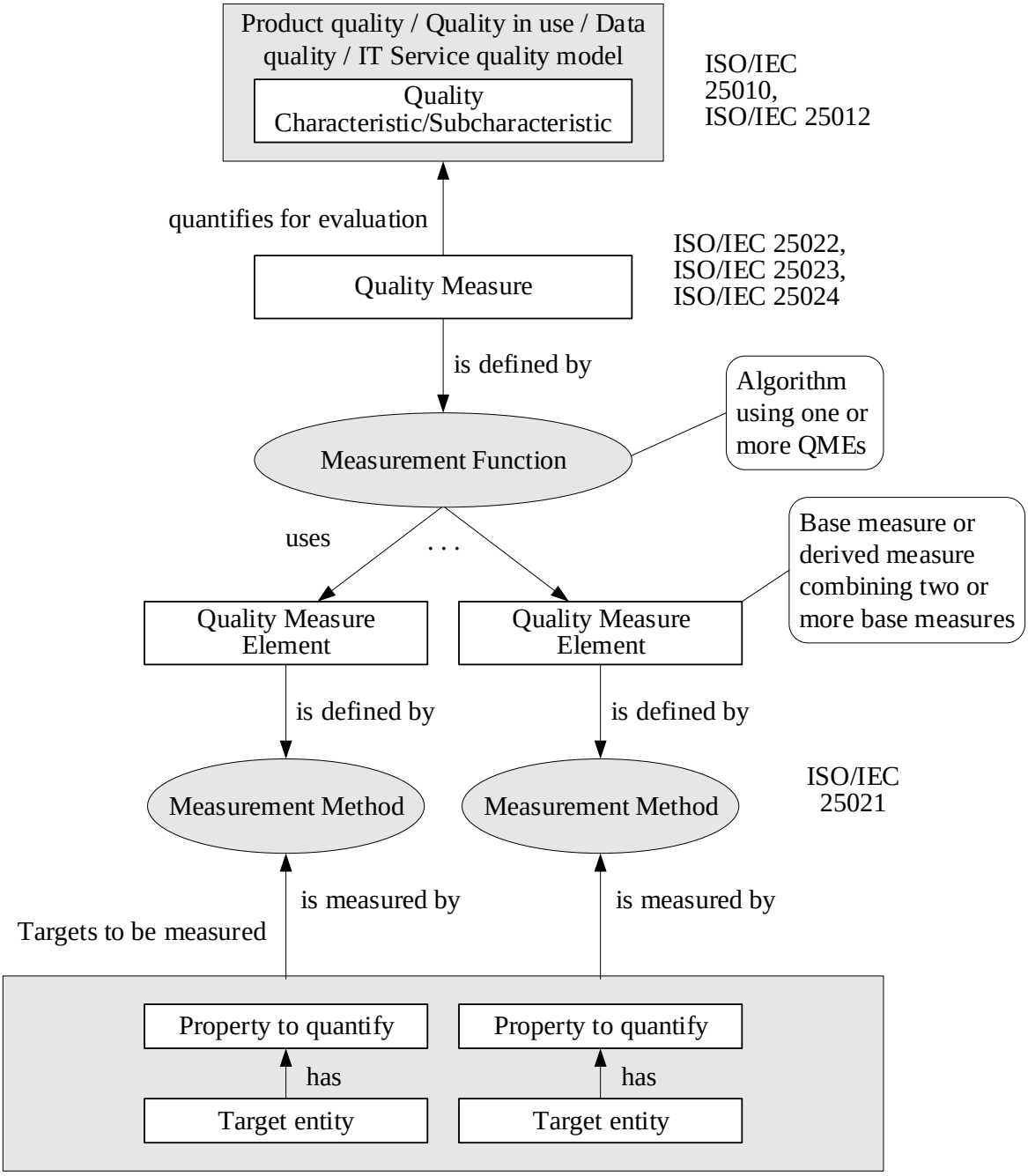


Fig. 5. Relationship among quality model, quality measures, quality measure elements, property to quantify, target entity

Quality properties are measured by means of a measurement method. A measurement method is a logical sequence of operations used to quantify properties relative to a specific scale. The result of applying the measurement method is quality measure elements. Quality characteristics and subcharacteristics can be quantified using the measurement function. A measure function is an algorithm used to combine the quality measure elements. Quality measures are constructed by applying a measurement function to a set of quality measure elements. The result of using the measurement function is called the software quality measure. Thus, software quality measures become quantitative indicators of quality characteristics and subcharacteristics. Several software quality measures can be used to measure a characteristic or subcharacteristic of quality.

ISO/IEC 25022 [7], ISO/IEC 25023 [8], ISO/IEC 25024 [9] provides a set of quality measures for the characteristics of system/software products for the quality in use and product quality models defined by ISO/IEC 25010, and data quality model defined by ISO/IEC 25012. This quality

measures can be used for specifying requirements, measuring and evaluating the system/software product quality. Based on the measurement task, quality measures are selected from standards ISO/IEC 25022, ISO/IEC 25023, ISO/IEC 25024 to satisfy the needs of developers, acquirers, managers, direct and indirect users and other stakeholders. Moreover, include measurement functions for each proposed quality measures, summary consideration for usage of quality measures and quality measure elements. Quality measure elements are presented by ISO/IEC 25021 [10].

Based on the analysis of SQuaRE Quality Model and Quality Measurement Divisions, an algorithm of Measurement of Software Quality is proposed:

1) define quality models by ISO/IEC 25010, ISO/IEC 25012 for identification of relevant software quality characteristics;

2) select quality measures for each quality characteristic using ISO/IEC 25022, ISO/IEC 25023, ISO/IEC 25024;

3) measure the quality measure elements using the measurement methods from ISO/IEC 25021;

4) selected quality measures are constructed by applying a measurement function to quality measure elements.

The table shows examples of the application of SQuaRE standards for measurement of software quality.

Table

Examples of the application of SQuaRE standards for measurement of software quality

Quality characteristic/ subcharacteristic	Quality measure. Description	Measurement function	Quality measure element	Measurement method
Functional completeness	Functional coverage. What proportion of the specified functions has been implemented?	$X = 1 - A / B,$ A – number of functions missing, B – number of functions specified	Number of available functions	View and analyze individual system/software functions that are available to a user with a disability to call and execute, and count the number of functions that could not be successfully used
Time behavior	Mean response time. How long is the mean time taken by the system to respond to a user task or system task?	$X = \sum_{i=1}^{n} A_i \Big/ n,$ A_i – time taken by the system to respond to a specific user task or system task at *i*-th measurement, n – number of responses measured	Duration	Duration is based on the total amount of time and is linked to the International System of Units (VIM)
Learnability	User guidance completeness What proportion of features are described in sufficient detail in the user documentation and/or help center to allow the user to apply the features?	$X = A / B,$ A – number of functions described in the user documentation and/or help center, if required, B – number of implemented functions that need to be documented	Number of documented functions	View and analyze individual system/software features that are available to a user with disabilities to call and execute, and count the number of features that are described in the user documentation

Conclusions

1. The SQuaRE 2501n Quality Models division describes software quality models that support clear definition of software quality requirements. The characteristics in the quality-in-use model and the product quality model are intended to be used as a set in the specification or assessment of the quality of a software product or computer system.

2. Measuring of software quality is based on two concepts: a quality measure and a quality measure element. A reference model for quality measurement is described in the ISO/IEC 25020 standard.

3. The ISO/IEC 25022, ISO/IEC 25023, ISO/IEC 25024 define the quality measures and the measurement function for each quality characteristic of the model.

4. The measurement function associates quality measures with quality measure elements of that is directly measured. A fairly wide list of elements of quality measures elements contains the ISO/IEC 25021.

5. The main advantages of a series of standards SQuaRE is that they provide coordination methodologies for measuring and evaluating quality software products, a guide to specifications of software quality requirements product and harmonization with the standard ISO/IEC 15939 in the form of a reference model of measurements quality.

References:

1. DSTU ISO/IEC 25000:2016 Systems and software engineering. Systems and software Quality Requirements and Evaluation (SQuaRE). Guide to SQuaRE (ISO/IEC 25000:2014, IDT). Kyiv, 2016 (in Ukrainian).
2. Kazuhiro Esaki. Introduction of Quality Requirement and Evaluation Based on ISO/IEC SQuaRE Series of Standard. // Global Perspectives on Engineering Management. May 2013, Vol. 2 Iss. 2, pp. 52-59.
3. DSTU ISO/IEC/IEEE 15939:2018 Systems and software engineering. Measurement process (ISO/IEC/IEEE 15939:2017, IDT). Kyiv, 2018 (in Ukrainian).
4. JCGM 200:2012. International vocabulary of metrology – Basic and general concepts and associated terms (VIM)
5. DSTU ISO/IEC 25010:2016 Systems and software engineering. Systems and software Quality Requirements and Evaluation (SQuaRE). System and software quality models (ISO/IEC 25010:2011, IDT). Kyiv, 2016 (in Ukrainian).
6. DSTU ISO/IEC 25020:2016 Systems and software engineering. Systems and software Quality Requirements and Evaluation (SQuaRE). Quality measurement framework (ISO/IEC 25020:2007, IDT). Kyiv, 2016 (in Ukrainian).
7. DSTU ISO/IEC 25022:2019 Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) (SQuaRE). Measurement of quality in use. (ISO/IEC 25022:2016, IDT). Kyiv, 2019 (in Ukrainian).
8. DSTU ISO/IEC 25023:2019 Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – (SQuaRE). Measurement of system and software product quality (ISO/IEC 25023:2016, IDT). Kyiv, 2019 (in Ukrainian).
9. ISO/IEC 25024:2015 Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – Measurement of data quality.
10. DSTU ISO/IEC 25021:2016 ДСТУ ISO/IEC 25021:2016 Інженерія систем і програмних засобів. Вимоги до якості систем і програмних засобів та її оцінювання (SQuaRE). Елементи показника якості (ISO/IEC 25021:2012, IDT).

Received 15.11.2021

Information about authors:

Natalya Shtefan – PhD, Associate Professor, Kharkiv National University of Radio Electronics, Department of Information and Measuring Technologies, Ukraine; e-mail: natalya.shtefan@nure.ua; ORCID: https://orcid.org/0000-0001-7926-8437

Oleg Zaporozhets – PhD, Associate Professor, Kharkiv National University of Radio Electronics, Department of Information and Measuring Technologies, Ukraine; e-mail: oleg.zaporozhets@nure.ua; ORCID: https://orcid.org/0000-0002-7831-8479

УДК 537.226.3 **DOI:10.30837/rt.2021.4.207.18**

Б.В. ЖУКОВ, канд. техн. наук, С.И. БОРБУЛЕВ, А.В. ОДНОВОЛ

ОПЕРАТИВНЫЙ КОНТРОЛЬ ПАРАМЕТРОВ ЖИДКИХ ГОРЮЧЕСМАЗОЧНЫХ МАТЕРИАЛОВ С ПРИМЕСЯМИ

Введение

Надежность работы современных двигателей внутреннего сгорания существенно зависит от качества горючесмазочных материалов (ГСМ). Поэтому развитию методов контроля качества ГСМ, в том числе экспресс-методов, основанных на измерении их диэлектрической проницаемости, в настоящее время уделяется большое внимание [1 – 6].

Возрастающие требования к топливам и моторным маслам приводят к необходимости введения дополнительных присадок, что усложняет химический состав и процесс контроля их качества [7 – 12].

Резонаторный метод СВЧ диэлектрометрии [13] обеспечивает высокое разрешение действительной ε' и мнимой ε'' составляющих комплексной диэлектрической проницаемости, необходимое для анализа жидких горючесмазочных материалов (ГСМ). Данный метод может быть реализован в виде экспресс-анализатора октановых чисел неэтилированных бензинов [14] или экспресс-анализатора качества образцов жидких горюче-смазочных материалов по положению соответствующих этим образцам точек на комплексной плоскости [15].

В первом варианте экспресс-анализатор должен быть прокалиброван под конкретную технологию производства бензинов [14]. Во втором варианте экспресс-анализатор универсален, то есть не зависит от вида технологии производства ГСМ, однако для получения количественной оценки требует разработки модельного перехода от положения точки на комплексной плоскости к интересующему параметру образца ГСМ.

Предварительные исследования образцов жидких ГСМ (бензины дизельные топлива, керосины, масла) показали, что величины ε'и ε'' перечисленных ГСМ находятся в рабочем диапазоне резонаторного СВЧ диэлектрометра. При этом на комплексной плоскости точки, соответствующие рассмотренным ГСМ, располагаются отдельными непересекающимися группами [15].

Высокая разрешающая способность СВЧ резонаторного метода определяет перспективность использования данного метода для анализа комплексной диэлектрической проницаемости смесей ГСМ с различными примесями, включая воду, спирты [16], бензол и др.

Основная часть

Смесь бензина с бензолом.

Одной из наиболее вредных примесей в составе бензинов является бензол, октановое число которого по моторному методу составляет 100 о.е. (октановых единиц). Наличие бензола вредно как для самого двигателя, так и для окружающей среды. Допустимое содержание бензола в составе бензина в настоящее время строго ограничивается, поэтому представляет интерес возможность оперативного выявления примеси бензола.

На рис. 1 на комплексной плоскости представлены результаты исследования комплексной диэлектрической проницаемости смеси «бензин + бензол».

По оси абсцисс отложена разность $\Delta f(\varepsilon') = f_0(\varepsilon') - f_{см}(\varepsilon')$ резонансных частот резонатора, нагруженного пустой кюветой $f_0(\varepsilon')$, и резонатора, нагруженного исследуемой сме-

сью бензина с бензолом $f_{см}(\varepsilon')$. По оси ординат отложены величины тока, прошедшего через резонатор, нагруженный исследуемой смесью бензина с бензолом $I(\varepsilon'')$. При этом величина тока при установленной пустой кювете во всех опытах устанавливалась равной 200 мкА.

Точка 1 на рис. 1 соответствует бензину, точка 2 – смеси 5 % бензола с бензином, точка 3 – смеси 10 % бензола с бензином, точка 4 – смеси 15 % бензола с бензином и точка 5 – бензолу.

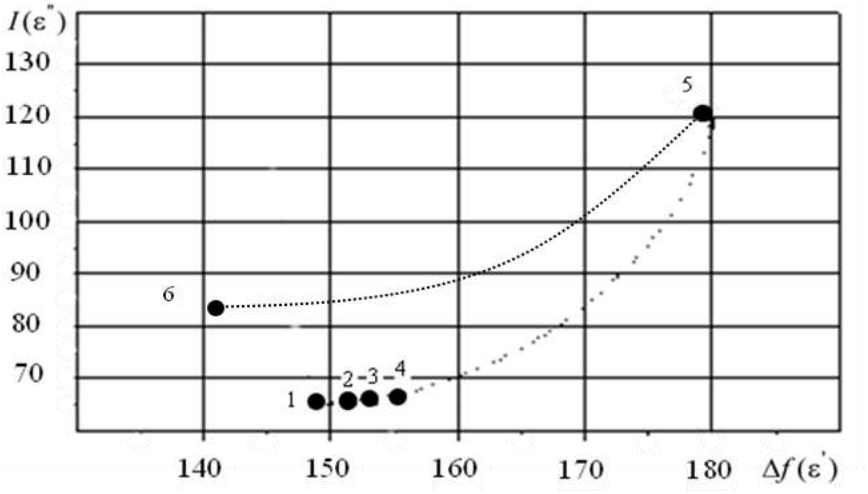


Рис. 1. Результаты исследований смеси «бензин + бензол»

Данные на рис. 1 показывают, что при малой процентной добавке бензола наблюдается существенное возрастание действительной части $\Delta f(\varepsilon')$ диэлектрической проницаемости смеси, а величина мнимой составляющей $I(\varepsilon'')$ смеси остаётся практически неизменной. При увеличении процентного содержания бензола от 15 % и выше наблюдается как увеличение действительной $\Delta f(\varepsilon')$, так и мнимой $I(\varepsilon'')$ составляющих диэлектрической проницаемости смеси.

Очевидно, что для смеси с бензолом (точка 5) другого исходного образца бензина, соответствующего, например, точке 6 на рис. 1, произойдет изменение расположения линии смеси 6 – 5, на комплексной плоскости (рис. 1). Для определения местоположения аппроксимирующей кривой 6 – 5 потребуется проведение исследований для образцов смесей нового бензина с бензолом.

Смесь трансформаторного масла с водой.

Основным требованием к трансформаторному маслу, обеспечивающим безопасность эксплуатации высоковольтных трансформаторов является минимизация в нем количества воды. Так, для заливки трансформаторов разрешается масло, в котором не более 14 граммов воды на тонну масла. Из-за особенностей технологического процесса заливки масла возможно попадание воды в заливаемое масло, что определяет необходимость текущего контроля количества воды в процессе его заливки в высоковольтные трансформаторы.

Однако в настоящее время отсутствует техническая возможность текущего, то есть в реальном времени, определения количества воды на уровне 10 грамм в тонне масла (разрешение на уровне до 10^{-5}). Поэтому для контроля количества воды применяют стандартизованный метод, суть которого заключается в измерении напряжения электрического пробоя масла, размещенного в мерной емкости.

Очевидно, что этот метод не может быть реализован в процессе заливки, поэтому контроль количества воды в масле осуществляется перед началом и после окончания процесса заливки. Таким образом, соответствие требованию не более 14 грамм воды на тонну масла

залитого в трансформатор может быть установлено только после окончания процесса его заливки.

На рис. 2 представлены результаты измерений комплексной диэлектрической проницаемости трех образцов трансформаторного масла: 1 – 14 грамм воды на тонну масла; 2 – 26 грамм воды на тонну масла и 3 – 56 грамм воды на тонну масла.

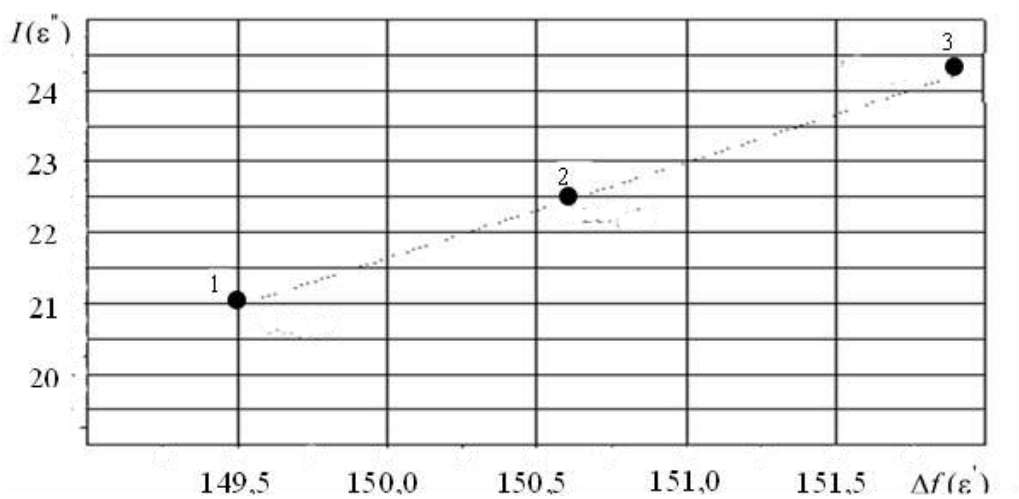


Рис. 2. Смесь трансформаторного масла с водой

По оси абсцисс также отложена разность $\Delta f(\varepsilon')$ резонансных частот резонатора, нагруженного пустой кюветой $f_0(\varepsilon')$, и резонатора, нагруженного исследуемой смесью трансформаторного масла с водой $f_{см}(\varepsilon')$. По оси ординат отложены величины тока $I(\varepsilon'')$, прошедшего через резонатор, нагруженный исследуемой смесью трансформаторного масла с водой.

Данные на рис. 2 свидетельствуют, что СВЧ диэлектрометр позволил раздельно определить на комплексной плоскости представленные образцы смесей масла с водой, поэтому метод СВЧ диэлектрометрии может считаться перспективным для контроля качества трансформаторного масла как в процессе заливки, так и для контроля соответствия масла в процессе эксплуатации высоковольтных трансформаторов. В обеих ситуациях контроль диэлектрической проницаемости исследуемого масла необходимо проводить синхронно с контролем диэлектрической проницаемости эталонного образца масла.

Бензины с добавкой спиртов.

В настоящее время все большее внимание уделяется производству и применению высокооктановых бензинов, полученных по технологии «смешения» низкооктановых бензинов с высокооктановыми техническими спиртами. Основными достоинствами спиртовых бензинов являются более высокая экологичность и меньшая себестоимость по сравнению с традиционными чисто нефтяными и газовыми аналогами [16, 17].

Для автомобильных бензинов актуальной задачей остается контроль качества в процессе производства и при транспортировке и хранении. Традиционные высокооктановые бензины производятся на крупных НПЗ в соответствии с ДСТУ. Отличительной особенностью НПЗ является использование полного цикла производства бензинов – от исходного сырья до высокооктановой готовой продукции. Контроль качества готовой продукции производится в специализированных лабораториях заводов в рамках стандартизованных методов.

Производители спиртовых бензинов обычно производят продукцию на мини-заводах, при этом параметры спиртовых бензинов соответствуют требованиям ТУ, а не ДСТУ [16]. Контроль параметров готовой продукции может производиться эпизодически, например в

лабораториях крупных НПЗ или нефтебаз. Поэтому представляет интерес перспективность использования результатов экспресс-анализа комплексной диэлектрической проницаемости спиртовых бензинов для контроля их качества.

Для получения высокооктанового бензина в низкооктановый бензин добавляют технический спирт – неочищенный, с большим количеством сивушных масел, обезвоженный и денатурированный бензином.

Спиртовое топливо делится на две категории – автобензин с содержанием биоэтанола не менее 30 % относится к альтернативным топливам, а если биоэтанола менее 30 %, то оно не является альтернативным, а относится к спиртовому [16]. Спиртовые марки бензинов и альтернативные топлива выпускаются по разным нормативным документам.

Основным недостатком бензиново-спиртовых топлив является их фазовая нестабильность, обусловленная наличием в них небольших количеств воды и, как следствие, ограниченной взаимной растворимостью компонентов. Введением в спиртовые топлива соответствующих модификаторов и стабилизаторов удается преодолеть возникающие трудности. Наибольшее влияние на расслаиваемость спиртовых бензинов оказывает содержание воды. Для обеспечения стабильности бензинов со спиртами при производстве, хранении и применении необходимо: предотвращать попадание в них воды; использовать стабилизирующие добавки или, иначе говоря, сорастворители, гомогенизирующие систему бензин – вода – спирт [16].

Необходимость введения стабилизирующих добавок существенно усложняет состав спиртовых бензинов. Так как спиртовые бензины производят по ТУ, то производитель сам определяет химический состав готового продукта, в том числе количество «вредных» составляющих, например, того же бензола, который приводит к повышенному износу цилиндров двигателя и, конечно, наносит вред окружающей среде. Если учесть, что и основа – низкооктановый бензин – может быть получен от разных производителей, то результирующий химический состав высокооктановых спиртовых бензинов становится разнообразным.

Наличие в составе высокооктанового бензина спиртовой добавки очевидным образом приводит к увеличению его диэлектрической проницаемости по сравнению с нефтяными и газовыми аналогами. Действительно, при использовании 2 мл кюветы резонансная частота резонатора, нагруженного образцами спиртовых бензинов, выходила за рабочий диапазон резонатора диэлектрометра.

На рис. 3 приведены результаты предварительных исследований при использовании 1 мл кюветы для нескольких образцов спиртовых бензинов разных производителей.

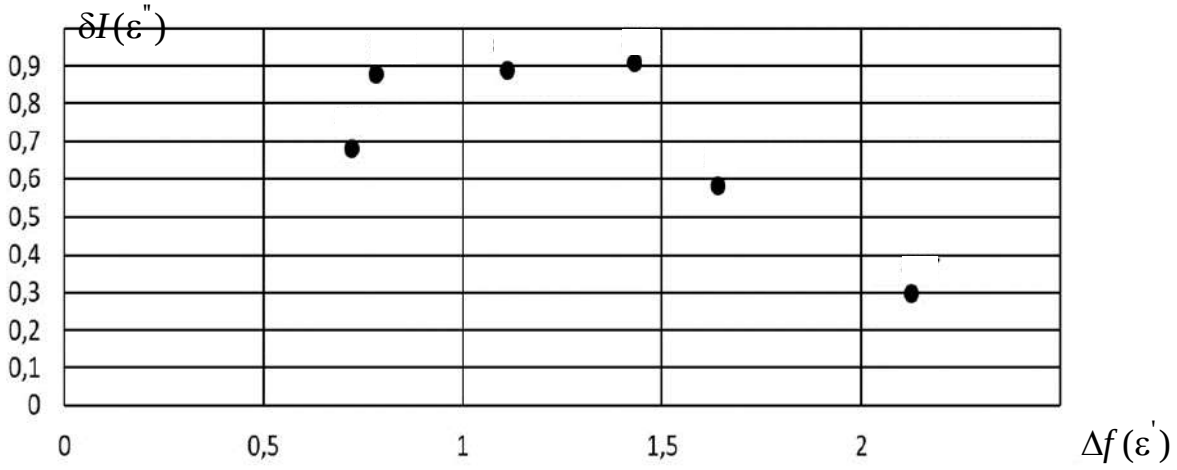


Рис. 3. Результаты исследования спиртовых бензинов

По оси абсцисс на этом рисунке отложены величины разности $\Delta f(\varepsilon')$ резонансных частот резонатора, нагруженного пустой кюветой $\Delta f(\varepsilon')$, и резонатора, нагруженного образцом исследуемого спиртового бензина $f_{сб}(\varepsilon')$, а по оси ординат величины $\delta I(\varepsilon'')$, представляющие отношение величины тока, прошедшего через резонатор, нагруженный исследуемым бензином $I_{сб}(\varepsilon'')$, к аналогичной величине, когда резонатор нагружен пустой кюветой $I_0(\varepsilon'')$.

Данные на рис. 3 показывают, что результаты начального этапа исследований пока не позволяют выявить преобладающее влияние спиртовой добавки на расположение экспериментальных точек на комплексной плоскости. Например, образцам с различными октановыми числами по моторному методу 82,8 (точка 2) и 84,5 (точка 1) соответствуют близкие величины $\Delta f(\varepsilon') < 0{,}8$ и $\delta I(\varepsilon'') > 0{,}68$ и в то же время у образца с октановым числом 82,7 (точка 6) близким к октановому числу 82,8 (точка 2) соответствуют сильно отличающиеся величины – $\Delta f(\varepsilon') = 2{,}12$ и $\delta I(\varepsilon'') = 0{,}301$.

Обеспечить требуемое октановое число производитель спиртовых бензинов может как путем увеличения содержания спирта, так и путем добавки других высокооктановых компонентов, например бензола, октановое число которого по моторному методу составляет 100 о.е. Очевидно, что интегральный химический состав у таких бензинов с близким октановым числом, а значит и положение соответствующих им точек на комплексной плоскости, будут различными.

Результаты исследований комплексной диэлектрической проницаемости спиртовых бензинов необходимо анализировать совместно с информацией о химическом составе образцов.

Кроме того, объема образцов 1 мл недостаточно для анализа спиртовых бензинов. Это следует из того, что перестройка резонансной частоты резонатора почти на порядок меньше, чем для обычных бензинов при объеме 2 мл. Поэтому необходимо увеличить объем образцов до 1,4 – 1,7 мл, чтобы восстановить разрешение по действительной части комплексной диэлектрической проницаемости спиртовых бензинов.

Выводы

Метод СВЧ диэлектрометрии обеспечивает разрешение, достаточное для экспресс-анализа на комплексной плоскости смесей жидких горючесмазочных материалов, результирующая диэлектрическая проницаемость которых находится в рабочем диапазоне частот резонатора.

Для проведения экспресс-анализа смесей бензинов необходимы эталонные образцы исходного бензина (трансформаторного масла). При отсутствии эталонных образцов анализ возможен с помощью предварительно созданной базы данных комплексной диэлектрической проницаемости для наиболее типичных образцов исходного бензина (масла).

Учитывая широкое многообразие типов исходных бензинов и спиртов, используемых для производства высокооктановых спиртовых бензинов, исследование комплексной диэлектрической проницаемости целесообразно совместить с исследованием их химического состава.

Список литературы:

1. М.А. Суслин. Микроволновый контроль авиационных ГСМ с использованием радиотехнических методов расчета цепей с распределенными параметрами. Москва : Машиностроение-1, 2006. 120 с.

2. М.П. Пархоменко, Д.С. Калёнов, И.С. Ерёмин, Н.А. Федосеев, В.М. Колесникова, Ю.Л. Баринов. Волноводный метод измерений электромагнитных параметров материалов в СВЧ диапазоне и оценка погрешности измерений // Журнал радиоэлектроники [электронный журнал]. 2018. № 9. С.1-19. Режим доступа: http://jre.cplire.ru/jre/sep18/6/text.pdf.

3. А.В. Мамыкин, А.Л. Кукла, А.С. Мастренко, Е П. Мацас, Л.М. Матвиенко. Способ экспресс-оценки октанового числа бензина с использованием портативного спектроимпедансного измерителя и методов статистического анализа // Технология и конструирование в электронной аппаратуре. 2017. № 4–5. С. 52-60. Метрология. Стандартизация ISSN 2225-5818.

4. С.А. Поляков Средство диэлектрометрического контроля бензина : дис. … канд. техн. наук. Орел, 2014. 122 с.
5. В.М. Колешко, В.Я. Сунка, А.А. Худницкий. Интеллектуальная система экспресс-контроля моторного топлива высокочастотными методами // Машиностроение : республ. межвед. сб. научн. трудов; М-во образования респ. Беларусь ; по материалам междунар. науч.-техн. конф. «Материалы, оборудование и ресурсосберегающие технологии в машиностроении» ; под. ред. Б.М. Хрусталева / Белорусский национальный технический университет. Минск : БНТУ. Вып.25. С.354-359.
6. В.М. Колешко, В.Я. Сунка, А.В. Шиманович, Ю.В. Левый, В.О. Грибовский. Экспресс анализатор моторного топлива для автомобилей // Машиностроение: республ. межвед. сб. научн. трудов; по материалам междунар. науч.-техн. конф. «Материалы, оборудование и ресурсосберегающие технологии в машиностроении» 06-09 апреля 2012 г. : в 2-х т. ; под. ред. Б.М. Хрусталева. Минск : БНТУ. 2012. Вып. 26, т.2. С. 248-255.
7. Р.А. Кремзер, К.В. Дорожкин, А.В. Бадьин, Д.С. Бодажков. Диэлектрические свойства автомобильного топлива с присадками в КВЧ диапазоне // 8-я Междунар. науч.-практ. конф. Актуальные проблемы радиофизики. АПР 2019 Сборник трудов конференции. 1-4 октября 2019, Томск. С.212-213.
8. Григоров А.Б., Карножицкий П.В., Слободской С.А. Диэлектрическая проницаемость как комплексный показатель, характеризующий изменение качества моторных масел в процессе их эксплуатации // Вестник Нац. техн. ун-та «ХПИ». Харьков : НТУ «ХПИ», 2006. №25. С. 169-175.
9. Григоров А.Б., Карножицкий П.В., Наглюк И.С. Изменение диэлектрической проницаемости дизельных моторных масел в эксплуатации // Автомобильный транспорт. Харьков : ХНАДУ, 2007. №20. С. 95-97.
10. Ляпина О.В., Власов Ю.А., Ляпин А.Н. Метод идентификации моторного топлива в смазочном масле автомобильных агрегатов // Фундаментальные исследования. 2015. № 2 (ч. 8). С. 1637-1641.
11. И.С. Наглюк Оценка качества моторных масел при эксплуатации легковых автомобилей // Автомобильный транспорт. 2011. Вып. 29. С.184-186.
12. О.В. Ляпина, Ю.А. Власов, А.Н. Ляпин. Метод идентификации моторного топлива в смазочном масле автомобильных агрегатов // Фундаментальные исследования. 2015. № 2 (ч. 8). С. 1637-1641.
13. В.П. Шестопалов, К.П. Яцук Методы измерения диэлектрической проницаемости вещества на сверхвысоких частотах // Успехи физических наук. 1961. Т. LXXIV, вып. 4. С. 721-755.
14. Жуков Б.В. СВЧ диэлектрометр для экспресс-анализа октановых чисел автомобильных топлив // Датчики и системы. 2008. № 11. С.15-17.
15. Б.В. Жуков, С.И. Борбулев. Оперативный контроль параметров жидких горюче-смазочных материалов // Радиотехника 2019. Вып. №196. С. 62-69.
16. Сысоев Д. Спиртовой» бензин в Украине – достойная альтернатива или обман? // Автохимия. Институт потребительских экспертиз. Опубл. 2021.03.24.
17. Плюсы и минусы использования спиртового бензина // https://plusiminusi.ru/plyusy-i-minusy-ispolzovaniya-spirtovogo-benzina.

Поступила в редколлегию 04.10.2021

Сведения об авторах:

Жуков Борис Владимирович – канд. техн. наук, Институт радиофизики и электроники им. А.Я. Усикова НАН Украины, старший научный сотрудник отдела физических основ радиолокации; Украина; e-mail: zkov31@meta.ua

Борбулев Станислав Игоревич – Институт современной обработки металлов; Институт радиофизики и электроники им. А.Я. Усикова НАН Украины, соискатель; Украина; e-mail: Stanislav.borbulev@gmail.com

Одновол Андрей Владимирович – Институт радиофизики и электроники им А. Я. Усикова НАН Украины, младший научный сотрудник; Украина.

МЕТОДИ ПЕРСПЕКТИВНИХ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ
МЕТОДЫ ПЕРСПЕКТИВНИХ КРИПТОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ
METHODS OF PROMISING CRYPTOGRAPHIC TRANSFORMATIONS

УДК 004.056.55

Обґрунтування та пропозиції щодо вибору, удосконалення та стандартизації механізму постквантового електронного підпису на національному та міжнародному рівнях / *І.Д. Горбенко, О.Г. Качко, О.В. Потій, Ю.І. Горбенко, В.А. Пономар, М.В. Єсіна, І.В. Стельник, С.О. Кандій, К.О.Кузнецова* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 207. С. 5 – 26.

Наразі та в перспективі для криптографічного захисту інформації застосовуються та будуть застосовуватись математичні методи, механізми та алгоритми стандартизованих асиметричних криптоперетворень типу електронний підпис (ЕП). Електронний підпис є основною та суттєвою складовою забезпечення кібербезпеки у сенсі якісного надання таких послуг з безпеки інформації як цілісність, неспростовність та автентичність інформації та даних, що обробляються. Але є реально обґрунтовані підозри, що у постквантовий період існуючі стандарти ЕП будуть зламуватись та компрометуватись з використанням класичних та квантових криптоаналітичних систем з відповідним математичним, програмним та апаратно-програмним забезпеченням. Проведено аналіз, що підтверджує, що уже практично розроблені, виготовлені та застосовуються квантові комп'ютери. При цьому вважається, що фактичний стан розроблення та застосування потужних квантових комп'ютерів та їх математичного і програмного забезпечення є, очевидно, строго конфіденційним та надійно захищається, а розголошуються тільки явно відомі дані про квантові комп'ютери та їх можливості застосування в криптології. Проведено попередній аналіз, який показує, що в Україні є розуміння існування загроз кібербезпеці та безпеці інформації у випадку застосування у перехідний та постквантовий періоди існуючих стандартизованих ЕП. Одним із основних проблемних питань щодо забезпечення необхідних рівнів безпеки в перехідний та постквантовий періоди є також розробка та прийняття постквантових стандартів ЕП. Метою статті є обґрунтування, порівняння альтернатив та розробка пропозицій щодо вибору та стандартизації постквантових стандартів ЕП на міжнародному та національному рівнях з урахування результатів 2-го та 3-го раундів конкурсу NIST США та національних досліджень.

Ключові слова: електронний підпис; криптографічний захист інформації; постквантовий період; «Сокіл»; Falcon; NIST PQC.

Табл. 4. Іл. 4. Бібліогр.: 35 назв.

УДК 004.056.55

Обоснование и предложения по выбору, усовершенствованию и стандартизации механизма постквантовой электронной подписи на национальном и международном уровнях / *И.Д. Горбенко, Е.Г. Качко, А.В. Потий, Ю.И. Горбенко, В.А. Пономарь, М.В. Есина, И.В. Стельник, С.О. Кандий, Е.А.Кузнецова* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 207. С. 5 – 26.

В настоящее время и в перспективе для криптографической защиты информации применяются и будут применяться математические методы, механизмы и алгоритмы стандартизированных асимметричных криптопреобразований типа электронная подпись (ЭП). Электронная подпись является основной и существенной составляющей обеспечения кибербезопасности в смысле качественного предоставления таких услуг по безопасности информации как целостность, неопровержимость и подлинность информации и обрабатываемых данных. Но есть реально обоснованные подозрения, что в постквантовый период существующие стандарты ЭП будут взламываться и компрометироваться с использованием классических и квантовых криптоаналитических систем с соответствующим математическим, программным и аппаратно-программным обеспечением. Проведен анализ, подтверждающий, что практически разработаны, изготовлены и применяются квантовые компьютеры. При этом считается, что фактическое состояние разработки и применения мощных квантовых компьютеров и их математического и программного обеспечения, очевидно, строго конфиденциально и надежно защищается, а разглашаются только явно известные данные о квантовых компьютерах и их возможности применения в криптологии. Проведен предварительный анализ, показывающий, что в Украине есть понимание существования угроз кибербезопасности и безопасности информации в случае применения в переходной и постквантовый периоды существующих стандартизированных ЭП. Одним из основных проблемных вопросов обеспечения необходимых уровней безопасности в переходной и постквантовый периоды является также разработка и принятие постквантовых стандартов ЭП. Цель статьи – обоснование, сравнение альтернатив и разработка предложений по выбору и стандартизации постквантовых стандартов ЭП на международном и национальном уровнях с учетом результатов 2-го и 3-го раундов конкурса NIST США и национальных исследований.

Ключевые слова: электронная подпись; криптографическая защита информации; постквантовый период; «Сокіл»; Falcon; NIST PQC.

Табл. 4. Ил. 4. Библиогр.: 35 назв.

UDC 004.056.55

Substantiation and proposals for the selection, improvement and standardization of the post-quantum electronic signature mechanism at the national and international levels / *I.D. Gorbenko, O.G. Kachko, O.V. Potii,*

Yu.I. Gorbenko, V.A. Ponomar, M.V. Yesina, I.V. Stelnik, S.O. Kandiy, K.O. Kuznetsova // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №207. P. 5 – 26.

At present and in the future, mathematical methods, mechanisms and algorithms of standardized asymmetric cryptotransformations such as electronic signature (ES) are and will be used for information cryptographic protection. Electronic signature is the main and essential component of cybersecurity, in terms of providing quality information security services such as integrity, irresistibility and authenticity of information and data processed. However, there are well-founded suspicions that in the post-quantum period the existing ES standards will be broken and compromised using classical and quantum cryptanalytic systems with appropriate mathematical, software and hardware-software. An analysis was performed, which confirms that quantum computers have already been developed, manufactured and used. It is believed that the actual state of development and use of powerful quantum computers and their mathematical and software is obviously strictly confidential and secure, and only publicly known data on quantum computers and their applications in cryptology are disclosed. A preliminary analysis has been carried out showing that in Ukraine there is an understanding of the existence of threats to cybersecurity and information security in the case of using available standardized ES in the transition and post-quantum periods. Currently, development and adoption of post-quantum ES standards is also one of the main issues in ensuring the necessary levels of security in the transition and post-quantum periods. The objective of this article is to substantiate, compare alternatives and develop proposals for the selection and standardization of post-quantum ES standards at the international and national levels, taking into account the results of the 2nd and 3rd rounds of the NIST US competition and national researches.

Key words: electronic signature; information cryptographic protection; post-quantum period; «Сокіл»; Falcon; NIST PQC.

4 tab. 4 fig. Ref: 35 items.

УДК 004.056.5

Теоретичні основи формування ефективних кодових слів для стеганографічного методу з кодовим управлінням / *А.А. Кобозєва, А.В. Соколов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 207. С. 27 – 39.

Стеганографія є важливою складовою сучасних систем захисту інформації. При цьому, в умовах сучасного кіберпростору, актуальною є розробка швидкодіючих стеганографічних методів, які мали б високий рівень стійкості до можливих атак стисненням, зашумленням і розмиттям. Одним з таких методів є стеганографічний метод з кодовим управлінням впровадження, заснований на ідеї попереднього додаткового кодування інформації, що впроваджуються за допомогою двійкових кодових слів, для яких трансформанти перетворення Уолша – Адамара мають задані властивості, що призводить до конкретної локалізації збурень в області перетворень Уолша – Адамара контейнера в результаті впровадження інформації. У роботі сформовано теоретичний базис для подальшого вдосконалення використовуваних у стеганографічному методі з кодовим управлінням кодових слів. Показано, що незважаючи на те, що зазначені кодові слова мають ідеальний вплив лише на задану трансформанту перетворення Уолша – Адамара, вони впливають відразу на кілька трансформант у просторі дискретного косинусного перетворення. Для вимірювання рівня вибірковості впливу на задану трансформанту дискретного косинусного перетворення (ДКП) введено поняття коефіцієнта селективності. Встановлено, що зі зростанням розміру блоків, що застосовуються, є тенденція до зменшення коефіцієнта селективності з огляду на наявність ефекту «близького сусіда». Ця тенденція, проте, обумовлена задіянням трансформант ДКП з близькими за значенням частотами, що мають подібну стійкість до можливих атак на впроваджене повідомлення. При цьому відношення суми модулів низькочастотних коефіцієнтів ДКП до суми модулів решти всіх коефіцієнтів ДКП зростає зі збільшенням розміру кодового слова. Доведено і практично підтверджено, що збільшення розміру кодового слова призводить до збільшення стійкості стеганографічного методу з кодовим управлінням. Теоретично обґрунтовано можливі способи подальшого практичного вдосконалення кодових слів, що застосовуються у стеганографічному методі з кодовим управлінням.

Ключові слова: стеганографія; дискретне косинусне перетворення; перетворення Уолша – Адамара; кодове управління впровадженням інформації; коефіцієнт селективності.

Табл. 3. Іл. 3. Бібліогр.: 27 назв.

УДК 004.056.5

Теоретические основы формирования эффективных кодовых слов для стеганографического метода с кодовым управлением / *А.А. Кобозева, А.В. Соколов* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 207. С. 27 – 39.

Стеганография является важной составляющей современных систем защиты информации. При этом в условиях современного киберпространства актуальной является разработка быстродействующих стеганографических методов, которые бы обладали высоким уровнем устойчивости к возможным атакам сжатием, зашумлением и размытием. Одним из таких методов является стеганографический метод с кодовым управлением внедрением, основанный на идее предварительного дополнительного кодирования внедряемой информации двоичными кодовыми словами, для которых трансформанты преобразования Уолша – Адамара имеют заданные свойства, что приводит к конкретной локализации возмущений в области преобразований Уолша – Адамара контейнера в результате внедрения информации. В работе сформирован теоретический базис для дальнейшего совер-

шенствования применяемых в стеганографическом методе с кодовым управлением кодовых слов. Показано, что, несмотря на то, что указанные кодовые слова имеют идеальное воздействие лишь на заданную трансформанту преобразования Уолша – Адамара, они воздействуют сразу на несколько трансформант в пространстве дискретного косинусного преобразования. Для измерения уровня выборочности воздействия на заданную трансформанту дискретного косинусного преобразования (ДКП) введено понятие коэффициента селективности. Установлено, что с ростом размера применяемых блоков имеется тенденция к уменьшению коэффициента селективности ввиду наличия эффекта «близкого соседа». Данная тенденция, тем не менее, обусловлена задействованием трансформант ДКП с близкими по значению частотами, имеющими сходную устойчивость к возможным атакам на встроенное сообщение. При этом отношение суммы модулей низкочастотных коэффициентов ДКП к сумме модулей всех остальных коэффициентов ДКП растет с увеличением размера кодового слова. Доказано и практически подтверждено, что увеличение размера кодового слова приводит к увеличению устойчивости стеганографического метода с кодовым управлением. Теоретически обоснованы возможные способы дальнейшего практического совершенствования кодовых слов, применяемых в стеганографическом методе с кодовым управлением.

Ключевые слова: стеганография; дискретное косинусное преобразование; преобразование Уолша – Адамара; кодовое управление внедрением информации; коэффициент селективности.

Табл. 3. Ил. 3. Библиогр.: 27 назв.

UDC 004.056.5

Theoretical foundations for constructing effective codewords for the code-controlled information embedding steganographic method / *A.A. Kobozeva, A.V. Sokolov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №207. P. 27 – 39.

Steganography is an important component of modern information security systems. At the same time, in the conditions of modern cyberspace, it is relevant to develop high-performance steganographic methods that would have a high level of resistance to possible attacks by compression, noise, and blur. One of such methods is the steganographic method with code-controlled information embedding, based on the idea of preliminary coding of the information being embedded using binary codewords, for which the transformants of the Walsh-Hadamard transform have the specified properties. A specific localization of disturbances in the Walsh-Hadamard transform domain of the container takes place because of the information embedding. In this paper, a theoretical basis has been formed for further improvement of the codewords used in the code-controlled information embedding steganographic method. It is shown that despite the fact that these codewords have an ideal effect only on a given transformant of the Walsh-Hadamard transform, they affect several transformants at once in the domain of the discrete cosine transform (DCT). The concept of the selectivity coefficient is introduced to estimate the level of selectivity of the impact on a given DCT transformant. It has been established that with an increase in the size of the blocks used, a tendency is observed to a decrease in the selectivity coefficient due to the presence of the “close neighbor” effect. This trend is conditioned by the involvement of the DCT transformants with similar frequencies that have similar resistance to possible attacks on the embedded message. In this case, the ratio of the sum of absolute values of low-frequency DCT transformants to the sum of absolute values of all other DCT transformants increases with the size of the codeword. In this paper it has been proven and practically confirmed that an increase in the size of a codeword leads to an increase in the resistance of the code-controlled information embedding steganographic method. Possible ways of further practical improvement of codewords used in the code-controlled information embedding steganographic method are theoretically substantiated.

Key words: steganography; discrete cosine transform; Walsh-Hadamard transform; code-controlled information embedding; selectivity coefficient.

3 tab. 3 fig. Ref: 27 items.

УДК 621.391.15 : 519.7

Оцінка обчислювальної складності алгоритму CSIDH на суперсингулярних скручених і квадратичних кривих Едвардса / *А.В. Бессалов, О.В. Циганкова, С.В. Абрамов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 207. С. 40 – 51.

Розглянуто властивості скручених і квадратичних суперсингулярних кривих Эдвардса, що утворюють пари квадратичного кручення з порядком $p+1$ над простим полем F_p. Приведена модифікація алгоритму CSIDH, побудованого на изогениях цих кривих замість традиційної арифметики кривих у формі Монтгомери. Розраховано і табульовано параметри цих двох класів суперсингулярних кривих Едвардса при $p = 239$, на ізогеніях яких наведено приклад реалізації алгоритму CSIDH як схеми неінтерактивного розподілу секрету на основі секретних і відкритих ключів Аліси та Боба. Показано, що послідовності параметрів $\pm d^{(i)}$ ланцюжків ізогеній відповідно для квадратичних та скручених суперсингулярних кривих Едвардса мають реверсний характер на періоді послідовності. Запропоновано рекурентний алгоритм обчислення координат точок, які створюють ядра ізогеній непарних степенів, розглянуто його реалізація в різних координатних системах. Дано порівняльний аналіз вартості обчислень параметру d' ізогенної кривої E' з застосуванням $(W:Z)$-координат Фарашахи – Хоссейні і класичних проєктивних координат $(X:Y:Z)$. Відзначено, що всі обчислення в алгоритмі

CSIDH, які необхідні для обчислення загального секрету d_{AB}, зводяться лише до обчислень параметру d' ізогенної кривої E' і виконуються польовими операціями та скалярним добутком точки. Обговорюється дискусійне питання про відмову від обчислення ізогенної функції $\phi(R)$ точки R кривої в алгоритмі CSIDH.

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. 1. Бібліогр.: 17 назв.

УДК 621.391.15 : 519.7

Оценка вычислительной сложности алгоритма CSIDH на суперсингулярных скрученных и квадратичных кривых Эдвардса / *А.В. Бессалов, О.В. Цыганкова, С.В. Абрамов* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 207. С. 40 – 51.

Рассмотрены свойства скрученных и квадратичных суперсингулярных кривых Эдвардса, образующих пары квадратичного кручения с порядком $p+1$ над простым полем F_p. Приведена модификация алгоритма CSIDH, построенного на изогениях этих кривых взамен традиционной арифметики кривых в форме Монтгомери. Рассчитаны и табулированы параметры этих двух классов суперсингулярных кривых Эдвардса при $p = 239$, на изогениях которых приведен пример реализации алгоритме CSIDH как схемы неинтерактивного разделения секрета на основе секретных и открытых ключей Алисы и Боба. Показано, что последовательности параметров $\pm d^{(i)}$ цепочек изогений соответственно для квадратичных и скрученных суперсингулярных кривых Эдвардса имеют реверсный характер на периоде последовательности. Предложен рекуррентный алгоритм вычисления координат точек, образующих ядра изогений нечетных степеней, рассмотрена его реализация в различных координатных системах. Дан сравнительный анализ стоимости вычислений параметра d' изогенной кривой E' с использованием $(W:Z)$-координат Фарашахи – Хоссейни и классических проєктивных координат $(X:Y:Z)$. Отмечено, что все вычисления в алгоритме CSIDH, необходимые для вычисления общего секрета d_{AB}, сводятся лишь к вычислениям параметра d' изогенной кривой E' и выполняются полевыми операциями и скалярным произведением точки. Обсуждается дискуссионный вопрос об отказе от вычисления изогенной функции $\phi(R)$ точки R кривой в алгоритме CSIDH.

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. 1. Библиогр.: 17 назв.

UDC 621.391.15 : 519.7

Estimation of the computational cost of the CSIDH algorithm on supersingular twisted and quadratic Edwards curves / *A.V. Bessalov, O.V. Tsygankova, S.V. Abramov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №207. P. 40 – 51.

The properties of twisted and quadratic supersingular Edwards curves that form pairs of quadratic torsion with order $p+1$ over a prime field F_p are considered. A modification of the CSIDH algorithm based on the isogenies of these curves instead of the traditional arithmetic of curves in the Montgomery form is presented. The parameters of these two classes of supersingular Edwards curves for $p = 239$ are calculated and tabulated. An example of the isogenies of these curves in the implementation of the CSIDH algorithm as a non-interactive secret sharing scheme based on the secret and public keys of Alice and Bob is given. It is shown that the sequences of parameters $\pm d^{(i)}$ of isogeny chains for quadratic and twisted supersingular Edwards curves, respectively, have a reverse nature on the period of the sequence. A recurrent algorithm for calculating the coordinates of points that form the kernels of isogenies of odd degrees is proposed, and its implementation in various coordinate systems is considered. A comparative analysis of the cost of calculating the parameter d' of the isogenic curve E' using the Farashakhi-Hosseini $(W:Z)$-coordinates and classical projective coordinates $(X:Y:Z)$ is given. It is noted that all calculations in the CSIDH algorithm necessary to calculate the shared secret d_{AB} are reduced only to the calculation of the isogenic curve E' parameter d' and are performed by field operations and the scalar multiplication of the point. The controversial issue of refusal to calculate the isogenic function $\phi(R)$ of a curve point R in the CSIDH algorithm is discussed.

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

1 tab. Ref: 17 items.

УДК 004.043

Методи та засоби деанонімізації транзакцій в блокчейн / *В.В. Дубіна, Р.В. Олійников* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 207. С. 52 – 58.

Наведено результати дослідження властивостей формування та обробки транзакцій в блокчейн системах, з метою виявлення існуючих перешкод на шляху досягнення безпечного функціонування мережі, обробки і передачі даних між користувачами та визначення можливих засобів деанонімізації транзакцій. Анонімність у мережі – одна з причин популярності криптовалют та широкого поширення технології блокчейн. Однак її наявність є основою виникнення нечесних транзакцій, злочинних дій шахраїв і атак на систему. Тому одними з найголовніших на сьогоднішній день залишаються питання забезпечення надійного зберігання інформації та можливості відстеження підозрілої активності і своєчасного захисту користувачів у блокчейн системах. В статті досліджено відомі методи для підвищення анонімності і збереженні конфіденційності у сучасних мережах, заснованих на принципах технології блокчейн, виникаючі загрози у зв'язку з їх використанням і можливі шляхи відстеження дій учасників системи. Наводиться порівняльна характеристика відомих інструментів відстеження і можливих засобів деанонімізації історії проведених транзакцій. В результаті дослідження запропоновано використання окремої платформи для аналізу мережі у реальному часі, виявлення загроз та їх своєчасного усунення, із можливістю візуалізації залежностей і побудови адресних графів в результаті відстеження всього ланцюжка транзакцій. Інструмент дозволяє реалізовувати пошук серед криптовалютних адрес, блоків, транзакцій та тегів, а також виявляти кластери, пов'язані з певною адресою. Система проводить аналіз мережі у реальному часі, щоб отримати уявлення про статистику. Особлива увага приділяється виявленню так званих аномалій, тобто ідентифікації тих транзакцій, які відхиляються від стандартних структур. Це дозволяє виявляти і відстежувати потенційно зловмисні дії на ранніх стадіях.

Ключові слова: Blockchain; транзакція; консенсус; анонімність; деанонімізація.

Іл. 4. Бібліогр.: 19 назв.

УДК 004.043

Методы и средства деанонимизации транзакций в блокчейн / *В.В. Дубина, Р.В. Олейников* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 207. С. 52 – 58.

Приведены результаты исследования свойств формирования и обработки транзакций в блокчейн системах, с целью выявления существующих препятствий для достижения безопасного функционирования сети, обработки и передачи данных между пользователями и определения возможных средств деанонимизации транзакций. Анонимность в сети – одна из причин популярности криптовалют и широкого распространения технологии блокчейн. Однако ее наличие является основой возникновения нечестных транзакций, преступных действий мошенников и атак на систему. Поэтому одними из главных на сегодняшний день остаются вопросы обеспечения надежного хранения информации и возможности отслеживания подозрительной активности и своевременной защиты пользователей в блокчейн системах. В статье исследованы известные методы повышения анонимности и сохранения конфиденциальности в современных сетях, основанных на принципах технологии блокчейн, возникающие угрозы в связи с их использованием и возможные пути отслеживания действий участников системы. Проводится сравнительная характеристика известных инструментов отслеживания и возможных средств деанонимизации истории проведенных транзакций. В результате исследования предложено использование отдельной платформы для анализа сети в реальном времени, выявление угроз и их своевременного устранения, с возможностью визуализации зависимостей и построения адресных графов в результате отслеживания всей цепочки транзакций. Инструмент позволяет реализовывать поиск среди криптовалютных адресов, блоков, транзакций и тегов, а также выявлять кластеры, связанные с определенным адресом. Система проводит анализ сети в реальном времени, чтобы получить представление о статистике. Особое внимание уделяется выявлению так называемых аномалий, то есть идентификации транзакций, которые отклоняются от стандартных структур. Это позволяет выявлять и отслеживать потенциально злонамеренные действия на ранних стадиях.

Ключевые слова: Blockchain; транзакция; консенсус; анонимность; деанонимизация.

Ил. 4. Библиогр.: 19 назв.

UDC 004.043

Methods and means of deanonymization of transactions in blockchain / *V.V. Dubina, R.V. Oliynykov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №207. P. 52 – 58.

This paper presents the results of a study of the properties of transactions formation and processing of in blockchain systems, aimed to identify existing barriers to the secure functioning of the network, processing and transmission of data between users, and to determine possible means of deanonymizing transactions. The anonymity of the network is one of the reasons for cryptocurrencies popularity and widespread use of blockchain technology. However, its presence is the basis for unscrupulous transactions, criminal actions of fraudsters and attacks on the system. Therefore, one of the main issues today is to ensure the reliable storage of information and the ability to track suspicious activity and timely protection of users in blockchain systems. The article examines known methods of increasing anonymity and maintaining confidentiality in modern networks based on the principles of blockchain technology, the threats arising from their use and the possible ways of tracking the actions of system participants. A comparative description of known tracking tools and possible means of de-anonymization of the history of completed transactions is given. As a result of the study, it was proposed to use a separate platform to analyze the network in real time, identify threats and their timely elimination, with the ability to visualize relationships and build address graphs as a result of tracking the entire chain of transactions. The tool makes it possible to implement a search among cryptocurrency addresses, blocks, transactions and tags, as well as to identify clusters associated with a particular address. The system analyzes the network in real time to gain insight into the statistics. Particular attention is paid to detecting so-called anomalies, i.e., the

identification of transactions that deviate from standard structures. This allows identifying and tracking potentially malicious activities at an early stage.

Key words: Blockchain; transaction; consensus; anonymity; deanonymization.

4 fig. Ref: 19 items.

УДК 003.026:004.056

Аналіз шляхів підвищення стійкості криптоалгоритмів на алгебраїчних решітках щодо часових атак / *О.Є. Петренко, О.С. Петренко, О.В. Сєвєрінов, О.І. Фєдюшин, А.В. Зубрич, Д.В. Щербина* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 207. С. 59 – 65.

Метою статті є дослідження алгоритмів, стійкість яких базується на пошуку короткого вектору решітки, а також визначення стійких до часових атак параметрів цих алгоритмів. Розглядаються існуючі способи генерації ключів та вибір параметрів для криптографічних перетворень на алгебраїчних решітках стійких до часових атак. Зазначено, що рівномірний розподіл коефіцієнтів для генерації ключів алгоритму NTRU має певні недоліки, а саме: алгоритм NTRU має обмежене число параметрів, придатних до застосування в криптоперетвореннях, що пов'язано з вразливістю даного алгоритму до часових атак. З огляду на це, розглянуто можливість застосування дискретного нормального (Гаусівського) розподілу для утворення ключової пари, який дозволить запобігти чутливості алгоритму до часових атак. Даний спосіб генерації дискретного нормального розподілу вимагає перевірки відповідності вибірки властивостям нормального закону. Запропоновано застосування набору тестів SAGA. Вони дозволяють перевірити вибірки Гауса, які отримані за допомогою дискретного нормального розподілу. Результат перевірки показує, має чи ні вибірка властивості, що притаманні нормальному закону розподілу. Застосовуючи статистичні тести SAGA над поліномами криптографічних перетворень NTRU, було зроблено висновок, що дискретна Гаусівська вибірка дозволяє генерувати стійкі до часових атак параметри, використовуючи в якості середньоквадратичного відхилення норму або довжину короткого базису (вектору) решітки.

Ключові слова: алгебраїчні рещітки; дискретний нормальний розподіл; тести SAGA; часові атаки.

Табл. 5. Бібліогр.: 5 назв.

УДК 003.026:004.056

Анализ путей повышения стойкости криптоалгоритмов на алгебраических решётках до временных атак / *О.Е. Петренко, А.С. Петренко, А.В. Северинов, А.И. Федюшин, А.В. Зубрич, Д.В. Щербина* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 207. С. 59 – 65.

Целью статьи является исследование алгоритмов, стойкость которых базируется на поиске короткого вектора решетки, а также определение стойких к временным атакам параметров этих алгоритмов. Рассмотрены существующие способы генерации ключей и выбор параметров для криптографических преобразований на алгебраических решетках, стойких к временным атакам. Показано, что равномерное распределение коэффициентов для генерации ключей алгоритма NTRU имеет недостатки, а именно: ограниченное число параметров, пригодных для использования в криптопреобразованиях. Это связано с уязвимостью алгоритма временными атаками. Рассмотрена возможность использования дискретного нормального распределения для формирования ключевой пары, которое позволит противостоять восприимчивости временным атакам. Данный способ генерации требует проверки полученной выборки на соответствие свойствам нормального распределения. Предложено использование тестов SAGA. Они позволяют проверить выборки Гаусса, которые получены с помощью дискретного нормального распределения. Результат проверки показывает, имеет или нет выборка Гаусса свойства нормального распределения. Применяя тесты SAGA над полиномами криптографических преобразований NTRU, сделали вывод, что Гауссовская выборка позволяет генерировать стойкие к временным атакам параметры, используя в качестве среднеквадратического отклонения норму или длину короткого вектора решетки.

Ключевые слова: алгебраические решетки; дискретное нормальное распределение; тесты SAGA; временные атаки.

Табл. 5. Библиогр.: 5 назв.

UDC 003.026:004.056

Analysis of ways to increase stability of cryptographic algorithms on algebraic lattices against time attacks / *O.E. Petrenko, O.S. Petrenko, O.V. Sievierinov, O.I. Fiediushyn, A.V. Zubrych, D.V. Shcherbina* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №207. P. 59 – 65.

The aim of this work is to study the algorithms, the stability of which is based on the search for a short lattice vector, as well as to obtain time-resistant parameters of these algorithms. Existing methods for generating keys and choosing parameters for cryptographic transformations on algebraic lattices resistant to time attacks are considered. It is shown that the uniform distribution of coefficients for generating the NTRU algorithm keys has certain shortages, namely, a limited number of parameters suitable for use in cryptographical transformations. This is due to the vulnerability of this algorithm to time attacks. The possibility of using a discrete normal (Gaussian) distribution to form a key pair, which will prevent the sensitivity of the algorithm to time attacks, is considered. This method of generation requires checking the obtained sample for compliance with the properties of the normal distribution. The usage of SAGA tests has been proposed. They make it possible to check the Gaussian samples obtained using the discrete normal distribution. The verification result shows whether or not the sample has properties that are inherent in the normal distribution. The application of the SAGA statistical tests to the NTRU cryptographic transformation polynomials allowed us to

conclude that the discrete Gaussian sample makes it possible to generate time-resistant parameters using the norm or the length of the short basis (vector) of the lattice as the mean-square deviation.

Key words: algebraic lattices; discrete normal distribution; SAGA tests; time attacks.

5 tab. Ref: 5 items.

УДК 004.056.55

Аналіз стійкості ARX схем шифрування до інтегральної атаки та атаки нездійснених диференціалів / *В.І. Руженцев, О.І. Федюшин, С.А. Кохан* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 207. С. 66 – 73.

Аналізуються поширені ARX (Addition-Rotation-XOR) алгоритми шифрування: Chacha, Speckey, Simon, Chaskey, Sparkle. Ці алгоритми використовують лише три операції: модульне додавання, XOR додавання та циклічний зсув. Розробляються 16-бітні зменшені моделі цих алгоритмів, обираються і розроблюються методи аналізу та виконується аналіз стійкості цих алгоритмів до найбільш ефективних атак: інтегральної атаки та атаки нездійснених диференціалів**.** За показником – кількість елементарних операцій, яка потрібна для отримання показників випадкової підстановки та відсутності нездійснених диференціалів й інтегралів – визначено найбільш ефективні ARX алгоритми. Такими стали Speckey, який оперує двома 8-бітовими підблоками та потребує 36 елементарних операцій, та Chaskey, який працює з чотирма 4-бітовими підблоками і потребує 72 елементарні операції. Якщо рахувати, що одна 8-бітова операція еквівалентна двом 4-бітовим, то ці схеми є рівними за обраним показником. Найгірші показники продемонстрували 8-бітова схема Simon та 4-бітова схема ChaCha, які потребують майже вдвічі більшої кількості операцій ніж кращі схеми. Також зроблено висновок про важливість використання не однієї, а декількох операцій XOR додавання з ключем для загальної криптографічної стійкості ARX алгоритмів.

Ключові слова: криптоаналіз; стійкість; ARX-алгоритм; модульне додавання; циклічний зсув; нездійснений диференціал; різність; інтегральний криптоаналіз; випадкова підстановка.

Табл. 11. Іл. 6. Бібліогр.: 7 назв.

УДК 004.056.55

Анализ стойкости ARX схем шифрования к интегральной атаке и атаке невыполнимых дифференциалов / *В.И. Руженцев, А.И. Федюшин, С.А. Кохан* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 207. С. 66 – 73.

Анализируются распространенные ARX (Addition-Rotation-XOR) алгоритмы шифрования: Chacha, Speckey, Simon, Chaskey, Sparkle. Эти алгоритмы используют три основные операции: модульное сложение, XOR сложение и циклический сдвиг. Разрабатываются 16-битовые уменьшенные модели этих алгоритмов, выбираются и разрабатываются методы анализа и выполняется анализ стойкости этих алгоритмов к наиболее эффективным для этого класса алгоритмов атакам: интегральная атака и атака невыполнимых дифференциалов**.** По показателю – количество элементарных операций, которое необходимо для получения показателей случайной подстановки и отсутствия невыполнимых дифференциалов и интегралов – определены наиболее эффективные ARX алгоритмы. Такими стали Speckey, которая оперирует двумя 8-битовыми подблоками и требует 36 элементарных операций, и Chaskey, которая работает с четырьмя 4-битовыми подблоками и требует 72 элементарные операции. Если считать, что одна 8-битовая операция эквивалентна двум 4-битовым, то эти схемы получаются равными по выбранному показателю. Худшие показатели продемонстрировали 8-битовая схема Simon и 4-битовая схема ChaCha, которые требуют почти вдвое больше операций, чем лучшие схемы. Также сделан вывод о важности использования не одной, а нескольких операций XOR сложения с ключом для общей криптографической стойкости ARX алгоритмов.

Ключевые слова: криптоанализ; стойкость; ARX-алгоритм; модульное сложение; циклический сдвиг; невіполнимый дифференциал; разность; интегральный криптоанализ; случайная подстановка.

Табл. 11. Ил. 6. Библиогр.: 7 назв.

UDC 004.056.55

Analysis of ARX encryption schemes resistance to the integral attack and impracticable differentials attack / *V.I. Ruzhentsev, O.I. Fediushyn, S.A. Kokhan* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №207. P. 66 – 73.

Common ARX (Addition-Rotation-XOR) encryption algorithms are analyzed. These algorithms are Chacha, Speckey, Simon, Chaskey, Sparkle. These algorithms use three basic operations: modular addition, XOR addition, and rotation. 16-bit reduced models of these algorithms are developed, methods of analysis are selected and developed, and the analysis of the resistance of these algorithms to the most effective attacks (integral attack and attack of impossible differentials) for this class of algorithms is performed. According to the selected indicator – the number of elementary operations that is necessary to obtain parameters of random substitution and the absence of impossible differentials and integrals – the most effective ARX algorithms are determined. These are Speckey, which operates on two 8-bit subblocks and requires 36 elementary operations, and Chaskey, which operates on four 4-bit subblocks and requires 72 elementary operations. If we assume that one 8-bit operation is equivalent to two 4-bit operations, then these schemes are equal in terms of the chosen indicator. The worst performers were the 8-bit Simon scheme and the 4-bit ChaCha scheme, which require almost twice as many operations as the best schemes. A conclusion was also made about the im-

portance of using not one, but several XOR operations of key addition for the overall cryptographic strength of ARX algorithms.

Key words: cryptanalysis; strength; ARX algorithm; modular addition; cyclic shift; impossible differential cryptanalysis; difference; integral cryptanalysis; random permutation.

11 tab. 6 fig. Ref: 7 items.

УДК 003.026:004.056

Сильні та слабкі сторони алгоритму на основі багатовимірних перетворень rainbow та його здатність блокувати атаки сторонніми каналами / *Д.В. Гармаш* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 207. С. 74 – 77.

Розглядається аналіз сутності та можливості захисту постквантового криптографічного алгоритму Rainbow. Розглядаються основні властивості алгоритмів на основі багатовимірних квадратичних перетворень. Наведено математичні схеми та операції, які використовуються алгоритмом Rainbow. Оцінюється перспектива застосування алгоритмів на основі багатовимірних квадратичних перетворень у постквантовий час. Дається оцінка того, які ресурси та обчислювальна енергія необхідна для вдалого використання алгоритмів на основі багатовимірних квадратичних перетворень. Наведено основні позитивні сторони алгоритму та його слабкості. Наведено аналізи стосовно здатності захисту алгоритму від атаки сторонніми каналами.

Ключові слова: Rainbow; криптоаналіз; вразливість; мінранк; схема; алгоритм.

Бібліогр.: 8 назв.

УДК 003.026:004.056

Сильные и слабые стороны алгоритма на основе многоизмерных преобразований rainbow и его способность блокировать атаки сторонними каналами / *Д.В. Гармаш* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 207. С. 74 – 77.

Рассматривается анализ сущности и возможности защиты постквантового криптографического алгоритма Rainbow. Рассматриваются главные характеристики алгоритмов на базе многомерных квадратических преобразований. Представлены математические схемы и операции, используемые алгоритмом Rainbow. Оценивается перспектива применения алгоритмов на основе многомерных квадратических преобразований в постквантовое время. Дана оценка того, какие ресурсы и вычислительная энергия необходимы для успешного использования алгоритмов на основе многомерных квадратических преобразований. Приведены основные положительные стороны алгоритма и их слабости. Приведены анализы способности защиты алгоритма от атаки посторонними каналами.

Ключевые слова: Rainbow; криптоанализ; уязвимость; минранк; схема; алгоритм.

Библиогр.: 8 назв.

UDC 003.026:004.056

Strengths and weaknesses of the algorithm based on multidimensional rainbow transformations and its ability to block attacks by third party channels / *D.V. Harmash* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №207. P. 74 – 77.

The paper considers the analysis of the essence and possibilities to protect the Rainbow post-quantum cryptographic algorithm. The main properties of algorithms based on multidimensional quadratic transformations are considered. Mathematical schemes and operations used by the Rainbow algorithm are given. The perspective of using algorithms based on multidimensional quadratic transformations in post-quantum time is estimated. An estimate of what resources and computing energy are required for the successful use of algorithms based on multidimensional quadratic transformations is given. The main positive aspects of the algorithm and its weaknesses are outlined. Analyzes are given regarding the ability of the algorithm to protect against attack by third-party channels.

Key words: Rainbow; cryptanalysis; vulnerability; minrank; scheme; algorithm.

УДК 004.7:517.9

Один підхід до побудови індивідуальних математичних моделей захисту у бездротових сенсорних мережах / *Є. В. Котух, В. О. Любчак, О. П. Страх* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 207. С. 78 –82.

Сучасний рівень розвитку техніки та технологій характеризується постійним розширенням різноманіття й складності механічних та керованих об’єктів, функціонування яких відбувається в неперервно-дискретному за часом режимі. Одним із таких об’єктів є процес поширення шкідливого програмного забезпечення у бездротових сенсорних мережах, постійне зростання тенденцій до яких обумовлене їх використанням як єдиного виду самоорганізованої мережі передачі даних з найменшою трудомісткістю та маловитратністю.

Концепція побудови сенсорних мереж остаточно не сформувалася. Тож вивчення певних властивостей таких мереж є дуже важливим як для вітчизняної, так і для світової науки. Більш того, для стратегічно важливих галузей країни, зокрема оборонної, захист бездротових сенсорних мереж є дуже важливою складовою.

Запропоновано нову модель поширення шкідливого програмного забезпечення, яка описується деякою крайовою задачею для імпульсної динамічної системи на часовій шкалі.

Ключові слова: бездротова сенсорна мережа; шкідливе програмне забезпечення; крайова задача.

Бібліогр.: 19 назв.

УДК 004.7:517.9

Один подход к построению индивидуальных математических моделей защиты в беспроводных сенсорных сетях / *Е. В. Котух, В. А. Любчак, А. П. Страх* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 207. С. 78 –82.

Современный уровень развития техники и технологий характеризуется постоянным расширением разнообразия и сложности механических и управляемых объектов, функционирование которых происходит в непрерывно-дискретном по времени режиме. Одним из таких объектов является процесс распространения вредоносного программного обеспечения в беспроводных сенсорных сетях, постоянный рост тенденций к которому обусловлен их использованием как единого вида самоорганизованной сети передачи данных с наименьшей трудоемкостью и малозатратностью.

Концепция построения сенсорных сетей совсем не сформировалась. Поэтому изучение определенных свойств таких сетей очень важно как для отечественной, так и для мировой науки. Более того, для стратегически важных отраслей страны, в частности оборонной, защита беспроводных сенсорных сетей является очень важной составляющей.

Предложена новая модель распространения вредоносного программного обеспечения, которая описывается некоторой краевой задачей для импульсной динамической системы на временной шкале.

Ключевые слова: беспроводная сенсорная сеть; вредоносное программное обеспечение; краевая задача.

Библиогр.: 19 назв.

UDC 004.7:517.9

One approach to the design of individual mathematical models of security in wireless sensor networks / *Y.V. Kotukh, V.O. Lyubchak, O.P. Strakh* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №207. P. 78 –82

The current level of development of engineering and technology is characterized by a constant expansion of the variety and complexity of mechanical and controlled objects, the operation of which occurs in a continuous-discrete time mode. One of these objects is the process of spreading malicious software in wireless sensor networks, the constant growth of trends towards which is due to their use as a single type of self-organized data transmission network with the least labor intensity and low cost.

The concept of building sensor networks has not been formed at all. Therefore, the study of certain properties of such networks is very important for both domestic and world science. Moreover, for the strategically important sectors of the country, in particular defense, the protection of wireless sensor networks is a very important component.

A new model of malware distribution is proposed, which is described by some boundary value problem for an impulsive dynamical system on a time scale.

Key words: wireless sensor network; malware; boundary value problem.

Ref: 19 items.

РАДІОЛОКАЦІЯ І РАДІОНАВІГАЦІЯ
РАДИОЛОКАЦИЯ И РАДИОНАВИГАЦИЯ
RADIOLOCATION AND RADIONAVIGATION

УДК 004.89: 621.396

Оцінка ефективності обробки радіолокаційних зображень на основі інтелектуального аналізу процесів / *В.В. Жирнов, С.В. Солонська, І.Ю. Шубін* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 207. С. 83 – 88.

Наведено результати розробки методу автоматичного виявлення радіолокаційних відміток повітряних об’єктів та їх розпізнавання з обробкою реальних записів в оглядових РЛС. Актуальність цієї роботи полягає у створенні системи автоматичної обробки інформації для забезпечення ефективного виявлення корисних сигналів за рахунок накопичення сигнальної (енергетичної) та смислової інформації. Метод заснований на визначенні семантичних складових на етапі формування і аналізу символьної моделі сигнальних відміток від точкових і протяжних повітряних об’єктів. Сигнальна інформація визначається предикатною функцією процесних знань формування та аналізу символьної моделі пачки імпульсних сигналів від точкових рухомих літальних апаратів таких як літак, вертоліт, БПЛА, і від протяжних атмосферних утворень – ангел-луна, хмари та інші. В результаті семантичного аналізу символьних зображень сигнальних відміток отримано класифікаційні відмітні ознаки повітряних об’єктів. Досліджено семантичні складові алгоритму прийняття рішень, що схожі на алгоритми прийняття рішень оператором. У розробленому алгоритмі сигнальна інформація записується предикатної функцією на множині амплітуд імпульсів сигнальної позначки, які перевищили деяке порогові значення. Розпізнавання повітряних об'єктів проводиться шляхом вирішення розроблених рівнянь предикатних операцій. Верифікація розробленого методу проведена на реальних даних, отриманих на оглядовій РЛС сантиметрового діапазону (тривалість імпульсу 1 мкс, частота зондування 365 Гц, період огляду 10 с). На основі цих даних змодельовано типи характерних позначок радіолокаційних сигналів. За результатами експериментів усі вони правильно ідентифіковані.

Ключові слова: семантичний аналіз; радіолокаційний сигнал; ідентифікація; протяжні атмосферні утворення; повітряний об'єкт.

Іл. 2. Бібліогр.: 15 назв.

УДК 004.89: 621.396

Оценка эффективности обработки радиолокационных изображений на основе интеллектуального анализа процессов / *В.В. Жирнов, С.В. Солонская, И.Ю. Шубин* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 207. С. 83 – 88.

Приводятся результаты разработки метода и экспериментальных исследований системы автоматического обнаружения радиолокационных отметок воздушных объектов и их распознавания с обработкою реальных записей в обзорных РЛС. Актуальность этих работ заключается в создании алгоритма системы автоматической обработки радиолокационной информации для обеспечения эффективного обнаружения полезных сигналов за счет накопления сигнальной (энергетической) и смысловой информации. Метод основан на определении семантических составляющих на этапе формирования и анализа символьной модели сигнальных отметок от точечных и протяженных воздушных объектов. Сигнальная информация описывается предикатной функцией процессных знаний формирования и анализа символьной модели пачки импульсных сигналов от точечных подвижных летательных аппаратов таких, как самолет, вертолет, БПЛА, и от протяженных атмосферных образований – ангел-эхо, облака, тучи. В результате семантического анализа символьных изображений сигнальных отметок получены классификационные отличительные признаки воздушных объектов. Исследованы семантические составляющие алгоритма принятия решений, которые подобны алгоритмам принятия решений оператором. В разработанном алгоритме сигнальная информация описывается предикатной функцией на множестве амплитуд импульсов сигнальной отметки, превысивших некоторое пороговое значение. Распознавание воздушных объектов проводится путем решения разработанных уравнений предикатных операций. Верификация разработанного метода проведена на реальных данных, полученных на обзорной РЛС сантиметрового диапазона (длительность импульса 1 мкс, частота зондирования 365 Гц, период обзора 10 с). На основе этих данных смоделированы типы характерных отметок радиолокационных сигналов. По результатам экспериментов все они были правильно идентифицированы.

Ключевые слова: семантический анализ; радиолокационный сигнал; идентификация; протяженные атмосферные образования; воздушный объект.

Ил. 2. Библиогр.: 15 назв.

UDC 004.89: 621.396

Evaluation of radar image processing efficiency based on intelligent analysis of processes / *V. Zhyrnov, S. Solonskaya, I. Shubin* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №207. P. 83 – 88.

The paper presents results of development of the method and experimental studies of the system for automatic detection of radar signals of aerial objects and their recognition with the processing of real records in surveillance radars. The relevance of this work consists in creation of algorithms for automatic information processing to ensure effective detection of useful signals due to accumulation of signal (energy) and semantic information. The method is based on the definition of semantic components at the stage of formation and analysis of the symbolic model of signals from point and extended air objects. Signal information is described by the predicate function of process knowledge of the formation and analysis of a symbolic model of a burst of impulse signals from point-like mobile aircraft such as an airplane, a helicopter, a UAV, and from extended atmospheric formations such as angel-echoes, clouds. As a result of semantic analysis of symbolic images of signal marks, classification distinctive features of air objects were obtained. The semantic components of the decision-making algorithm, similar to the decision-making algorithms used by the operator, have been investigated. In the developed algorithm, signal information is described by a predicate function on the set of signal mark pulse amplitudes that have exceeded a certain threshold value. Recognizing of aerial objects is carried out by solving the developed equations of predicate operations. The verification of the developed method was carried out on real data obtained on a survey radar of the centimeter range (pulse duration was 1 μs, probing frequency wass 365 Hz, survey period was 10 s). Based on these data, the types of characteristic marks of radar signals are modeled. According to the results of the experiments, they were all correctly identified.

Key words: semantic analysis; radar signal; identification; extended atmospheric formations; aerial object.

2 fig. Ref: 15 items.

УДК 007.51

Особливості управління завадостійкістю оглядової РЛС при її придушенні активними завадами та інформаційними впливами, що заважають / *В.М. Канцедал, А.А. Могила* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 207. С. 89 – 101.

Розглядаються особливості управління цілепокладанням при забезпеченні інформаційної стійкості режимів зондування оглядової РЛС при її придушенні активними завадами та інформаційними впливами, що заважають. Подолання складності процесів цілепокладання, обґрунтованості та оперативності прийняття рішень при дефіциті часу на його прийняття пов'язані із забезпеченням системності процесів цілепокладання, підвищенням рівнів їх інтелектуалізації та формалізації. Це сприятиме наданню бажаних властивостей багатоцільовим стратегіям та ситуаційному закону управління процесами РЕЗ та координації дій, що синтезуються в ході конфлікту.

Особливості подолання складності вирішуваної проблеми пов'язані з системністю процесів цілепокладання, підвищенням їх рівнів інтелектуалізації та формалізації.

Підвищення рівня інтелектуалізації процесів цілепокладання забезпечується:

- декомпозицією загальної задачі цілепокладання на окремі більш прості підзадачі з ефективними рішеннями, які реалізуються у відповідних підсистемах САУуст (або базових об'єднаннях її функціональних елементів) на етапах інформаційного забезпечення, підготовки, прийняття та реалізації рішень на ієрархічних рівнях управління;

- когнітивним аналізом цілей та рефлексивним синтезом процесів цілепокладання з залученням можливостей спеціалізованої інтелектуальної системи підтримки прийняття рішень для посилення креативно-рефлексивних здібностей суб'єкта управління та підвищення рівня його професійних компетенцій;

– поєднанням універсальності етапів раціональних управління синтезом стратегії управління процесами РЕЗ зі специфікою конфліктних ситуацій, суб'єктністю, когнітивним та рефлексивним характером інтелектуального управління.

Представлені способи та засоби часткової формалізації процесів цілепокладання, коли структурування головної мети проводиться з урахуванням належності до стратегій внутрішнього та зовнішнього управлінь РЕЗ, декомпозиції двосторонньої динамічної моделі конфлікту між системами комплексу РЕП і РЛС, ієрархії рівнів управління, застосованих різних підходів до цілепокладання і кризисного управління в цілому, а також методів обґрунтування цілей, витрат ресурсів та і контролю якості досягнення поставлених цілей.

Ці особливості дозволяють суттєво знизити ступінь суб'єктивності керуючих рішень щодо цілепокладання, і домогтися їх обґрунтованості, повноти, несуперечності та узгодженості.

Ключові слова: система управління; конфліктна ситуація; невизначеність; стійкість; цілепокладання; прийняття рішень, радіоелектронний захист.

Іл. 1. Бібліогр.: 24 назв.

УДК 007.51

Особенности управления помехозащищенностью обзорной РЛС при ее подавлении активными помехами и мешающими информационными воздействиями / *В.М. Канцедал, А.А. Могила* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 207. С. 89 – 101.

Рассматриваются особенности управления целеполаганием при обеспечении информационной устойчивости режимов зондирования обзорной РЛС при ее подавлении активными помехами и мешающими информационными воздействиями. Преодоление сложности процессов целеполагания, обоснованности и оперативности принятия решений при дефиците времени на его принятие связано с обеспечением системности процессов целеполагания, повышением уровней их интеллектуализации и формализации. Это будет способствовать приданию синтезируемым в ходе конфликта многоцелевым стратегиям и ситуационному закону управления процессами РЭЗ и координации действий желательных свойств.

Повышение уровня интеллектуализации процессов целеполагания обеспечивается:

- декомпозицией общей задачи целеполагания на отдельные более простые подзадачи с эффективными решениями, реализуемые в соответствующих подсистемах САУ$_{уст}$ (или базовых объединениях ее функциональных элементов) на этапах информационного обеспечения, подготовки, принятия и реализации решений на иерархических уровнях управления;

- когнитивным анализом целей и рефлексивным синтезом процессов целеполагания с привлечением возможностей специализированной интеллектуальной системы поддержки принятия решений для усиления креативно-рефлексивных способностей субъекта управления и повышения уровня его профессиональных компетенций;

- совмещением универсальности этапов рациональных управления синтезом стратегии управления процессами РЭЗ со спецификой конфликтных ситуаций, субъектностью, когнитивностью и рефлексивным характером интеллектуального управления.

Представлены способы и средства частичной формализации процессов целеполагания, когда структурирование главной цели производится с учетом принадлежности к стратегиям внутреннего и внешнего управлений РЭЗ, декомпозиции двусторонней динамической модели конфликта между системами комплекса РЭП и РЛС, иерархии уровней управления, применяемых различных подходов к целеполаганию в кризисном управлении, а также методов обоснования целей, затрат ресурсов и контроля качества достижения поставленных целей.

Эти особенности позволяют существенно снизить степень субъективности управляющих решений для целеполагания и добиться их обоснованности, полноты, непротиворечивости и согласованности.

Ключевые слова: **с**истема управления; конфликтная ситуация; неопределенность; устойчивость; целеполагание; принятие решений, радиоэлектронная защита.

Ил. 1. Библиогр.: 24 назв.

UDC 007.51

Specific features of immunity control of survey radar under its suppression by active interference and interfering information effects / *V.M. Kantsedal, A.A. Mogyla* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №207. P. 89 – 101.

The features of goal-setting control while ensuring the information stability of the sounding modes of a surveillance radar when it is suppressed by active interference and interfering information influences are considered. Overcoming

the complexity of goal-setting processes, the validity and efficiency of decision-making with a shortage of time for its adoption is associated with insuring the consistency of goal-setting processes, increasing the levels of their intellectualization and formalization. This will contribute to imparting the desired properties, synthesized during the conflict, to the multipurpose strategies and the situational law of the control of the REP processes and the coordination of actions.

An increase in the level of intellectualization of goal-setting processes is ensured by:

- decomposition of the general goal-setting problem into separate, simpler subtasks with effective solutions, implemented in the corresponding subsystems of the ACS_{stab} (or basic associations of its functional elements) at stages of information support, preparation, adoption and implementation of the decision at the stages of hierarchical levels of management;
- cognitive analysis of goals and reflexive synthesis of goal-setting processes using the capabilities of a specialized intelligent decision support system to enhance the creative-reflexive abilities of the subject of management and increase the level of his professional competencies;
- combining the universality of the stages of rational management of the synthesis of the strategy for managing the REP processes with the specifics of conflict situations, subjectivity, cognition and reflexivity nature of intellectual control.

Methods and means for partial formalization of goal-setting processes are presented, when the structuring of the main goal is carried out taking into account belonging to the strategies of internal and external control of the REP, the decomposition of the two-sided dynamic model of the conflict between the systems of the RES complex and the radar, the hierarchy of management levels, various approaches applied to goal-setting in a crisis management, as well as methods of justifying goals, resource costs and control of achieving the goals.

These features can significantly reduce the degree of subjectivity of management for goal-setting and achieve their validity, completeness, consistency.

Key words: control system; conflict situation; uncertainty; stability; goal setting; decision making. electronic protection.

1 fig. Ref: 24 items.

УДК 621.396.96, 621.397.48:004.932.2

Комплексування інформаційних каналів систем виявлення та спостереження безпілотних літальних апаратів з позицій теорії статистичних рішень / *В.М. Карташов, В.О. Посошенко, В.І. Колісник, А.І. Капуста, М.В. Рибников, Є.В. Першин, В.О. Кізка* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 207. С. 102 – 112.

Безпілотні літальні апарати (БПЛА) забезпечують виконання широкого спектру корисних для людства завдань, але, з іншого боку, вони представляють серйозну загрозу в господарській, військовій та інших областях діяльності людини. Труднощі спостереження БПЛА з використанням сучасних технічних засобів, а також їх відносно невисока вартість призводять до розширення сфери протиправних дій з використанням БПЛА. Тому захист різних об'єктів від БПЛА є серйозним науково-технічним завданням сучасності.

Оскільки можливості відомих методів виявлення БПЛА різні, то на практиці реалізується спільне використання систем різного виду з метою підвищення інформативності одержуваних даних шляхом сумісної (комплексної) їх обробки.

Число публікацій в даній області постійно збільшується, значна увага приділяється й інтегрованим системам, побудованим з використанням різних фізичних сенсорів. Однак ефективність функціонування мультисенсорних систем з комплексною обробкою вихідних сигналів каналів на практиці залишається недостатньою.

Стаття присвячена дослідженню методів синтезу нових більш ефективних алгоритмів комплексування радіолокаційних, акустичних, оптичних і інфрачервоних інформаційних каналів інтегральних систем виявлення та розпізнавання БПЛА, які виконуються з позицій статистичної теорії оптимізації радіосистем.

Такий підхід дозволяє синтезувати оптимальну (відповідно до обраного критерію якості) комплексну систему обробку інформації, що забезпечує отримання максимальної кількості інформації з векторного процесу, що спостерігається на входах інформаційних каналів. Показана можливість побудови оптимального детектора БПЛА з використанням пізньої стратегії об'єднання інформації на рівні рішень, прийнятих в окремих каналах системи.

Ключові слова: безпілотний літальний апарат; виявлення; спостереження; комплексування; радіолокаційна станція; інтегрована система; інформаційний канал; обробка сигналів.

Іл. 1. Бібліогр.: 23 назв.

УДК 621.396.96, 621.397.48:004.932.2

Комплексирование информационных каналов систем обнаружения и наблюдения беспилотных летательных аппаратов с позиций теории статистических решений / *В.М. Карташов, В.А. Посошенко, В.И. Колесник, А.И. Капуста, Н.В. Рыбников, Е.В. Першин, В.А. Кизка* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 207. С. 102 – 112.

Беспилотные летательные аппараты (БПЛА) обеспечивают выполнение широкого спектра полезных для человечества задач, но, с другой стороны, они представляют серьезную угрозу в хозяйственной, военной и других областях деятельности человека. Трудности наблюдения БПЛА с использованием современных техниче-

ских средств, а также их относительно невысокая стоимость приводят к расширению сферы противоправных действий с использованием БПЛА. Поэтому защита различных объектов от БПЛА представляет собой серьёзную научно-техническую задачу современности.

Поскольку возможности известных методов обнаружения БПЛА различны, то на практике реализуется совместное использования систем различного вида с целью повышения информативности получаемых данных путем совместной (комплексной) их обработки.

Число публикаций в данной области постоянно увеличивается, значительное внимание уделяется и интегрированным системам, построенным с использованием различных физических сенсоров. Однако эффективность функционирования мультисенсорных систем с комплексной обработкой выходных сигналов каналов на практике остаётся недостаточной.

Статья посвящена исследованию методов синтеза новых более эффективных алгоритмов комплексирования радиолокационных, акустических, оптических и инфракрасных информационных каналов интегральных систем обнаружения и распознавания БПЛА, выполняемых с позиций статистической теории оптимизации радиосистем.

Такой подход позволяет синтезировать оптимальную (в соответствии с выбранным критерием качества) комплексную систему обработку информации, обеспечивающую получение максимального количества информации из векторного процесса, наблюдаемого на входах информационных каналов. Показана возможность построения оптимального обнаружителя БПЛА с использованием поздней стратегии объединения информации на уровне решений, принимаемых в отдельных каналах системы.

Ключевые слова: беспилотный летательный аппарат; обнаружение; наблюдение; комплексирование; радиолокационная станция; интегрированная система; информационный канал; обработка сигналов.

Ил. 1. Библиогр.: 23 назв.

UDC 621.396.96, 621.397.48:004.932.2

Complexing of information channels of UAV detection and observation systems from the statistic solutions theory standpoint / *V.M. Kartashov, V.O. Pososhenko, V.I. Kolisnyk, A.I. Kapusta, M.V. Rybnykov, I.V. Pershyn*, V.A. Kizka // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №207. P. 102 – 112.

Currently, unmanned aerial vehicles (UAVs) provide a wide range of useful tasks for humanity, but, on the other hand, they pose a serious threat in economic, military and other areas of human activity. Difficulties in observing UAVs using modern technical means, as well as their relatively low cost, lead to an expansion of the scope of UAVs based illegal actions. Therefore, the protection of various objects against UAVs is a serious scientific and technical task of today.

Since the possibilities of the known methods of UAV detection are different, the joint use of systems of different types is realized in practice nowadays, in order to increase the informativeness of the obtained data by their joint (complex) processing.

The number of publications in this field is constantly increasing, and considerable attention is paid to integrated systems built on the basis of various physical sensors. However, the efficiency of multi-sensor systems with integrated processing of the output signals of the channels in practice remains insufficient.

This article is devoted to the study of methods for the synthesis of new, more efficient algorithms for complexing radar, acoustic, optical and infrared information channels of integrated UAV detection and recognition systems, which are performed from the standpoint of statistical theory of radio system optimization.

This approach allows synthesizing the optimal (according to the selected quality criterion) complex information processing system, which ensures obtaining the maximum amount of information from the vector process observed at the inputs of information channels. There shown the possibility of constructing an optimal UAV detector with the use of the late strategy of combining information at the level of decisions made in individual channels of the system.

Key words: unmanned aerial vehicle; detection; observation; integration; radar station; integrated system; information channel; signal processing.

1 fig. Ref: 23 items.

УДК 621.396.96, 621.397.48

Виявлення радіолокаційних сигналів, розсіяних на акустичних збуреннях, створюваних БПЛА / *В.М. Карташов, В.О. Посошенко, В.І. Колісник, І.С. Селезньов, Р.І. Бобнев, А.І. Капуста* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 207. С. 113 – 122.

Розглянуто задачу радіолокаційного моніторингу БПЛА за його акустичним випромінюванням. Показано, що у низці практичних випадків такий підхід переважає спостереження радіолокаційними методами безпосередньо планера БПЛА. Відзначено, що радіосигнали, що розсіяно на акустичних пакетах від БПЛА, характеризуються невідомою заздалегідь комплексною огинаючою, що не дозволяє використовувати методи оптимальної фільтрації для їх виявлення та оцінювання. Показано, що для вирішення цих задач доцільно використовувати принцип накопичення на інтервалі спостереження приведеної до дисперсії шуму енергії вузькосмугового випадкового процесу, використовуючи статистичні відмінності шумових коливань і адаптивної суміші "сигнал плюс шум". Показано, що наведена оцінка енергії має або центральний, або нецентральний розподіл "хі-квадрат" з певним числом ступенів свободи та параметром нецентральності, який більше або дорівнює нулю. В результаті

порівняння поточного значення параметра нецентральності з пороговим значенням приймається рішення про наявність або відсутність на інтервалі спостереження корисного сигналу при мінімальній апріорній інформації про його параметри. Відзначено, що відомі вирази для диференційної щільності ймовірностей центрального та нецентрального розподілу "хі-квадрат" дозволяє отримати якісні оцінки пристрою виявлення, що синтезовано. Запропоновано практичну структурну схему цього пристрою з використанням обробки у квадратурних каналах коливань, що приймаються.

Ключові слова: акустичне випромінювання БПЛА; радіолокація акустичних пакетів; апріорна невизначеність; центральний розподіл "хі-квадрат"; нецентральний розподіл "хі-квадрат"; статистичне накопичення; енергетичний підхід; пороговий виявник.

Іл. 3. Бібліогр.: 35 назв.

УДК 621.396.96, 621.397.48

Обнаружение радиолокационных сигналов, рассеянных на акустических возмущениях, создаваемых БПЛА / *В.М. Карташов, В.А. Посошенко, В.И. Колесник, И.С. Селезнев, Р.И. Бобнев, А.И. Капуста* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 207. С. 113 – 122.

Рассмотрена задача радиолокационного мониторинга БПЛА по его акустическому излучению. Показано, что в ряде практических случаев такой подход предпочтительней наблюдения радиолокационными методами непосредственно планера БПЛА. Отмечено, что радиосигналы, рассеянные на акустических пакетах от БПЛА, характеризуются неизвестной заранее комплексной огибающей, что не позволяет использовать методы оптимальной фильтрации для их обнаружения и оценивания. Показано, что для решения этих задач целесообразно использовать принцип накопления на интервале наблюдения приведенной к дисперсии шума энергии узкополосного случайного процесса, используя статистические различия шумовых колебаний и аддитивной смеси "сигнал плюс шум". Показано, что приведенная к шумам оценка энергии имеет либо центральное, либо нецентральное распределение "хи-квадрат" с определенным числом степеней свободы и параметром нецентральности, большим или равным нулю. В результате сравнения текущего значения параметра нецентральности с пороговым значением выносится решение о наличии или отсутствии на интервале наблюдения полезного сигнала при минимальной априорной информации о его параметрах. Отмечено, что известные выражения для дифференциальных плотностей вероятности центрального и нецентрального распределений "хи-квадрат" позволяют получить качественные оценки синтезированного обнаружителя. Предложена практическая структурная схема обнаружителя с использованием обработки принимаемых колебаний в квадратурных каналах.

Ключевые слова: акустическое излучение БПЛА; радиолокация акустических пакетов; априорная неопределенность; центральное распределение "хи-квадрат"; нецентральное распределение "хи-квадрат"; статистическое накопление; энергетический подход; пороговый обнаружитель.

Ил. 3. Библиогр.: 35 назв.

UDC 621.396.96, 621.397.48

Detection of radar signals scattered by acoustic disturbances generated by UAVs / *V.M. Kartashov, V.A. Pososhenko, V.I. Kolesnik, I.S. Seleznjov, R.I. Bobnev, A.I. Kapusta* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №207. P. 113 – 122.

The problem of UAV radar monitoring by its acoustic radiation is considered. It is shown that in a number of practical cases such an approach is preferable to observation by radar methods directly from the UAV airframe. It is noted that the radio signals scattered by acoustic packets from the UAV are characterized by an unknown in advance complex envelope, which does not allow the use of optimal filtering methods for their detection and estimation. It is shown that to solve these problems, it is advisable to use the principle of accumulation over the observation interval of the energy of a narrow-band random process reduced to the noise dispersion, using the statistical differences between noise fluctuations and the additive "signal-plus-noise" mixture. It is shown that the energy estimate reduced to noise has either a central or an off-center "chi-square" distribution with a certain number of degrees of freedom and an off-center parameter greater than or equal to zero. As a result of comparing the current value of the no centrality parameter with the threshold value, a decision is made on the presence or absence of a useful signal in the observation interval with minimal a priori information about its parameters. It is noted that the well-known expressions for the differential probability densities of the central and non-central chi-square distributions allow one to obtain qualitative estimates of the synthesized detector. A practical structural diagram of a detector using processing of received oscillations in quadrature channels is proposed.

Key words: UAV acoustic radiation; radar acoustic packages; a priori uncertainty; central chi-square distribution; off-center chi-square distribution; statistical accumulation; energy approach; threshold detector.

3 fig. Ref: 35 items.

УДК 621.396.96

Оцінка відносної пропускної здатності літакових відповідачів вторинних радіолокаційних систем спостереження повітряного простору / *М.Г. Ткач* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 207. С. 123 – 131.

Значну роль в інформаційному забезпеченні систем контролю повітряного простору і управління повітряним рухом відіграють вторинні радіолокаційні системи спостереження повітряного простору. Ці системи забез-

печують радіолокаційне спостереження за повітряними об'єктами, які обладнані літаковими відповідачами і забезпечують двосторонній зв'язок за каналами запиту та відповіді для передачі даних між наземними радіолокаційними станціями та повітряними об’єктами.

У роботі проведено оцінку відносної пропускної здатності літакових відповідачів вторинних радіолокаційних систем спостереження повітряного простору при дії в каналі запиту корельованих та некорельованих завад. Аналіз пропускної здатності літакового відповідача показує, що літаковий відповідач не досягає максимального завантаження, яке закладено в наявну систему ідентифікації при дії навмисних корельованих завад. Це вказує на неоптимальне визначення коефіцієнта завантаження літакового відповідача існуючої вторинної радіолокаційної системи. Неправильне визначення максимального завантаження літакового відповідача призводить до зниження завадостійкості як літакового відповідача, так і всієї вторинної радіолокаційної системи. При цьому слід зазначити, що зацікавлена сторона має можливість несанкціонованого використання літакового відповідача для отримання інформації або паралізації останнього при застосуванні завад потрібної інтенсивності.

Ключові слова: вторинна радіолокаційна система; система спостереження; повітряний простір; літаковий відповідач; відносна пропускна здатність; ідентифікація; сигнал запиту; сигнал відповіді; завада.

Іл. 3. Бібліогр.: 38 назв.

УДК 621.396.96

Оценка относительной пропускной способности самолетных ответчиков вторичных радиолокационных систем наблюдения воздушного пространства / *М.Г. Ткач* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 207. С. 123 – 131.

Значительную роль в информационном обеспечении систем контроля воздушного пространства и управлении воздушным движением играют вторичные радиолокационные системы наблюдения воздушного пространства. Эти системы обеспечивают радиолокационное наблюдение за воздушными объектами, которые оборудованы самолетными ответчиками и обеспечивают двустороннюю связь по каналам запроса и ответа передачи данных между наземными радиолокационными станциями и воздушными объектами.

В работе проведена оценка относительной пропускной способности самолетных ответчиков вторичных радиолокационных систем наблюдения воздушного пространства при действии в канале запроса коррелированных и некоррелированных помех. Анализ пропускной способности самолетного ответчика показывает, что самолетный ответчик не достигает максимальной загрузки, заложенной в существующую систему идентификации при действии преднамеренных коррелированных помех. Это указывает на неоптимальное определение коэффициента загрузки самолетного ответчика существующей вторичной радиолокационной системы. Неправильное определение максимальной загрузки самолетного ответчика приводит к снижению помехоустойчивости как самолетного ответчика, так и всей вторичной радиолокационной системы. При этом следует отметить, что заинтересованная сторона имеет возможность несанкционированного использования самолетного ответчика для получения информации или парализации последнего при применении помех нужной интенсивности.

Ключевые слова: вторичная радиолокационная система; система наблюдения; воздушное пространство; самолетный ответчик; относительная пропускная способность; идентификация; сигнал запроса; сигнал ответа; помеха.

Ил. 3. Библиогр.: 38 назв.

UDC 621.396.96

Estimation of the relative throughput of aircraft transponders of secondary airspace surveillance radar systems / *M.G. Tkach* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №207. P. 123 – 131.

Secondary radar systems for monitoring airspace play a significant role in the information support of airspace control systems and air traffic control. These systems provide radar surveillance of airborne objects equipped with aircraft transponders and provide two-way communication via data request and response channels between ground radar stations and airborne objects.

The paper assesses the relative throughput of aircraft transponders of secondary radar systems for monitoring airspace under the influence of correlated and uncorrelated interference in the request channel. The assessment of the throughput of the aircraft transponder shows that the aircraft transponder does not reach the maximum load included in the existing identification system under the influence of deliberate correlated interference. This indicates a sub-optimal determination of the aircraft transponder load factor of the existing secondary radar system. Incorrect determination of the maximum load of the aircraft transponder leads to a decrease in the noise immunity of both the aircraft transponder and the entire secondary radar system. At the same time, it should be noted that the interested party has the possibility of unauthorized use of an aircraft transponder to obtain information or paralyze the latter when applying interference of the required intensity.

Key words: secondary radar system; surveillance system; air space; aircraft transponder; relative throughput; identification; request signal; response signal; interference.

3 fig. Ref: 38 items.

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

УДК 621.37: 004.056.5

Використання нестаціонарних шумових завад для протидії пасивним радіозакладкам / *С.П. Сергієнко, В.Г. Крижановський,, Д.В. Чернов, Л.В. Загоруйко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 207. С. 132– 138.

Використання шумових завад для протидії несанкціонованому зніманню інформації стало розповсюдженою практикою для захисту інформації. В останній час з'явилися публікації, в яких показано потенційну можливість використання шумових завад для знімання інформації пасивними радіопідслуховуючими пристроями. В особливості підвищується вразливість приміщень, які захищають від підслуховуючих пристроїв, якщо радіочастотне зашумлення включається в періоди часу, коли там ведуться конфіденційні перемовини. Використання енергії хвиль радіозашумлення для підслуховування робить такі пристрої непримітними для нелінійних радіолокаційних приладів пошуку радіопідслуховуючих пристроїв, якщо вони включаються тільки при дії шумових сигналів. В роботі показано, що використання нестаціонарного шуму дає можливість протидії несанкціонованому зніманню інформації. Аналіз ефективності нестаціонарного радіочастотного шуму проводився на моделі кореляційного приймача сигналу. Кореляційний приймач має найбільшу чутливість, і він більш ефективно працює з шумоподібними сигналами. В роботі показано, що для протидії несанкційного знімання інформації треба використовувати шум, амплітудно модульований випадковим сигналом, спектр якого співпадає зі спектром потенційного інформаційного сигналу. Накладання більш потужного модуляційного шуму на більш слабкий інформаційний сигнал робить неможливим передачу інформації. На прикладі зміни потужності монохроматичного сигналу при передачі радіозакладкой з використанням стационарного і нестаціонарного шумів показано, що завдяки параметричному перерозподілу енергії сигналу по спектру модуляції нестаціонарного шуму потужність монохроматичного сигналу зменшується більш ніж на 10 дБ порівняно з передачею такого ж сигналу стаціонарним шумом. На основі цих результатів можна зробити висновок, що використання для радіочастотного придушення нестаціонарних шумових сигналів робить неможливим використання сигналів радіочастотного придушення для роботи пасивних підслуховуючих пристроїв.

Ключові слова: пасивні радіопідслуховуючі пристрої; радіочастотне придушення; нестаціонарний шум; захист інформації.

Іл. 6. Бібліогр.: 15 назв.

УДК 621.37: 004.056.5

Использование нестационарных шумовых помех для противодействия пассивным радиозакладкам / *С.П. Сергиенко, В.Г. Крыжановский, Д.В. Чернов, Л.В. Загоруйко* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 207. С. 132 – 138.

Использование шумовых помех для противодействия несанкционированному съему информации стало распространенной практикой для защиты информации. В последнее время появились публикации, в которых показана потенциальная возможность использования шумовых помех для съема информации пассивными радиоподслушивающими устройствами. Особенно повышается уязвимость помещений, защищаемых от подслушивающих устройств, если радиочастотное зашумление включается в периоды времени, когда там ведутся конфиденциальные переговоры. Использование энергии волн радиозашумления для подслушивания делает такие устройства незаметными для нелинейных радиолокационных приборов поиска радиоподслушивающих устройств, если они включаются только при воздействии шумовых сигналов. В работе показано, что использование нестационарного шума создает возможность противодействию несанкционированному съему информации. Анализ эффективности нестационарного радиочастотного шума проводился на модели корреляционного приемника сигнала. Корреляционный приемник имеет наибольшую чувствительность, и он более эффективно работает с шумоподобными сигналами. В работе показано, что для противодействия несанкционированного съема информации надо использовать шум, амплитудно-модулированный случайным сигналом, спектр которого совпадает со спектром потенциального информационного сигнала. Наложение более мощного модуляционного шума на более слабый информационный сигнал делает невозможным передачу информации. На примере изменения мощности монохроматического сигнала при передаче радиозакладкой с использованием стационарного и нестационарного шумов показано, что благодаря параметрическому перераспределению энергии сигнала по спектру модуляции нестационарного шума, мощность монохроматического сигнала уменьшается более чем на 10 дБ по сравнению с передачей такого же сигнала стационарным шумом. На основе этих результатов можно сделать вывод, что использование для радиочастотного подавления нестационарными шумовыми сигналами делает невозможным использование сигналов радиочастотного подавления для работы пассивных подслушивающих устройств.

Ключевые слова: пассивные радиоподслушивающие устройства; радиочастотное подавления; нестационарный шум; защита информации.

Ил. 6. Библиогр.: 15 назв.

UDC 621.37: 004.056.5

The use of non-steady state noise interferences to counteract passive eavesdropping devices / *S.P. Serhiienko, V.G. Krizhanovski, D.V. Chernov, L.V. Zagoruiko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №207. P. 132 – 138.

The use of noise interference has become a common practice for information security. Recently appeared publications showing a potential possibility to use the noise radio frequency interference for information skimming by passive radio eavesdropping device. In particular, the vulnerability of the premises protected from eavesdropping devices is increased, if the radio frequency noising is switched on when confidential negotiations are being conducted. The use of radio noise waves energy for eavesdropping makes such devices invisible to nonlinear locators for listening devices if they activated only by noise signals. The paper shows that the use of non-steady state noise allows counteracting the unauthorized pickup of information. The analysis of non-steady state radio frequency noise effectiveness was carried out using the correlation receiver model. The correlation receiver has the highest sensitivity, and it works more efficiently with noise-like signals. It is shown that for counteracting the information pickup, it is necessary to use a noise, amplitude modulated by a random signal, whose spectrum coincides with a spectrum of a potential informational signal. Imposition a more powerful modulation noise to a weak informational signal makes impossible the information transfer. It is shown on the example of changing the power of a monochromatic signal while "beetle" transmits using steady-state and non-steady state noises, that due to the signal energy parametric redistribution over the non-steady-state noise modulation spectrum, the power of monochromatic signal is reduced by more than 10 dB compared to the transmission of the same signal using a steady-state noise. It can be concluded that the use of non-steady state noise signals for radio frequency suppression makes impossible their use for passive eavesdropping devices operation.

Key words: passive radio eavesdropping devices; radio-frequency suppression; non-steady state noise; information protection.

6 fig. Ref: 15 items.

УДК 621.369:534

Дослідження можливостей використання клавіатурного почерку для задач ідентифікації студентів у системах дистанційної освіти / *Д.Ю. Горєлов, О.О. Іванова, О.В Литвиненко, А.А. Довбня, Д.О. Мінін* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 207. С. 139 – 148.

В процесі використання систем дистанційної освіти виникає проблема інформаційної безпеки навчального процесу, яка, крім зовнішніх, містить також внутрішні загрози. Однією з таких загроз може стати легальний користувач, який заплатив шахраю за складання тестів та видимість навчальної діяльності під своїм ім'ям. Використання традиційних методів ідентифікації має два істотних недоліки: по-перше, неоднозначність користувача, який ідентифікується, оскільки в даному випадку встановлення особи користувача відбувається за введеною парольною фразою; по-друге, відсутність можливості виявлення підміни ідентифікованого користувача в процесі роботи з системою. Зазначені недоліки усуваються при використанні біометричних методів скритного та неперервного моніторингу.

У першій частині роботи проаналізовано типи тестових завдань. З урахуванням специфіки використання алгоритмів скритного клавіатурного моніторингу запропоновано: 1) використовувати тести, що не містять варіантів відповідей; 2) використовувати тести при поточному контролі знань з метою формування біометричного еталона користувача; 3) використовувати тести з числовими відповідями з метою мінімізації аналізованих дифрафів клавіатури.

У другій частині роботи запропоновано алгоритм формування профілю користувача та його ідентифікації, що поєднує якісний (розподіл частот використання груп цифрових клавіш, клавіш-розділювачів цілої та дробової частини, знаків «плюс» та «мінус» на основній та додатковій клавіатурах) та кількісний (аналіз статистичних властивостей диграфів) підходи. Експериментально отримані оцінки точності ідентифікації запропонованого алгоритму склали: FAR=4,64 % та FRR=6,25 %.

Ключові слова: інформаційна безпека систем дистанційної освіти; ідентифікація; клавіатурний почерк; диграф клавіатури; багатофакторна класифікація.

Табл. 2. Іл. 4. Бібліогр.: 16 назв.

УДК 621.369:534

Исследование возможностей использования клавиатурного почерка для задач идентификации студентов в системах дистанционного образования / *Д.Ю. Горелов, Е.А. Иванова, А.В Литвиненко, А.А. Довбня, Д.А. Минин* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 207. С. 139 – 148.

При использовании систем дистанционного образования возникает проблема информационной безопасности учебного процесса, которая, кроме внешних, подразумевает также и внутренние угрозы. Одной из таких угроз может стать легальный пользователь, который заплатил мошеннику за сдачу тестов и видимость учебной деятельности под своим именем. Использование традиционных методов идентификации имеет два существенных недостатка: во-первых, неоднозначность идентифицируемого пользователя, поскольку в данном случае установление личности пользователя происходит по введенной парольной фразе; во-вторых, отсутствие возможности обнаружения подмены идентифицированного пользователя в процессе работы с системой. Указанные недостатки устраняются при использовании биометрических методов скрытного и непрерывного мониторинга.

В первой части работы проанализированы типы тестовых заданий. С учетом специфики использования алгоритмов скрытного клавиатурного мониторинга предложено: 1) использовать тесты, не содержащие вариантов ответов; 2) использовать тесты при текущем контроле знаний с целью формирования биометрического эталона пользователя; 3) использовать тесты с численными ответами с целью минимизации анализируемых диграфов клавиатуры.

Во второй части работы предложен алгоритм формирования профиля пользователя и его идентификации, сочетающий качественный (распределение частот использования групп цифровых клавиш, клавиш-разделителей целой и дробной части, знаков «плюс» и «минус» на основной и дополнительной клавиатурах) и количественный (учет статистических свойств диграфов) подходы. Экспериментально полученные оценки точности идентификации предложенного алгоритма составили: FAR=4,64 % и FRR=6,25 %.

Ключевые слова: информационная безопасность систем дистанционного обучения; идентификация; клавиатурный почерк; диграф клавиатуры; многофакторная классификация.

Табл. 2. Ил. 4. Библиогр.: 16 назв.

UDC 621.369:534

Study of the possibilities to use keyboard handwriting for the tasks of identifying students in e-learning systems / *D.Y. Gorelov, O.O. Ivanova, O.V. Lytvynenko, A.A. Dovbnia, D.O. Minin* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №207. P. 139 – 148.

When using distance education systems, the problem of information security of the educational process arises, which, in addition to external ones, also implies internal threats. One of these threats can be a legitimate user who paid a fraudster to take tests and give visibility to educational activities under his own name. The use of traditional identification methods has two significant drawbacks: firstly, the ambiguity of the identified user, because the identification of the user occurs by the entered pair login-password; secondly, the inability to detect the substitution of an identified user in the process of working with the system. These disadvantages are eliminated by using biometric methods of covert and continuous monitoring.

In the first part of the work the different types of control knowledge tests are analyzed. Taking into account the specifics of the use of covert keyboard monitoring algorithms, the following is proposed: 1) to use tests that do not contain answers; 2) use tests after each learning activities in order to form a user's biometric vector; 3) use tests with numerical answers in order to minimize the analyzed keystroke digraphs.

An algorithm for user's profile formation and its identification is proposed in the second part of the work. Its combine qualitative (distribution of the frequencies of using numeric keys groups, comma-separated keys, "plus" and "minus" keys on the main and additional keyboard units) and quantitative (analysis of statistical properties of keystroke digraphs) approaches. The experimentally obtained estimates of the identification accuracy of the proposed algorithm: FAR=4.64% and FRR=6.25%.

Key words: information security of e-learning; authentication; keystroke; keystroke digraph; multi-factor classification.

2 tab. 4 fig. Ref: 16 items.

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

УДК 537.868

Вплив феримагнітного резонансу на перетворення енергії електромагнітної хвилі ЗІГ-резонатором в механічну енергію / *Г.Л. Комарова* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 207. С. 149 – 158.

Методом фізичного моделювання отриманий алгоритм обчислення сили, з якою стояча електромагнітна хвиля діє на феритову сферу довільного радіуса, розміщену в постійному магнітному полі. Величина напруженості постійного магнітного поля відповідає виникненню феримагнітного резонансу. Досліджено залежність магнітного поля електромагнітної хвилі в середині феритової сфери від розміру її резонансного радіусу і сферичних координат. У центрі феритової сфери, резонансний радіус якої дорівнює 4,2634 мм, напруженість магнітного поля НВЧ в 83796 разів більше в порівнянні з напруженістю магнітного поля в падаючій плоско поляризованій хвилі. Середнє квадратичне значення напруженості магнітного поля за обсягом кулі збільшується в 4,8 раз. Стояча електромагнітна хвиля, створена падаючою у вільному просторі з щільністю потоку потужності 622 кВт/м^2 і довжиною 3,2 см і відбитої від металевого екрана, розташованого від центру феритової сфери на відстані, рівній ($\lambda_o/8 + n \cdot \lambda_o/2$, де n = 0, 1, 2, 3 ...), діє на резонатор з силою, рівною 0,12 Н. Резонансний радіус феритової сфери дорівнює 4,2634 мм. Результати обчислень сили, діючої на ЗІГ-резонатор, збігаються з експериментальними результатами, наведеними в відомих роботах (щільність потоку потужності дорівнює 43 кВт / м2, радіус феритової сфери дорівнює 1,775 мм, сила дорівнює 6 ± 0,5 мкН) в межах похибки вимірювання. Застосування феримагнітного резонансу стоячої електромагнітної хвилі та ЗІГ-резонатора дозволило збільшити коефіцієнт перетворення енергії СВЧ в механічну в 8,6·10^4 разів у порівнянні з використанням фери-

тового циліндра в відомих роботах. Отримані результати можуть бути використані розробниками перетворювачів НВЧ енергії в механічну енергію.

Ключові слова: електромагнітна енергія; феримагнітний резонанс; перетворення; механічна енергія; ЗІГ-резонатор.

Табл. 1. Іл. 4. Бібліогр.: 14 назв.

УДК 537.868

Влияние ферримагнитного резонанса на преобразование энергии электромагнитной волны ЖИГ-резонатором в механическую энергию / *Г.Л. Комарова* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 207. С. 149 – 158.

Методом физического моделирования получен алгоритм вычисления силы, с которой стоячая электромагнитная волна действует на ферритовую сферу произвольного диаметра, помещенную в постоянное магнитное поле. Величина напряженности постоянного магнитного поля соответствует возникновению ферримагнитного резонанса. Исследованы зависимости магнитного поля электромагнитной волны в середине ферритовой сферы от размера ее резонансного радиуса и сферических координат. В центре ферритовой сферы, резонансный радиус которой равен 4,2634 мм, напряженности магнитного поля СВЧ в 83796 раз больше по сравнению с напряженностью магнитного поля в падающей плоскополяризованной волне. Среднее квадратичное значение напряженности магнитного поля по объему сферы увеличивается в 4,8 раз. Стоячая электромагнитная волна, созданная распространяющейся в свободном пространстве с плотностью потока мощности 622 кВт/м^2 и длиной 3,2 см и отраженной от металлического экрана, расположенного от центра ферритовой сферы на расстоянии, равном ($\lambda_o/8 + n\cdot\lambda_o/2$, где n = 0, 1, 2, 3…), действует на резонатор, с силой равной 0,12 Н. Резонансный радиус ферритовой сферы равен 4,2634 мм. Результаты вычисленный силы, действующей на ЖИГ-резонатор, совпадают с экспериментальными результатами, приведенными в известных работах (плотность потока мощности равна 43 кВт/м^2, радиус ферритовой сферы равен 1,775 мм, сила равна 6 ± 0,5 мкН) в пределах погрешности измерения. Применение ферримагнитного резонанса, стоячей электромагнитной волны и ЖИГ-резонатора позволило увеличить коэффициент преобразования энергии СВЧ в механическую энергию в $8{,}6\cdot10^4$ раз по сравнению с использованием ферримагнитного цилиндра в известных работах. Результаты исследований могут быть использованы разработчиками преобразователей СВЧ энергии в механическую энергию.

Ключевые слова: электромагнитная энергия; ферримагнитный резонанс; преобразование; механическая энергия; ЖИГ-резонатор.

Табл. 1. Ил. 4. Библиогр.: 14 назв.

UDC 537.868

Influence of ferrimagnetic resonance on conversion of electromagnetic energy by a YIG resonator into mechanical one / *G.L. Komarova* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №207. P. 149 – 158.

Using the method of physical modeling, an algorithm for calculating the force with which a standing electromagnetic wave acts on a ferrite sphere of arbitrary diameter placed in a constant magnetic field is obtained. The value of constant magnetic field intensity provides appearance of ferrimagnetic resonance. Dependence of the magnetic field of an electromagnetic wave in the middle of a ferrite sphere on the size of its resonant radius and spherical coordinates are studied. In the center of the ferrite sphere, the resonance radius of which is 4.2634 mm, the microwave magnetic field strength is 83796 times greater than the magnetic field strength in the incident plane polarized wave. Mean-square value of the magnetic field strength over the volume of the sphere increases 4.8 times. Standing wave, formed in a free space with power flow density of 622 kW/m^2 and wavelength of 3.2 cm, reflects from metallic shield placed at a distance of $\lambda_o/8 + n\lambda_o/2$, n = 0, 1, 2, 3… measured from the center of ferrite sphere and impacts with force of 0,12 N on ferrite sphere with resonance radius of 4,2634 mm. The results of the calculated force acting on the YIG – resonator coincide with the experimental results given in the well-known works (the power flux density is 43 kW/m^2, the radius of the ferrite sphere is 1.775 mm, the force is 6 ± 0.5 μN) within the measurement error. Application of spatial resonance, standing electromagnetic wave and YIG resonator allows to increase of energy conversion factor of microwave energy conversion into mechanic one $8{,}6\cdot10^4$ times in compare to application of ferrite cylinder only in known papers. The research results can be used by the developers of converters of microwave energy into mechanical energy.

Key words: electromagnetic energy; ferrimagnetic resonance; transformation; mechanical energy; YIG resonator.

1 tab. 4 fig. Ref: 14 items.

ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНІ ТЕХНОЛОГІЇ
ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНЫЕ ТЕХНОЛОГИИ
INFORMATION AND MEASURING TECHNOLOGIES

УДК 004.45:004.057.02

Модель якості програмного забезпечення на основі стандартів SQuaRE / *Н.В. Штефан, О.В. Запорожець* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 207. С. 159 – 165.

Якість є одним із факторів, що забезпечують комерційний успіх та безпеку використання програмного забезпечення. Під якістю розуміють відповідність явним і неявним вимогам різних зацікавлених сторін. Необхідно забезпечити спільне взаєморозуміння між розробниками та користувачами, інженери повинні розуміти зна-

чення поняття якості, характеристики та важливість якості для розробленого або підтримуваного програмного забезпечення. Основою забезпечення якості є вимірювання. Воно є основним інструментом керування життєвим циклом програмних продуктів, оцінки виконання планів і моніторингу. Для кількісного визначення якості необхідно виміряти характеристики програмного забезпечення. Стандартизація передбачає уніфікацію вимог до якості, її вимірювання та оцінки. Використання стандартів дає безліч потенційних переваг для будь-якої організації, особливо у таких ключових областях, як вимірювання якості програмних продуктів, інформаційних та вимірювальних систем. Визнані міжнародні організації із стандартизації опублікували серію стандартів ISO/IEC 25000 щодо вимог та оцінки якості систем та програмного забезпечення SQuaRE, які набувають широкого практичного застосування. У статті обговорюється серія міжнародних стандартів SQuaRE, аналізується взаємозв'язок між моделлю якості, характеристиками якості, показниками якості та новою концепцією – елементом показника якості програмного забезпечення, представлено вимірювання якості на основі цих стандартів.

Ключові слова: якість; модель якості; програмне забезпечення; вимірювання; стандарт; показник якості.

Табл. 1. Іл. 5. Бібліогр.: 10 назв.

УДК 004.45:004.057.02

Модель качества программного обеспечения на основе стандартов SQuaRE / *Н.В. Штефан, О.В. Запорожец* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 207. С. 159 – 165.

Качество – один из основных факторов, обеспечивающих коммерческий успех и безопасность использования программного обеспечения. Качество понимается как соответствие явным и неявным требованиям различных заинтересованных сторон. Необходимо обеспечить совместное понимание между разработчиками и пользователями, инженеры должны понимать смысл, вкладываемый в концепцию качества, характеристики и значение качества в отношении разрабатываемого или сопровождаемого программного обеспечения. Основой обеспечения качества являются измерения. Они – основной инструмент управления жизненным циклом программных продуктов, оценки выполнения планов и мониторинга. Для количественного определения качества необходимо измерить характеристики программного обеспечения. Стандартизация обеспечивает унификацию требований к качеству, его измерению и оценке. Использование стандартов дает множество потенциальных преимуществ для любой организации, особенно в таких ключевых областях, как измерение качества программных продуктов, информационных и измерительных систем. Признанные международные организации по стандартизации опубликовали серию стандартов ISO/IEC 25000 по требованиям и оценке качества систем и программного обеспечения SQuaRE, которые получает все более широкое практическое применение. В статье рассмотрена серия международных стандартов SQuaRE, проанализировано отношение между моделью качества, характеристиками качества, показателями качества и новым понятием – элемент показателя качества программного обеспечения, представлено измерение качества на основе этих стандартов.

Ключевые слова: качество; модель качества; программное обеспечение; измерение; стандарт; показатель качества.

Табл. 1. Ил. 5. Библиогр.: 10 назв.

UDC 004.45:004.057.02

Software quality model based on SQuaRE standards / *N. Shtefan, O. Zaporozhets* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №207. P. 159 – 165.

Quality is one of the factors that ensure the commercial success and safety of using the software. Quality is understood as conformity the explicit and implicit requirements of various stakeholders. It is necessary to ensure a joint understanding between developers and users, engineers need to understand the meaning of the concept of quality, characteristics and importance of quality for the developed or maintained software. Measurements are the basis for quality assurance. They are the main tool for managing the life cycle of software products, assessing the implementation of plans and monitoring. To quantify quality, it is necessary to measure the characteristics of the software. Standardization provides unification of requirements for quality, its measurement and assessment. The use of standards has many potential benefits for any organization, especially in key areas such as measuring the quality of software products, information and measurement systems. Recognized international standards organizations have published the ISO/IEC 25000 series of standards for systems and software quality requirements and evaluation SQuaRE, which is gaining widespread practical application. The paper discusses a series of international standards SQuaRE, analyzes the relationship between the quality model, quality characteristics, quality measures and a new concept – a quality measure element of the software, presents the measurement of quality based on these standards.

Key words: quality; quality model; software; measurement; standard; quality measure.

1 tab. 5 fig. Ref: 10 items.

СУМІЖНІ ПРОБЛЕМИ РАДІОТЕХНІКИ
СМЕЖНЫЕ ПРОБЛЕМЫ РАДИОТЕХНИКИ
RELATED PROBLEMS OF RADIO ENGINEERING

УДК 537.226.3

Оперативний контроль параметрів рідких паливомастильних матеріалів з домішками / *Б.В. Жуков, С.І. Борбулєв, А.В. Одновол* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 207. С. 166 – 171.

Розглянуто можливості оперативного контролю параметрів рідких пально-мастильних матеріалів (ПММ) з домішками за допомогою резонаторного методу НВЧ діелектрометрії. Попередні дослідження рідких ПММ (бензини, дизельні палива, гаси, олії) показали, що величини дійсної та уявної складових комплексної діелектричної проникності перерахованих ПММ знаходяться в робочому діапазоні резонаторного НВЧ діелектрометра.

Висока роздільна здатність НВЧ резонаторного методу визначає перспективність використання даного методу для аналізу комплексної діелектричної проникності сумішей ПММ з різними домішками, включаючи воду, спирти, бензол та ін.

Для суміші бензину з бензолом експериментально встановлено, що при невеликій добавці бензолу (не більше 15 %) спостерігається зростання дійсної складової комплексної діелектричної проникності суміші, а при вмісті бензолу, що перевищує 15 %, має місце зростання обох складових комплексної діелектричної проникності суміші.

У процесі досліджень також було встановлено, що НВЧ діелектрометр забезпечив можливість ідентифікувати в реальному часі зразки трансформаторної олії за наявності води в кількості 14, 28 і 56 грам на тонну масла. Результати досліджень свідчать, що метод НВЧ діелектрометрії може вважатися перспективним для контролю якості трансформаторного масла як у процесі заливання, так і для контролю якості в процесі експлуатації високовольтних трансформаторів.

Результати початкового етапу досліджень спиртових бензинів поки що не дозволили виявити переважний вплив спиртової добавки на розташування експериментальних точок на комплексній площині. Ця обставина, найімовірніше, пов'язана з тим, що спиртові бензини з близьким октановим числом можуть мати хімічний склад, що істотно відрізняється.

Ключові слова: комплексна діелектрична проникність; НВЧ резонаторний метод; спиртовий бензин; масло трансформаторне; бензол; комплексна площина; октанове число.

Іл. 3. Бібліогр.: 17 назв.

УДК 537.226.3

Оперативный контроль параметров жидких горючесмазочных материалов с примесями / *Б.В. Жуков, С.И. Борбулев, А.В. Одновол* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 207. С. 166 – 171.

Рассмотрены возможности оперативного контроля параметров жидких горючесмазочных материалов (ГСМ) с примесями с помощью резонаторного метода СВЧ диэлектрометрии. Предварительные исследования жидких ГСМ (бензины, дизельные топлива, керосины, масла) показали, что величины действительной и мнимой составляющих комплексной диэлектрической проницаемости перечисленных ГСМ находятся в рабочем диапазоне резонаторного СВЧ диэлектрометра.

Высокая разрешающая способность СВЧ резонаторного метода определяет перспективность использования данного метода для анализа комплексной диэлектрической проницаемости смесей ГСМ с различными примесями, включая воду, спирты, бензол и др.

Для смеси бензина с бензолом экспериментально установлено, что при небольшой добавке бензола (не более 15 %) наблюдается возрастание действительной составляющей комплексной диэлектрической проницаемости смеси, а при содержании бензола, превышающем 15 %, имеет место возрастание обеих составляющих комплексной диэлектрической проницаемости смеси.

В процессе исследований также было установлено, что СВЧ диэлектрометр обеспечил возможность идентифицировать в реальном времени образцы трансформаторного масла при наличии в них воды в количестве 14, 28 и 56 грамм на тонну масла. Результаты исследований свидетельствуют, что метод СВЧ диэлектрометрии может считаться перспективным для контроля качества трансформаторного масла как в процессе заливки, так и для контроля его качества в процессе эксплуатации высоковольтных трансформаторов.

Результаты начального этапа исследований спиртовых бензинов пока не позволили выявить преобладающее влияние спиртовой добавки на расположение экспериментальных точек на комплексной плоскости. Данное обстоятельство, вероятно, связано с тем, что спиртовые бензины с близким октановым числом могут иметь существенно отличающийся химический состав.

Ключевые слова: комплексная диэлектрическая проницаемость; СВЧ резонаторный метод; спиртовой бензин; масло трансформаторное; бензол; комплексная плоскость; октановое число.

Ил. 3. Библиогр.: 17 назв.

UDC 537.226.3

Operational control of the parameters of liquid fuels and lubricants with impurities / *B.V. Zhukov, S.I. Borbulev, A.V. Odnovol* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №207. P. 166 – 171.

The possibilities of operational control of the parameters of liquid fuels and lubricants with impurities using the resonator method of microwave dielectrometry are considered. Preliminary studies of liquid fuels and lubricants (gasolines, diesel fuels, kerosene, oils) showed that the values of the real and imaginary components of the complex dielectric constant of the listed fuels and lubricants are in the operating range of the resonator microwave dielectrometer.

The high resolution of the microwave resonator method determines the prospects of using this method for analyzing the complex dielectric constant of mixtures of fuels and lubricants with various impurities, including water, alcohols, benzene, etc.

For a mixture of gasoline with benzene, it was experimentally established that with a small addition of benzene (no more than 15%), an increase in the real component of the complex dielectric constant of the mixture is observed, and with a benzene content exceeding 15%, an increase in both components of the complex dielectric constant of the mixture takes place.

The process has also been installed, but the NHF dielectrometer has made it possible to identify the transformer in real time due to the presence of water in the amount of 14, 28 and 56 grams per ton of oil. The research results indicate that the microwave dielectrometry method can be considered promising for monitoring the quality of transformer oil both during the filling process and for monitoring its quality during the operation of high-voltage transformers.

The results of the initial stage of research on alcohol gasolines have not yet revealed the predominant effect of the alcohol additive on the location of the experimental points on the complex plane. This circumstance is most likely due to the fact that alcohol gasolines with a close octane number can have a significantly different chemical composition.

Key words: complex dielectric constant; microwave resonator method; alcohol gasoline; transformer oil; benzene; complex plane; octane number.

3 fig. Ref: 17 items.

ЗБІРНИК НАУКОВИХ ПРАЦЬ
РАДІОТЕХНІКА
Випуск 207
Українською, російською, та англійською мовами

СБОРНИК НАУЧНЫХ ТРУДОВ
РАДИОТЕХНИКА
Выпуск 207
На украинском, русском и английском языках

COLLECTION OF SCIENTIFIC PAPERS
RADIOTEKHNIKA
Issue 207
In Ukrainian, Russian and English

Коректор Л.І. Сащенко

Підп. до друку 24.12.2021. Формат 60x90/8. Папір офсет. Гарнітура Таймс. Друк. ризограф.
Ум. друк. арк**.** 10,5. Обл.-вид. арк. 10,68. Тираж 300 прим. Зам. № 493. 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.