MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE

KHARKIV NATIONAL
UNIVERSITY OF RADIO ELECTRONICS

RADIOTEKHNIKA

All-Ukrainian
interdepartmental scientific and technical collection

ISSN 0485-8972
eISSN 2786-5525

Founded in 1965

I S S U E 2 0 9

Kharkiv
Kharkiv National
University of Radio Electronics
2022

UDC 621.3

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

Website: rt.nure.ua

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

The authors are responsible for the content of the article.

Editorial Team

I.V. Svyd, *PhD, Assoc. prof.*, NURE, Ukraine (Chief Editor)
O.G. Avrunin, *Dr. Sc. (Tech.), prof.*, NURE, Ukraine
D.V. Ageiev, *Dr. Sc. (Tech.), prof.*, NURE, Ukraine
V.M Bezruk., *Dr. Sc. (Tech.), prof.*, NURE, Ukraine
I.M. Bondarenko, *Dr. Sc. (Phys.-Math.), prof.*, NURE, Ukraine
I.D. Gorbenko, *Dr. Sc. (Tech.), prof.*, KhNU V. N. Karazin, Ukraine
D.V. Gretskih , *Dr. Sc. (Tech.), Assoc. prof.*, NURE, Ukraine
K.Yu. Dergachov, PhD, Senior Researcher, Sciences, prof., NAU «KhAI», Ukraine
V.O. Doroshenko, *Dr. Sc. (Phys.-Math.)*, prof., NURE, Ukraine
I.P. Zakharov, *Dr. Sc. (Tech.)*, prof., NURE, Ukraine
V.M. Kartashov, *Dr. Sc. (Tech.)*, prof., NURE, Ukraine
O.O. Konovalenko, *Dr. Sc. (Phys.-Math.)*, prof., Academician of NASU, IRA NASU, Ukraine
A.S. Kulik, *Dr. Sc. (Tech.)*, prof., NAU «KhAI», Ukraine
L.M. Lytvynenko, *Dr. Sc. (Phys.-Math.)*, prof., Academician of NASU, IRA NASU, Ukraine
A.I. Luchaninov, *Dr. Sc. (Phys.-Math.)*, prof., NURE, Ukraine
K.M. Muzyka, *Dr. Sc. (Tech.)*, Senior Researcher, NURE, Ukraine
E.M. Odarenko, *Dr. Sc. (Tech.)*, prof., NURE, Ukraine
O.G. Pashchenko, PhD, Assoc. prof., NURE, Ukraine
V.V. Semenets, *Dr. Sc. (Tech.)*, prof., NURE, Ukraine
S.I. Tarapov, *Dr. Sc. (Phys.-Math.)*, prof., member-cor. NASU, IRE NASU, Ukraine
V.M. Tkachov, *PhD, Assoc. prof.*, NURE, Ukraine
P.L. Tokarsky, *Dr. Sc. (Phys.-Math.)*, prof., IRA NASU, Ukraine
O.I. Filipenko, *Dr. Sc. (Tech.)*, prof., NURE, Ukraine
H.Z. Khalimov, *Dr. Sc. (Tech.)*, prof., NURE, Ukraine
O.M. Tsymbal, *Dr. Sc. (Tech.)*, Assoc. prof., NURE, Ukraine
O.I. Tsopa, *Dr. Sc. (Tech.)*, prof., NURE, Ukraine

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

Boris Chichkov (*Germany*), Marianna Ivashina (*Sweden*), Konstyantyn Markov (*Germany*), Georgiy Sevskiy (*Germany*), Larysa Titarenko (*Poland*), Vitaliy Zhurbenko (*Denmark*)

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

Recommended by the Scientific and Technical Council of Kharkiv National University of Radio Electronics, protocol № 5 dated 24.06.2022.

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

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

The use of materials is possible only with the consent of the editorial board.

© Kharkiv National University of Radio Electronics, 2022.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ
УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ

РАДІОТЕХНІКА

Всеукраїнський
міжвідомчий науково-технічний збірник

ISSN 0485-8972
eISSN 2786-5525

Засновано в 1965 р.

В И П У С К 2 0 9

Харків
Харківський національний
університет радіоелектроніки
2022

УДК 621.3

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

Сайт: rt.nure.ua

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

За зміст статті відповідальні автори.

Редакційна колегія

І.В. Свид, *к.т.н., доц.,* ХНУРЕ*, Україна (головний редактор)*
О.Г. Аврунін, *д.т.н., проф., ХНУРЕ, Україна*
Д.В. Агеєв, *д.т.н., проф., ХНУРЕ, Україна*
В.М. Безрук*, д.т.н., проф., ХНУРЕ, Україна*
І.М. Бондаренко, *д.ф.-м.н., проф., ХНУРЕ, Україна*
І.Д. Горбенко, *д.т.н., проф., ХНУ ім. В.Н. Каразіна, Україна*
Д.В. Грецьких, *д.т.н., доц., ХНУРЕ, Україна*
К.Ю. Дергачов, *к.т.н., с.н.с., НАУ ім. М.Є. Жуковського «ХАІ», Україна*
В.О. Дорошенко, *д.ф.-м.н., проф., ХНУРЕ, Україна*
І.П. Захаров, *д.т.н., проф., ХНУРЕ, Україна*
В.М. Карташов, *д.т.н., проф., ХНУРЕ, Україна*
А.А. Коноваленко, *д.ф.-м.н., академік НАНУ, РІАН, Україна*
А.С. Кулік, *д.т.н., проф., НАУ ім. М.Є. Жуковського «ХАІ», Україна*
Л.М. Литвиненко, *д.ф.-м.н., академік НАНУ, РІАН, Україна*
А.І. Лучанінов, *д.ф.-м.н., проф., ХНУРЕ, Україна*
К.М. Музика, *д.т.н., с.н.с., ХНУРЕ, Україна*
Є.М. Одаренко, *д.т.н., проф., ХНУРЕ, Україна*
О.Г. Пащенко, *к.ф.-м.н., доц., ХНУРЕ, Україна*
В.В. Семенець, *д.т.н., проф., ХНУРЕ, Україна*
С.І. Тарапов, *д.ф.-м.н., проф., член-кор. НАНУ, ІРЕ НАНУ, Україна*
В.М. Ткачов, *к.т.н., доц., ХНУРЕ, Україна*
П.Л. Токарський, *д.ф.-м.н., проф., РІАН, Україна*
О.І. Филипенко, *д.т.н., проф., ХНУРЕ, Україна*
Г.З. Халімов, *д.т.н., проф., ХНУРЕ, Україна*
О.М. Цимбал, *д.т.н., доц., ХНУРЕ, Україна*
О.І. Цопа, *д.т.н., проф., ХНУРЕ, Україна*

Міжнародна редакційна колегія

Boris Chichkov (*Німеччина*), Marianna Ivashina (*Швеція*), Konstyantyn Markov (*Німеччина*), Georgiy Sevskiy (*Німеччина*), Larysa Titarenko (*Польща*), Vitaliy Zhurbenko (*Данія*)

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

Рекомендовано Науково-технічною радою Харківського національного університету радіоелектроніки, протокол № 5 від 24.06.2022.

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**.

Використання матеріалів можливе лише за згодою редколегії.

© Харківський національний університет радіоелектроніки, 2022.

CONTENT

METHODS, ALGORITHMS AND TOOLS FOR CRYPTOGRAPHIC PROTECTION OF INFORMATION

M.V. Yesina, O.V. Potii, Yu.I. Gorbenko, V.A. Ponomar Risk estimation methodology in the post-quantum period 7

O.O. Kuznetsov, Yu.I. Горбенко, M.O. Poluyanenko, S.O. Kandiy, E.D. Matveeva Properties of the cost function in the iterative algorithm for generating nonlinear substitutions 16

I.D. Gorbenko, C.O. Kandiy, Ye.V. Ostrianska Comparison of the quality of sampling algorithms from discrete normal distribution on NTRU lattices 29

Я.А. Дерев'янко, Yu.I. Gorbenko, O.O. Kuznetsov Factorial number system for nonlinear substitutions generation 38

D.V. Harmash RAINBOW algorithm and its ability to resist RBS attacks and third party channels 59

G. Maleeva Analysis of partial key recovery attack on multivariate cryptographic transformations using rank systems 64

O.O. Kuznetsov, , M.O. Poluyanenko, S.O. Kandiy, O.I. Peliukh Study of a new cost function for generating random substitutions of symmetric ciphers 71

O.G. Kachko, M.V. Yesina, K.O. Kuznetsova Analysis of methods and algorithms for generating key data for FALCON-like electronic signature algorithms 83

Ye.Yu. Kaptiol Analysis of the RAINBOW post-quantum electronic signature algorithm state and attacks on it for the period of the NIST PQC third round completion 87

O.O. Kuznetsov, M.O. Poluyanenko, S.O. Kandiy, Y.O. Lohachova Substantiation of the parameters of the annealing simulation algorithm for searching non-linear substitutions of symmetric ciphers 93

INFORMATION PROTECTION METHODS IN TELECOMMUNICATION SYSTEMS

O.V. Sievierinov, V.M. Fedorchenko, R.Y. Gvozdov, V.O. Poddubnyi Object-oriented model of a formal description of an information and communication system 110

I. Gorbenko, O. Zamula, *Yu. Osipenko* The concept of assessing the risks of cybersecurity of the information system of the critical infrastructure object 118

V.I. Yukhymenko, O.I. Fediushyn Scaling analysis of the Telegram Open Network blockchain project 130

V.I. Yesin, V.V. Vilihura Research on the main methods and schemes of encryption with search capability 138

A.N. Oleynikov, V.A. Pulavsky, I.N. Chigirev Improving the efficiency of methods and means for suppressing unauthorized speech recording 156

RADIOLOCATION AND RADIONAVIGATION

I.V. Svyd, V.V. Semenets, O.S. Maltsev, M.G. Tkach, S.V. Starokozhev, O.O. Datsenko, I.O. Shevtsov Comparative analysis of methods for determining the air objects' coordinates using wide-area multilateration systems 162

ELECTRODYNAMICS, RADIO WAVES PROPAGATION

A.I. Kovalenko, S.V. Titov, E.V. Titova, O.S. Cherna Estimation of requirements to signal parameters at V-shaped frequency distribution in mathematical model of multi-position transmitter system 178

AUTOMATION AND COMPUTER INTEGRATED TECHNOLOGIES

I.Sh. Nevliudov, S.P. Novoselov, O.V. Sychova, S.I. Tesliuk Equipment for studies of semiconductor temperature resistance dependence 185

BIOMEDICAL RADIO ELECTRONICS

I. Prasol, O. Yeroshenko Modeling the electrical stimulation intensity dependence on stimulus frequency 192

N.V. Khmil, V.G. Kolesnikov, O.L. Altuhov Evaluation of disorders of adaptive mechanisms in heart failure by microwave dielectrometry 200

RELATED PROBLEMS OF RADIO ENGINEERING

I. Razumov-Fryziuk, D. Gurin, D. Nikitin, R. Strilets, D. Blyzniuk Modeling a screw extruder for FFF 3D printing 206

Yu.Ye. Khoroshailo, N.Ya. Zaichenko, O.B. Zaichenko Improvement of spectroscopic method for determining refractive index of filament sample material for 3D printing in terahertz range 215

O.V. Vovk, I.B. Chebotarova, D.V. Polenok Study of color reproduction features at "Nargus" LLC 226

V.A. Tikhonov, V.M. Kartashov, O.V. Kartashov Model for estimating statistical characteristics of the pre-stroke warehouse process based on average monthly temperatures analysis 239

ABSTRACTS 246

ЗМІСТ

МЕТОДИ, АЛГОРИТМИ ТА ЗАСОБИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

М.В. Єсіна, О.В. Потій, Ю.І. Горбенко, В.А. Пономар Методологія оцінки ризику в постквантовий період 7

О.О. Кузнецов, Ю.І. Горбенко, М.О. Полуяненко, С.О. Кандій, Є.Д. Матвєєва Властивості функції вартості в ітеративному алгоритмі генерації нелінійних підстановок 16

І.Д. Горбенко, С.О. Кандій, Є.В. Острянська Порівняння якості алгоритмів семплування з дискретного нормального розподілу на NTRU решітках 29

Я.А. Дерев'янко, Ю.І. Горбенко, О.О. Кузнецов Факторіальна система числення для генерації нелінійних підстановок 38

Д.В. Гармаш Алгоритм RAINBOW та його здатність протидіяти атакам RBS за сторонніми каналами 59

Г.А. Малєєва Аналіз атаки часткового відновлення ключа на мультиваріативні криптографічні перетворення з використанням рангових систем 64

О.О. Кузнецов, М.О. Полуяненко, С.О. Кандій, О.І. Пелюх Дослідження нової функції вартості для генерації випадкових підстановок симетричних шифрів 71

О.Г. Качко, М.В. Єсіна, К.О. Кузнецова Аналіз методів та алгоритмів генерації ключових даних для FALCON подібних алгоритмів електронного підпису 83

Є.Ю. Каптьол Аналіз стану постквантового алгоритму електронного підпису RAINBOW та атак на нього на період завершення третього раунду NIST PQC 87

О.О. Кузнецов, М.О. Полуяненко, С.О. Кандій, Є.О. Логачова Обґрунтування параметрів алгоритму імітації відпалу для пошуку нелінійних підстановок симетричних шифрів 93

МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ В ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

О.В. Сєвєрінов, В.М. Федорченко, Р.Ю. Гвоздьов, В.О. Поддубний Об'єктно-орієнтована модель формального опису інформаційно-комунікаційної системи 110

І.Д. Горбенко, О.А. Замула, Ю.С. Осипенко Концепція оцінки ризиків кібербезпеки інформаційної системи об'єкта критичної інфраструктури 118

В.І. Юхименко, О.І. Федюшин Аналіз масштабування блокчейн проекту Telegram Open Network 130

В.І. Єсін, В.В. Вілігура Дослідження основних методів і схем шифрування з можливостю пошуку 138

А.М. Олейніков,, В.А. Пулавський, І.М. Чигірьов Підвищення ефективності методів і засобів подавлення несанкціонованого запису мови 156

РАДІОЛОКАЦІЯ І РАДІОНАВІГАЦІЯ

І.В. Свид, В.В. Семенець, О.С. Мальцев, М.Г. Ткач, С.В. Старокожев, О.О. Даценко, І.О. Шевцов Порівняльний аналіз методів визначення координат повітряних об'єктів системами широкозонової мультилатерації 162

ЕЛЕКТРОДИНАМІКА, ПОШИРЕННЯ РАДІОХВИЛЬ

А.І. Коваленко, С.В. Тітов, О.В. Тітова, О.С. Чорна Оцінка вимог до параметрів сигналів при V-подібному розподілі частот у математичній моделі багатопозиційної системи випромінювачів 178

АВТОМАТИЗАЦІЯ ТА КОМП'ЮТЕРНО-ІНТЕГРОВАНІ ТЕХНОЛОГІЇ

І.Ш. Невлюдов, С.П. Новоселов, О.В. Сичова, С.І. Теслюк Визначення координат мобільного робота у промисловому приміщенні з використанням технології BLE на основі даних RSSI, отриманих від базових станцій 185

БІОМЕДИЧНА РАДІОЕЛЕКТРОНІКА

І.В. Прасол, О.А. Єрошенко Моделювання залежності інтенсивності електростимуляції від частоти слідування стимулів 192

Н.В. Хміль, В.Г. Колесніков, О.Л. Алтухов Оцінка порушень адаптаційних механізмів при серцевій недостатності методом мікрохвильової діелектрометрії 200

СУМІЖНІ ПРОБЛЕМИ РАДІОТЕХНІКИ

Є.А. Разумов-Фризюк, Д.В. Гурін, Д.О. Нікітін, Р.Є. Стрілець, Д.С. Близнюк Вплив структури активної області резонансно-тунельного діоду на критичні точки його вольт-амперної характеристики 206

Ю.Є. Хорошайло, Н.Я. Зайченко, О.Б. Зайченко. Удосконалення спектроскопічного методу визначення коефіцієнта заломлення матеріалу зразка філаменту для 3D друку в терагерцовому діапазоні 215

О.В. Вовк, І.Б. Чеботарьова, Д.В. Поленок Дослідження особливостей кольоровідтворення на підприємстві ТОВ «НАРГУС» 226

В.А. Тихонов, В.М. Карташов, О.В. Карташов Модель оцінювання статистичних характеристик довгострокової складової випадкового процесу на прикладі аналізу середньомісячних температур 239

РЕФЕРАТИ 246

УДК 004.056.55 **DOI:10.30837/rt.2022.2.209.01**

М.В. ЄСІНА, канд. техн. наук, О.В. ПОТІЙ, д-р техн. наук,
Ю.І. ГОРБЕНКО, канд. техн. наук, В.А. ПОНОМАР, канд. техн. наук

МЕТОДОЛОГІЯ ОЦІНКИ РИЗИКУ В ПОСТКВАНТОВИЙ ПЕРІОД

Вступ

У світі відбувається процес інтенсивного створення та застосування квантових технологій. Президент США підписав 4 травня 2022 р. «Меморандум про національну безпеку з просування лідерства в галузі квантових обчислень при одночасному зниженні ризиків для вразливих криптографічних систем, що свідчить про надзвичайну важливість квантових обчислень та їх застосування в криптології» [1]. Тому, просування лідерства в галузі квантових обчислень взагалі при одночасному зниженні ризиків для вразливих криптографічних систем є важливою проблемою. Відповідно на міжнародному та національному рівнях повинне бути обґрунтовано, прийняте та застосовуватись стандартизоване науково-методичне забезпечення оцінки ризиків взагалі для квантових обчислень, що є надзвичайно важливим для квантових обчислень при його застосуванні в криптології [1].

Метою цієї статі є обґрунтування та розробка методології оцінки ризиків для квантових обчислень при його застосуванні в криптології у так званий «постквантовий період» з урахуванням таких складових вирішення цієї проблеми [1 – 4]:

- використання способів боротьби із загрозами кібербезпеці, яка ще не виникла;
- визначення сутності методології квантової оцінки ризику;
- ідентифікація та документування інформаційних активів та їх поточний криптографічний захист;
- дослідження стану квантових комп'ютерів та квантово-безпечної криптографії. Оцінка термінів доступності цих технологій. Вплив на розробку та перевірку квантово-безпечної криптографії;
- визначення суб'єктів загрози та оцінка їх часу, необхідного для отримання доступу до квантової технології «z» [2];
- визначення часу існування ваших активів «x» і час, необхідний для перетворення технічної інфраструктури організації в квантово-безпечний стан «y» [2];
- визначення квантового ризику за допомогою обчислення, чи стануть бізнес-активи вразливими, перш ніж організація зможе їх захистити;
- визначення та розставлення пріоритетів заходів, необхідних для підтримки обізнаності та переведення технологій організації в квантово-безпечний стан;
- визначення та застосування варіантів захисту від квантових загроз на даний момент.

1. Можливості реалізації квантових обчислень, переваги та недоліки

1.1. Класифікація перспективних фізичних реалізацій квантових комп’ютерів

На основі робіт [2 – 5] створена високорівнева класифікація перспективних фізичних реалізацій квантових комп’ютерів:

• Квантова оптика, коли інформація зберігається та захищається в станах квантів світла на основі поляризації або станах з певним числом фотонів, та може бути реалізована в чіпі за допомогою інтегрованої оптики.

• Надпровідні системи, коли інформація зберігається та обробляється (захищається) в електричних ланцюгах, які використовують властивості надпровідних матеріалів.

• Топологічні системи, коли інформація зберігається та захищається з використанням деяких топологічних властивостей, тобто властивостей, які залежать від «глобальних» (геометричних) властивостей, нечутливих до «локальних» змін – квантових систем.

• Іонні пастки, коли інформація зберігається (захищається) та маніпулюється з використанням властивостей іонів (атомів із незникаючим повним електричним зарядом), які обмежені електромагнітними полями.

• Квантові спінові системи, коли інформація зберігається (захищається) та маніпулюється у внутрішньому ступені свободи, який називається квантовим спіном. Такі системи можуть бути реалізовані в кремнії, як стандартні мікрочіпи, або в менш звичайних системах, як алмази з точковими дефектами, відомі як азотно-заміщена (коротше NV) вакансія [5].

Гази холодних атомів, де нейтральні атоми (а не іони) охолоджуються до значення близького до абсолютного нуля. У той час як іони відштовхуються один від одного через свій електричний заряд, нейтральні атоми цього не роблять, і можуть бути захоплені і організовані в дуже регулярні масиви за допомогою лазерних променів, що створюють так звані оптичні решітки. Атомами можна керувати аж до рівня окремих ділянок в решітці.

1.2. Основні переваги та недоліки квантових комп'ютерів

Основними перевагами та недоліками фізичних реалізацій квантових комп'ютерів є [1, 5]:

• масштабованість, тобто можливість створення та управління все більшими і більшими квантовими пристроями зі все більшою кількістю кубітів, використовуючи фізичні/інженерні ресурси, які керуються керованим способом;

• сумісність з різними обчислювальними моделями та простота їх реалізації;

• типовий час декогерентності (тобто скільки часу залишаються збереженими характеристики та використані в працездатному стані, а також можуть бути використані квантові особливості, такі як суперпозиції);

• швидкість і точність, з якою вентилі можуть бути застосовані.

1.3. Стан розроблення та прийняття в якості національного постквантових стандартів в Україні

Основним застосуванням квантових обчислень є забезпечення криптографічної стійкості певних криптографічних властивостей від класичних та квантових атак, атак на основі помилок та спеціальних атак [7].

Наразі в Україні в якості національного стандарту прийнято постквантовий стандарт криптографічних перетворень асиметричного шифрування та інкапсуляції ключів ДСТУ 8961-2019, розроблено та знаходяться на етапі прийняття проєкти національних стандартів електронного підпису (ЕП) «Вершина» та «Сокіл». Держспецзв'язку, ТК-20 та Національний центр стандартизації проводять роботу з прийняття в якості національного постквантового проєкту стандарту ЕП «Вершина» та проводять громадське обговорення щодо прийняття рішення відносно проєкту постквантового національного стандарту ЕП «Сокіл». Прийняті та впроваджуються національні постквантові стандарти симетричних криптоперетворень ДСТУ 7624-2014, ДСТУ 7564-2014 та ДСТУ 8845-2019. Наука, що стоїть за квантовими комп'ютерами, бере свій початок з фізики квантової механіки, яка вносить фундаментальні зміни в наше розуміння Всесвіту. Багато фізиків мали проблеми з цими революційними ідеями, але експерименти та спостереження підтвердили квантову теорію, і її основні принципи очевидні в звичайних пристроях, таких як лазери та транзистори. Ці технології лише натякають на повну перспективність квантової техніки, але ще потрібна значна робота, перш, ніж буде можливість створити справжній квантовий комп'ютер [1 – 7].

1.4. Стан розроблення та використання квантових комп'ютерів у світі

Коли ефективні квантові комп'ютери [1 – 7] стануть доступними, вони по суті усунуть криптографічну складність існуючих криптосистем з відкритим ключем. Більш традиційні криптосистеми із спільним ключем (такі як AES) також будуть уразливими, що знизить їх ефективну надійність безпеки приблизно до половини того, що є на сьогоднішній день. Цей факт матиме руйнівний вплив на системи, що використовуються для захисту електронних комунікацій та цифрових транзакцій. Більшість безпечних Інтернет-процесів орієнтується на протоколи, які використовують криптографію з відкритим ключем, включаючи ті, що використовуються для захисту веб-сайтів, банківських транзакцій, безпечної електронної пошти та електронних підписів.

Квантові комп'ютери використовують обчислювальну потужність квантових систем і дають можливість вирішувати обчислювальні проблеми, які раніше вважалися важкорозв'язними. Квантові особливості, на які покладаються квантові комп'ютери, дуже важко зберегти та контролювати. Саме це робить створення квантового комп'ютера складним завданням. Однак, будучи створеними, квантові комп'ютери зламають деякі основи інфраструктури кібербезпеки.

Квантову загрозу кібербезпеці можна пом'якшити шляхом розгортання нових криптографічних інструментів (як звичайних, так і квантових), які, як вважається та/або відомо, є стійкими до квантових атак. Тим не менш, перехід до квантово-безпечної криптографії сам по собі є проблемою, оскільки вимагає розробки та розгортання апаратних і програмних рішень, встановлення стандартів, міграції застарілих систем тощо.

Стан розроблення та застосування квантових комп'ютерів для криптоаналізу наведено нижче [6]:

- IBM повідомила про план запуску в жовтні 2019 р. 53-кубітного квантового комп'ютера (КВК);
- 53-кубітний КВК IBM має нову конструкцію процесора, має можливість масштабуватись, знижена ймовірність помилок, надійний в хмарі;
- IBM відкриває новий обчислювальний центр в Нью-Йорку, 1–53 кубіт, 5–20 кубіт (14 в перспективі);
- 72-кубітний КВК Google за 3,5 хвилини виконує еквівалент роботи 10 тисяч операцій надпотужного кластера.

Згідно з [9, 11] IBM представили квантовий 127-кубітний процесор Eagle. Він прийшов на зміну 65-кубітному квантовому процесору Hummingbird, що відповідає дорожній карті квантових технологій від IBM [10]. Як зазначено в [9], відмінністю Eagle від попередніх процесорів полягає в тому, що він потребує значно меншої кількості електроніки для контролю та зчитування на кубіт регістру завдяки застосуванню мультиплексування зчитування. Також IBM повідомляють про наміри щодо побудови нової інтегрованої квантової обчислювальної системи IBM Quantum System Two на основі покращених чіпів, замість вже існуючої системи IBM Quantum System One.

Також є відомості [11] про наміри IBM представити 433-кубітний процесор Osprey наступного року, та 1121-кубітного процесору Condor в 2023 році, що відповідає дорожній карті, наведеній в [10].

В той самий час, компанія D-wave, що відома своїми розробками в сфері побудови псевдо-квантових (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 близько 2023 – 2024 року та про наміри щодо розробки власних надпровідникових квантових машин гейтового типу (розробкою яких наразі замаються IBM, Google та інші) [12].

Зрозуміло, що фактичний стан розроблення та застосування квантових комп'ютерів та їх математичного та програмного забезпечення є строго конфіденційним та надійно захищається.

Сутність та стан вирішення проблеми постквантової криптографії на світовому рівні – NIST США провів три етапи конкуру щодо кандидатів на стандарти постквантових асиметричних криптографічних примітивів. Наразі проведено семінар, на якому розглянуто попередні підсумки 3-го етапу конкурсу проєктів асиметричних криптографічних перетворень.

Основні вимоги до кандидатів на стандарти постквантових криптоперетворень можна конкретизувати у трьох напрямках [7, 8]:

- вимоги з безпеки (вимоги щодо стійкості до криптографічного аналізу);
- техніко-економічні вимоги (в основному щодо часової та просторової складностей);
- технічні характеристики реалізації алгоритмів асиметричних криптоперетворень.

Вимоги до стійкості ЕП мають бути сформульовані у відповідності до моделі загроз EUF-CMA (Existentially unforgeable under adaptive chosen message attacks), тобто забезпечення захисту від екзістенційної підробки при атаках на основі адаптивно підібраного (вибраного) шифртексту [8].

1.5. Вимоги до параметрів квантових комп'ютерів

Основними вимогами є:

- час міграції: кількість років для міграції системи до квантово-безпечного рішення;
- часова шкала загроз: кількість років до того, як відповідні суб'єкти загрози зможуть зламати квантово-вразливі системи.

Якщо термін загрози менший за суму терміну зберігання та часу міграції, організації не зможуть захистити свої активи протягом необхідних років від квантових атак. Краще розуміння часової шкали загроз надає інформацію про час, доступний для безпечного переходу до постквантових кіберсистем.

Оцінити квантові загрози дуже складно через наукові та інженерні перешкоди, пов'язані з побудовою працюючого квантового комп'ютера. Експерти загалом визнають, що досі не знають, коли з'являться квантові комп'ютери, які можуть загрожувати кіберсистемам. Проте було б дуже корисно мати уявлення про перспективи цієї загрози, що стане реальною в короткостроковій та середньостроковій перспективі, про швидкість прогресу та про основні віхи, на які слід звернути увагу менеджерам із кіберризиків.

Основною проблемою в побудові квантового комп'ютера є створення надійних фундаментальних компонентів, так званих фізичних кубітів, кількість яких можна масштабувати, зберігаючи контроль і якість. У цьому відношенні експерти вказали, що найбільш перспективною фізичною платформою для реалізації криптографічно релевантного квантового комп'ютера є надпровідні системи, за якими відносно близько слідують захоплені іони, а також кілька інших фізичних реалізацій, що мають значний потенціал.

Дуже важливим кроком вперед буде експериментальна демонстрація того, що схеми виправлення помилок покращують надійність так званих логічних кубітів у порівнянні з фізичними кубітами. Щоб це сталося, має бути можливість достатньо добре підготувати, маніпулювати та виміряти основні фізичні кубіти. Наскільки добре має бути це «досить добре», залежить від найвідоміших схем виправлення помилок, які самі по собі можуть бути замінені новими та кращими схемами.

Іншим етапом стане демонстрація так званої «квантової переваги», тобто здатності квантового пристрою виконувати певні обчислення, які були б практично неможливими навіть для найпотужнішого класичного суперкомп'ютера, незалежно від корисності таких обчислень. Хоча досягнення квантової переваги не обов'язково призведе до вирішального криптографічного прогресу стосовно квантового комп'ютера, це означатиме досягнення відносно високого рівня контролю над відносно великою кількістю фізичних кубітів, що є

необхідною складовою для квантових обчислень. Експерти погодилися, що цей етап, ймовірно, буде пройдено в найближчі пару років [5].

2. Методологія оцінки ризику в постквантовий період

2.1. Способи боротьби із загрозою, яка ще не виникла

Незважаючи на постійний прогрес у розвитку квантових обчислень, ймовірно, що реально квантові комп'ютери стануть доступними та будуть застосовуватись для криптоаналізу, щонайменше через 5 – 15 років [2 – 8]. Можливо, це пояснює низький рівень занепокоєння тих, хто відповідає за планування кібербезпеки та прийняття рішень. Безсумнівно, їхня увага зосереджена на безлічі кіберзагроз, з якими сьогодні стикаються всі організації, і, можливо, вони вважають, що буде достатньо часу, щоб відповісти, як тільки квантові комп'ютери справді з'являться.

Щодо цієї точки зору є декілька проблем. Як тільки квантовий комп'ютер буде винайдено, це негайно вплине на безпеку всіх Інтернет-комунікацій і даних. Якщо організації не будуть готові до цієї раптової кризи, вони зіткнуться з негайною потребою замінити свої існуючі криптографічні системи безпеки на квантово-безпечні рішення.

Адаптація всієї криптографічної інфраструктури організації в період, коли всі інші намагаються зробити те ж саме, ймовірно, буде складною і дорогою. Небагато організацій самостійно розробляють можливості криптографічної безпеки, більшість отримує їх у постачальників, часто інтегрованих у мережу чи продукти безпеки. Без попередньої підготовки організація може не мати уявлення про здатність своїх постачальників надавати квантово-безпечні рішення, а також не знати про труднощі, з якими вона зіткнеться при інтеграції нової технології в своє середовище. Однак це не єдина проблема, з якою можуть зіткнутися погано підготовлені організації.

Було запропоновано кілька квантово-безпечних рішень, але небагато з них вийшли з фази дослідження, і навіть вони потребують багато роботи, щоб перевірити, чи можуть вони протистояти як звичайним, так і квантовим атакам. Протягом останніх 15 або більше років поточні протоколи кібербезпеки стикалися з реальними проблемами та перейшли до свого поточного стану. Ми довіряємо їм частково через їх математичні основи, а також тому, що вони витримали випробування часом. Якщо ми хочемо довіряти квантово-безпечній криптографії, важливо, щоб тестування в реальному світі розпочалося якомога швидше.

Управління цією проблемою вимагатиме усвідомлення, планування та підготовки. Добре підготовлена організація може вжити заходів для інтеграції квантово-безпечних рішень у існуюче планування кібербезпеки та управління життєвим циклом, де їх можна оцінити на предмет функціональності, продуктивності, простоти використання та інших факторів. При необхідності існуючу інфраструктуру можна покращити або замінити. І все це може статися до того, як ці зміни стануть критичними для безпеки організації.

Організації також повинні мати можливість захищати свою конфіденційну інформацію протягом усього терміну її існування. Інформація, яка вважається безпечною для зберігання або передачі, оскільки вона зашифрована, може стати вразливою для квантового комп'ютера протягом його життя. Розуміння цього ризику вимагає вивчення поточних засобів кіберзахисту та доступу суб'єктів потенційної загрози до технології квантових обчислень.

Управління переходом повного набору інструментів, що використовуються для захисту різноманітних бізнес-функцій та інформаційних активів, може здатися складним завданням без чіткої відправної точки чи пріоритетів.

Квантова оцінка ризику – це ідеальний підхід для виявлення та визначення пріоритетів загроз і вразливостей, а також закладання основи для надійного та економічно ефективного розвитку систем, щоб вони були стійкими до квантових атак.

2.2. Сутність методології квантової оцінки ризику

Квантова оцінка ризику дає організації знання, необхідні для розуміння ступеня їх квантового кіберризику та термінів, за які можуть виникнути квантові загрози. Це забезпечить організацію основою для проактивного вирішення квантових ризиків, побудови шляху до квантово безпечного стану, а також для впровадження та підтвердження квантово-безпечних рішень як частини нормального управління життєвим циклом, а не як відповідь на кризу.

Квантова оцінка ризику (QRA) не замінює звичайну оцінку кіберризику (RA). Частина інформації, зібраної під час RA, також вимагається квантовим процесом, тому QRA зазвичай проводиться разом із традиційним RA або після нього. Однак QRA зосереджена на конкретних питаннях безпеки, які виникають у квантових комп'ютерах; вона не стосується безпосередньо кількох аспектів традиційного процесу оцінювання.

Кілька років тому Mosca запропонував модель для оцінки квантового ризику [2]. Описаний далі шестифазний процес QRA узгоджується з моделями оцінки ризиків таких організацій, як NIST, а також включає квантову модель ризику Mosca «x, y, z».

2.2.1. Фаза 1 «Ідентифікація та задокументування інформаційних активів та їх поточний криптографічний захист»

Як і будь-яка оцінка ризику, QRA починається з інвентаризації важливих активів. У центрі уваги тут є чутливі або цінні інформаційні активи, які потребують криптографічного захисту відповідно до політики безпеки організації. Важливо визначити характер використовуваної криптографії, спосіб створення, зберігання та застосування ключів шифрування, а також походження інструментів або пристроїв, які використовуються в цих процесах.

На високому рівні організація повинна розуміти природу своєї конфіденційної/цінної інформації, включаючи її цінність для бізнесу, механізми контролю доступу та спільного використання даних, процедури резервного копіювання та відновлення, а також те, як вона обробляється наприкінці терміну служби. Багато організацій мають правові або нормативні вимоги, які впливають на це. Для визначення вразливості організації до зовнішніх і внутрішніх загроз необхідний комплексний огляд усіх цих факторів.

2.2.2. Фаза 2 «Дослідження стану квантових комп'ютерів та квантово-безпечної криптографії. Оцінка термінів доступності цих технологій. Вплив на розробку та перевірку квантово-безпечної криптографії»

Ця фаза не є унікальною для конкретної QRA, це скоріше безперервний процес, який проводиться групою експертів з квантових технологій, які розуміють перешкоди та події, з якими стикаються в кількох галузях квантових досліджень, і можуть використовувати інформацію для прогнозування ймовірних термінів для надання квантового комп'ютера та розуміння його впливу на кібербезпеку організації.

Існує багато джерел інформації про стан квантових технологій, але розуміння актуальності та справжнього впливу конкретних дослідницьких розробок не є тривіальним процесом. Наявність спеціальної команди експертів з квантової галузі або відносини з організацією, що спеціалізується на квантових технологіях, є надзвичайно важливим для завершення QRA. У всьому світі існує кілька груп, які проводять незалежні дослідження та використовують різні підходи до розробки квантових комп'ютерів і квантово-безпечної криптографії. Важливо мати доступ до експертів, які стежать за подіями в обох сферах і можуть контекстуалізувати їх, щоб прогнозувати їхній вплив на кібербезпеку.

В ідеалі результати цієї фази QRA використовуються для впливу на розвиток квантово-безпечної криптографії. Робота з квантовими експертами, які мають міцні зв'язки з академічними та дослідницькими спільнотами, дозволяє реальним проблемам, виявленим QRA, впливати на напрямок квантово-безпечних досліджень.

2.2.3. Фаза 3 «Визначення суб'єктів загрози та оцінка їх часу, необхідного, щоб отримати доступ до квантової технології «z»»

Організація, яка піклується про безпеку, знатиме всі загрози для своїх найбільш значущих суб'єктів та матиме список попередніх спроб проникнути в їхній кіберзахист. QRA розглядає вплив квантових обчислень на ці загрози, зосереджуючи увагу на ймовірності того, що вони зможуть використовувати квантові комп'ютери, і часові межі доступу до них. Також треба розглядати нові діючі сторони загроз, які можуть з'явитися, коли квантові обчислення стануть реальністю. У сукупності вони утворюють частину Collapse Time (z) моделі Mosca, тобто час, доки поточні засоби кіберзахисту не впадуть перед загрозами, які мають доступ до квантових технологій.

Цей процес знову вимагає постійної оцінки експертів, які знають розвиток кібербезпеки та квантових обчислень.

2.2.4. Фаза 4 «Визначення часу існування ваших активів «x» і час, необхідний для перетворення технічної інфраструктури організації в квантово-безпечний стан «y»»

Визначення терміну служби бізнес-інформації має вирішальне значення для розуміння квантової вразливості організації. Якщо зловмисник може захопити та заархівувати зашифровану інформацію, як довго вона буде корисною? Це регулюватиметься характером бізнесу, продуктів і клієнтів, а також нормативними вимогами, які можуть застосовуватися до організації.

Розглядаються доступні інструменти для боротьби з квантовими загрозами. Наскільки ефективні поточна політика та процедури щодо захисту зашифрованої інформації організації як від внутрішніх, так і від зовнішніх загроз? Досліджується міцність існуючої криптографії та наскільки ефективно вона застосовується та використовується. Розглядаються доступні квантово-безпечні криптографічні методи, щоб визначити, чи можуть вони бути доречною заміною існуючих можливостей. Можна зв'язатися з постачальниками, які виготовили продукти, які використовуються в організації, щоб визначити, чи можна впровадити нові алгоритми або протоколи в існуючі інструменти та пристрої, чи може знадобитися оновлене обладнання. Переглядаючи політику, процеси управління та закупівлі, які застосовуються до IT та інфраструктури безпеки організації, оцінюється, чи можна інтегрувати квантову безпеку в процеси управління життєвим циклом IT організації.

Маючи цю інформацію, можна обчислити решту значень моделі Mosca – термін зберігання даних організації (x) та час міграції інфраструктури (y).

2.2.5. Фаза 5 «Визначення квантового ризику за допомогою обчислення, чи стануть бізнес-активи вразливими, перш, ніж організація зможе їх захистити (x+y>z?)»

Використовуючи інформацію, зібрану до цього моменту, можна оцінити ризик, з яким стикається організація, коли з'являються квантові комп'ютери. Враховується тривалість життя конфіденційних даних, включаючи ймовірність їхнього впливу. Це порівнюється з проміжком часу, протягом якого квантові технології будуть доступні відповідним суб'єктам загрози. У сукупності це дає розумну оцінку того, коли організації необхідно вжити активних заходів для пом'якшення квантового ризику. Цілком можливо, що деякі організації вже стикаються з цим ризиком, залежно від терміну життя їхніх даних і процесів, які діють для їх захисту сьогодні.

Далі необхідно оцінити вплив на бізнес-процеси, який є результатом очікуваних змін:

- скільки часу знадобиться для впровадження необхідних змін у продукти, протоколи та процедури?
- чи призведуть квантово-безпечні технології до проблем із затримками, надійністю чи продуктивністю, які потребують вирішення?
- чи потрібні зміни в політиці чи процедурі для покращення переглянутої системи чи загальної безпеки інформації організації?

2.2.6. Фаза 6. «Визначення та розставлення пріоритетів заходів, необхідних для підтримки обізнаності та переведення технологій організації в квантово-безпечний стан»

Квантова оцінка ризику надає інформацію та вказівки щодо статусу квантової безпеки, але навряд чи цього стану можна досягти за допомогою інструментів і технологій, доступних сьогодні. Квантові технології продовжують розвиватися, як і наше розуміння сильних і вразливих сторін квантово-безпечних підходів. Плани міграції також повинні реагувати на зміни, оскільки постачальники включають ці розробки у свої продукти та інструменти. Важливо відстежувати все це, і більшість організацій повинні розробити план, який вирішує безпосередні проблеми, дозволяючи впроваджувати нові квантові технології, коли вони стають доступними.

Будь-яку оцінку кіберризиків необхідно періодично оновлювати, щоб врахувати нові загрози та скористатися перевагами покращених рішень безпеки. Особливо це стосується квантових технологій, які швидко розвиваються. Зараз досліджуються різні варіанти квантових технологій, але не всі вони створюють однакову загрозу кібербезпеці, і може бути важко оцінити вплив будь-якої нової квантової розробки. Тому рекомендується, щоб QRA була першим кроком у створенні шляху до квантової безпеки.

Цей шлях буде розроблений для забезпечення постійного доступу до фахівців, які дотримуються цих технологій і розуміють наслідки нових розробок у квантових обчисленнях і квантовій криптографії. Це може стати основою для початку обговорення з працівниками організації, партнерами, клієнтами та постачальниками продуктів, гарантуючи, що всі знають про кроки, які вживаються, і переконавшись, що вони розуміють який вплив це матиме на їхні власні процеси та інфраструктуру.

Висновки

1. Квантова оцінка ризику – це ідеальний підхід для виявлення та визначення пріоритетів загроз і вразливостей, а також закладання основи для надійного та економічно ефективного розвитку систем, щоб вони були стійкими до квантових атак.

2. Квантова оцінка ризику дає організації знання, необхідні для розуміння ступеня їх квантового кіберризику та термінів, за які можуть виникнути квантові загрози. Це забезпечить організацію основою для проактивного вирішення квантових ризиків, побудови шляху до квантово безпечного стану, а також для впровадження та підтвердження квантово-безпечних рішень.

3. Квантова оцінка ризику (QRA) не замінює звичайну оцінку кіберризику (RA). Частина інформації, зібраної під час RA, також вимагається квантовим процесом, тому QRA зазвичай проводиться разом із традиційним RA або після нього.

4. У [2] Mosca запропонував модель для оцінки квантового ризику. Описаний шестифазний процес QRA узгоджується з моделями оцінки ризиків таких організацій, як NIST, а також включає квантову модель ризику Mosca «x, y, z».

5. Якщо організація використовує будь-яку інформаційну технологію, то криптографія завжди використовується для кібербезпеки. Тому не можна дозволити чекати появи квантових комп’ютерів, щоб зрозуміти ризики, з якими можна стикнутись.

6. Необхідно вжити наступні заходи для того щоб [2 – 8]:

• переконатися, що є наявним поточний, ретельний організаційний інвентар, який містить відомості про вбудовану криптографію, яка може існувати в різних продуктах;

• відстежувати оточення на предмет загроз і забезпечувати регулярну оцінку ризиків;

• проводити квантову оцінку ризику як частину регулярного процесу оцінки ризику або після нього;

• зрозуміти позицію постачальників телекомунікацій та безпеки щодо квантових обчислень, на які з їхніх продуктів це вплине, а також про те, як вони підготуються до управління цим ризиком;

• оцінити квантову готовність як частину ваших поточних процесів закупівлі мереж і систем безпеки, обговорити стан квантового планування поточних постачальників;

• співпрацювати з інформованим партнером, щоб відстежувати розвиток квантових обчислень і квантово-безпечних рішень, а також створити план квантової готовності для організації.

7. Найбільшому ризику піддаються організації, які чекають на прибуття квантових комп'ютерів або уникають дій, поки не будуть розроблені ідеальні криптографічні рішення. Це напевно змусить таку організацію боротися зі своєю раптовою вразливістю до квантової атаки в осяжному майбутньому.

Список літератури:

1. National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems. [Електронний ресурс]. Режим доступу: https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/.
2. Michele Mosca, John Mulholland A Methodology for Quantum Ass Risk Assessment. [Електронний ресурс]. Режим доступу: https://globalriskinstitute.org/publications/3423-2/.
3. Mosca M., Piani M. (2019). Quantum Threat Timeline. Global Risk Institute. [Електронний ресурс]. Режим доступу: https://globalriskinstitute.org/publications/quantum-threat-timeline/.
4. Mosca M., Piani M. Quantum Threat Timeline Report 2020. Global Risk Insitute. [Електронний ресурс]. Режим доступу: https://globalriskinstitute.org/publications/quantum-threat-timeline-report-2020/.
5. Mosca M., Piani M. Quantum Thremtntat Timeline Report 2021. Global Risk Insitute. [Електронний ресурс]. Режим доступу: https://globalriskinstitute.org/publications/2021-quantum-threat-timeline-report/.
6. Viktor Onoprienko The state of innovative research and development in the field of information security in Ukraine (JSC "IIT") / Viktor Onoprienko, Marina Yesina, Ivan Gorbenko, Yuri Gorbenko, Elena Kachko // Forum: Innovative solutions in a digitalized economy: Germany – Ukraine. [Електронний ресурс]. Режим доступу: https://www.facebook.com/events/596729504987733/.
7. Gorjan Alagic NISTIR 8309 Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process / Gorjan Alagic, Jacob Alperin-Sheriff, Daniel Apon, David Cooper, Quynh Dang, John Kelsey, Yi-Kai Liu, Carl Miller, Dustin Moody, Rene Peralta, Ray Perlner, Angela Robinson, Daniel Smith-Tone. Режим доступу: https://doi.org/10.6028/NIST.IR.8309.
8. Горбенко Ю. І. Побудування та аналіз систем, протоколів та засобів криптографічного захисту інформації / Ю. І. Горбенко, за ред. Горбенко І. Д. Харків : Форт, 2016. 959 с.
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. Nature News. Philip Ball [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/.

Надійшла до редколегії 02.03.2022

Відомості про авторів:

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

Потій Олександр Володимирович – д-р техн. наук., професор, полковник, 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

УДК 004.056.5 **DOI:10.30837/rt.2022.2.209.02**

О.О. КУЗНЕЦОВ, д-р техн. наук, Ю.І. ГОРБЕНКО, канд. техн. наук,
М.О ПОЛУЯНЕНКО, канд. техн. наук, С.О. КАНДІЙ, Є.Д. МАТВЄЄВА

ВЛАСТИВОСТІ ФУНКЦІЇ ВАРТОСТІ В ІТЕРАТИВНОМУ АЛГОРИТМІ ГЕНЕРАЦІЇ НЕЛІНІЙНИХ ПІДСТАНОВОК

Вступ

При проєктуванні шифру із симетричним ключем складну задачу становить генерація криптографічно стійких нелінійних підстановок (S-блоків) [1 – 3]. По перше, нелінійні підстановки повинні бути випадковими, тобто не містити простих алгебраїчних конструкцій, бо це може створити передумови для ефективного алгебраїчного криптоаналізу [4, 5]. По друге, S-блоки повинні забезпечувати необхідні криптографічні властивості, які значно ускладнюють реалізацію різних криптоаналітичних атак (диференційного, лінійного, статистичного та інш.) [3, 6, 7]. Отже задача генерації нелінійних підстановок є складною та надзвичайно важливою з точки зору подальшого удосконалення криптографічних алгоритмів із симетричним ключем.

Найбільш перспективними для генерації високонелінійних S-блоків вважаються евристичні техніки. Вони дозволяють ітеративним шляхом змінювати початковий випадковий S-блок доти він не буде відповідати встановленим критеріям. Однак час такої генерації може бути занадто великим. Наприклад, для кращого відомого результату генерація випадкових бієктивних 8-бітних підстановок із нелінійністю понад 104 вимагає понад 65 тисяч ітерацій [8, 9]. Метою цієї роботи є оптимізація евристичних методів для прискорення генерації високонелінійних S-блоків.

Пов’язані роботи

В цій роботі розглядаються евристичні техніки генерації нелінійних підстановок. До таких алгоритмів відносяться евристичні методи:

- алгоритм локального пошуку (Local Search Algorithm) [1, 8 – 10];
- алгоритм сходження на пагорб (Hill climbing) [8, 11 – 13];
- метод градієнтного спуску (gradient descent method) [6, 14];
- алгоритм імітації відпалу (simulated annealing) [12, 15 – 17] та [10, 18];
- генетичний алгоритм (Genetic Algorithm) [19 – 21] тощо.

Основне завдання евристичних технік – зниження (або у деяких випадках збільшення) функції вартості, яка пов’язана з бажаною властивістю S-блоку. Під час роботи алгоритму пошуку виконується наближення характеристик поточного S-блоку до бажаного значення. Слід зазначити, що успіх генерації дуже чутливий до обраної функції вартості, а отже до вибору її параметрів. Серед відомих функції вартості слід виділити такі найбільш популярні:

- функція вартості Кларка (Clark’s cost functions *WHS*) [15] та її модифікація [10, 18];
- функція вартості Пічека (Picek’s cost functions *PCF*) [8, 22];
- функція вартості Фрейре – Ечеваррія (Freyre – Echevarría cost functions *WCF*) [8, 9].

У даній роботі розглядається функція вартості WCF, яка була запропонована у роботах [8,9]. Використовуючи алгоритм сходження на пагорб (Hill climbing) [2, 11, 23] та функцію WCF авторами було отримано кращий відомий на сьогоднішній день результат з генерації 8-бітних бієктивних підстановок із нелінійністю 104 [8, 9]. Середня кількість ітерацій алгоритму пошуку до знаходження S-блоку з нелінійністю 104 становила 65,933 [9]. В [9] наведено, що з 30 незалежних експериментів у 11 випадках було знайдено S-блок з нелінійністю 104. У іншій публікації тих самих авторів [8] наведено середнє значення у 70,596 ітерацій.

В цій роботі перевіряються результати робіт [8, 9] та оптимізуються параметри функції WCF. Зокрема, ми підтверджуємо результати [8, 9] та показуємо, що функція WCF може

бути ще ефективнішою. В наших експериментах ми отримали найменше значення числа ітерацій для функції WCF та Hill climbing алгоритму. Фактично нам вдалося значно підвищити ефективність евристичного пошуку через зменшення кількості ітерацій.

Методика дослідження

Для пошуку бієктивних S-блоків з високою нелінійністю в цій роботі використовується алгоритм Hill climbing [8, 11 – 13]. Сходження на пагорб – це ітераційний алгоритм, який починає свій пошук з деякої можливої точки, випадково обраної в просторі станів. Потім послідовно застосовується механізм генерації для пошуку кращого рішення (з точки зору значення функції вартості), досліджуючи сусідство поточного рішення. Якщо знайдено краще рішення, воно стає поточним рішенням. Алгоритм закінчує роботу, коли не вдається знайти покращення, а поточне рішення розглядається як приблизне рішення задачі оптимізації.

Алгоритм сходження на пагорб оптимізує функцію вартості, досліджуючи сусідні точки рішення відносно поточної точки в просторі рішень. Нижче розглядаємо (S, f) приклад комбінаторної задачі оптимізації (де S – набір можливих рішень; f – функція вартості, яку слід мінімізувати).

Алгоритм сходження на пагорб (для задачі мінімізації) можна узагальнити наступним псевдокодом 1:

Псевдокод 1. Пошук локального мінімуму

1. Вибрати початкове рішення S_i;
2. Генерувати рішення S_j із сусідства поточного рішення S_i;
3. Якщо ($f(S_j) < f(S_i)$), то S_j стає поточним рішенням;
4. Якщо ($f(S_j) \geq f(S_i)$) для певної кількості S_j, то закінчити;
5. Перейди до кроку 2.

В роботі було запрограмовано алгоритм сходження на пагорб, який одночасно виконував пошук в декількох потоках, працюючих паралельно. Кількість потоків вказується у вхідному параметрі thread_count (в нашому випадку thread_count = 2). Алгоритм починає свою роботу з підстановки, яку згенеровано випадково. Ця підстановка встановлюється як поточне рішення S_i. Поточне рішення є загальним для всіх потоків. На кожній ітерації циклу утворюється декілька (відповідно до параметру thread_count) нових рішень S_j, які генеруються за заданими операторами мутації. Оператор мутації обирає випадковим чином $k = 2$ різних позицій у підстановці S_i і переставляє елементи у обраних позиціях. Нове рішення S_j порівнюється з поточним S_i. В разі отримання кращого, ніж поточне, рішення воно встановлюється як поточне.

Всі ітерації пошуку за алгоритмом сходження на пагорб виконуються у внутрішньому циклі. Ітерації внутрішнього циклу вкладено в зовнішній цикл. Зовнішній цикл не є обов'язковим для роботи алгоритму, він введений лише для відстеження поточного стану процесу пошуку та оптимізації вибору його параметрів. Докладніше алгоритм розглянуто у [10].

В якості цільового S-блоку було обрано бієктивний 8-бітний S-блок з нелінійністю $N_f = 104$. В якості інших параметрів використовувались наступні:

- кількість внутрішніх циклів – max_inner_loops=10000;
- максимальна кількість зовнішніх циклів – max_outer_loops=50;

- максимальна кількісті поспіль зовнішніх циклів, при яких не виконано жодного покращення функції вартості – max_frozen_outer_loops=5.

Критерії зупинки алгоритму:

- знаходження бієктивного S-блоку з нелінійністю 104;
- досягнення максимальної кількості ітерацій (відповідає значенню thread_count x max_inner_loops x max_outer_loops);
- досягнення кількості поспіль зовнішніх циклів, при яких не виконано жодного покращення функції вартості значення max_frozen_outer_loops.

Дослідження функції вартості *WCF*

Як основний апарат аналізу та вивчення особливостей критеріїв зручно вибрати перетворення Фур'є та Уолша булевих функцій [1, 11, 24].

Перетворення Уолша – Адамара

Позначимо через **x, ω** двійкові набори довжини n над $GF(2)$, а x_i, ω_i – координати цих наборів. Якщо, $f(x_1, x_2, \ldots, x_n)$ – булева функція двійкових змінних, то через $f'(x_1, x_2, \ldots, x_n) = (-1)^{f(x_1, x_2, \ldots, x_n)}$ позначимо спряжену функцію, визначену на тій самій множині. Функції f та f' однозначно визначають один одного. Скалярний добуток **x** та **ω** – це цілочисельна функція, яка визначається як

$$\langle \mathbf{x}, \boldsymbol{\omega} \rangle = \sum_{i=1}^{n} x_i \cdot \omega_i \ .$$

Перетворення Уолша булевої функції $f(\mathbf{x})$ позначається, як

$$W_f\left(f(\mathbf{x}), \omega\right) = \sum_{\mathbf{x}=F_2^n} f(\mathbf{x}) \cdot (-1)^{\langle \mathbf{x}, \omega \rangle} \ .$$

Спектральне перетворення функції $f'(\mathbf{x})$ позначається через

$$WHT\left(f(\mathbf{x}), \omega\right) = \sum_{\mathbf{x}=F_2^n} (-1)^{f(\mathbf{x}) + \langle \mathbf{x}, \omega \rangle},$$

та носить назву перетворення Уолша – Адамара булевої функції.

Спектральні перетворення дозволяють безпосередньо оцінити збалансованість, нелінійність та кореляційну імунність булевої функції [1, 11, 24]. Зокрема, нелінійність S-блоку виражається як

$$N(S) = 2^{n-1} - \frac{1}{2} \cdot \max\left(|WHT|\right), \tag{1}$$

де $\max\left(|WHT|\right)$ – максимальне абсолютне значення в спектрі Уолша-Адамара за всіма компонентними булевими функціями S-блоку.

Розподіл спектральних коефіцієнтів Уолша – Адамара

Приклад значень спектральних коефіцієнтів Уолша – Адамара для випадково сформованого бієктивного 8x8 S-блоку, представлено на рис. 1 (представлено фрагмент для 256 значень).

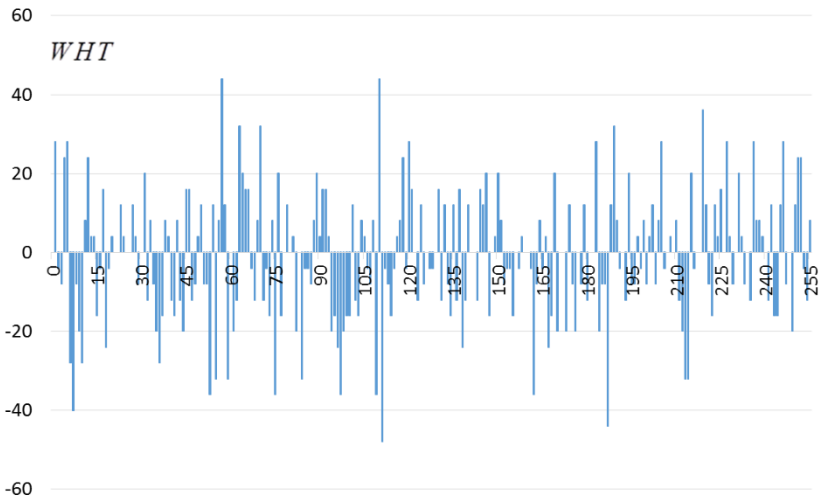


Рис. 1. Перші 256 спектральних коефіцієнтів Уолша – Адамара для випадково сформованого бієктивного S-блоку (приклад)

Як бачимо для даного прикладу, значення WHT змінюються від – 48 до +57. Зміна значень WHT завжди відбувається з шагом 4. Гістограма розподілу кількості коефіцієнтів WHT за їх значеннями (для всіх 65 280 значень) наведена на рис. 2. По лінії абсцис відкладено значення, яке приймає WHT, а за ординат – кількість випадків, коли у спектрі з'являється таке значення WHT.

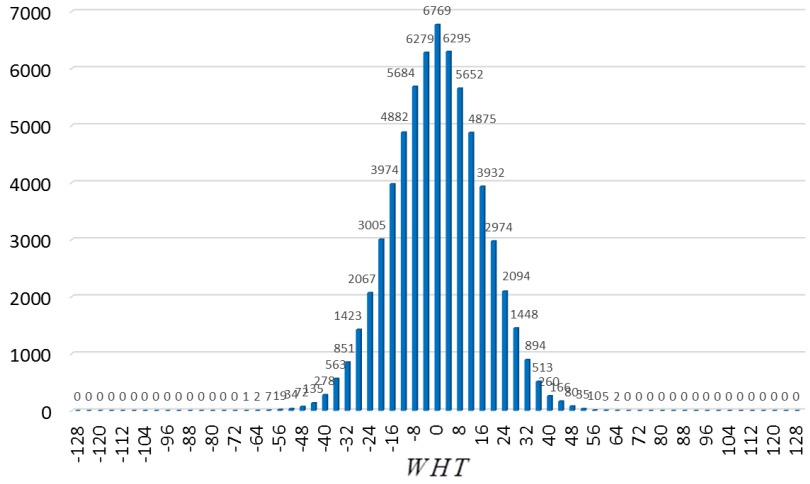


Рис. 2. Розподіл значень спектральних коефіцієнтів Уолша – Адамара для випадково сформованого бієктивного S-блоку (приклад)

З урахуванням (1) нас цікавить максимальне значення спектру, тобто $\max\left(\left|WHT\right|\right)$. У наведеному прикладі це буде -68, тобто $N(S)=94$.

При використанні евристичних алгоритмів пошуку цільового S-блоку здійснюється поступове зменшення $\max\left(\left|WHT\right|\right)$, що призводить до підвищення нелінійності S-блоку. Так, на рис. 3 наведено фінальний розподіл кількості WHT за їх значеннями при $N(S)=104$. На рис. 4 наведено гістограму змін розподілу кількості WHT від начального стану (випадково сформованого бієктивного S-блоку) до кінцевого стану. В цьому експерименті застосовувався алгоритм сходження на пагорб (Hill climbing). Всього було виконано 117 покращень функції *WCF*. Символом k позначено кількість прийнятих покращень у алгоритмі пошуку.

Як бачимо з наведених результатів, форма розподілу та його максимум суттєво не змінюється під час покращень за обраним алгоритмом пошуку. Тому, цілком доречно виглядає ідея враховувати лише частину розподілу спектру коефіцієнтів Уолша – Адамара, яка наближена до $\max\left(\left|WHT\right|\right)$, що і було реалізовано у функції вартості *WCF*.

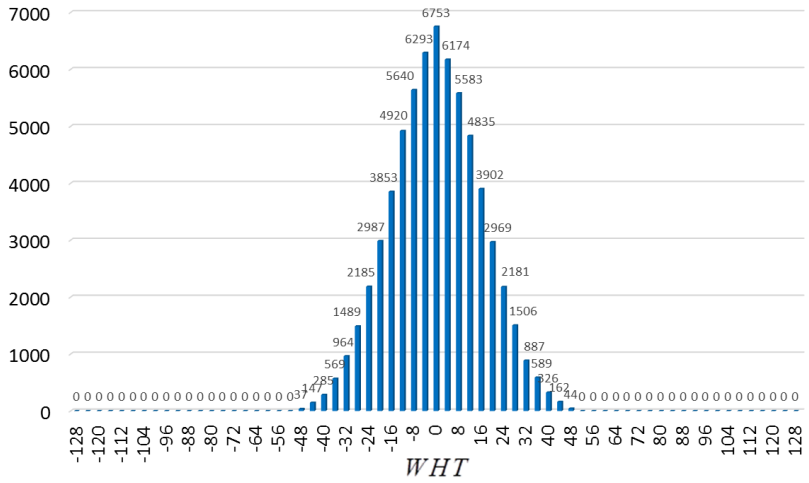


Рис. 3. Розподіл значень спектральних коефіцієнтів Уолша – Адамара для отриманого бієктивного S-блоку з нелінійністю $N(S)=104$

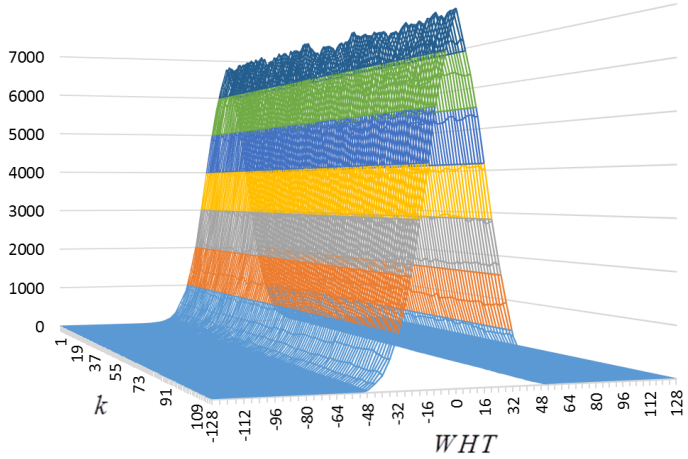


Рис. 4. Гістограма змін розподілу значень спектральних коефіцієнтів Уолша – Адамара

Опис функції вартості WCF

Функція вартості *WCF* у загальному випадку має наступний вигляд [8, 9]:

$$WCF=\sum_{b=1}^{255}\sum_{i=0}^{255}\prod_{\substack{j=start\\ j+=step}}^{end}\left|\left|WHT[b,i]\right|-j\right|, \tag{2}$$

де

- *WHT* – спектральні коефіцієнти Уолша – Адамара;
- $start, step, end$ – деякі цілі значення, як правило $start=0, step=4$ (виходячи з кратності коефіцієнтів *WHT* чотирма);
- i – змінна циклу за всіма компонентними функціями та їх лінійними комбінаціями;
- b – змінна циклу за всіма лінійними функціями.

Для кожного S-блоку розміру 8x8 є $256 \cdot 256 = 65536$ значень спектральних коефіцієнтів Уолша – Адамара. Причому, при $b = 0$ перше значення завжди буде дорівнювати 256, а наступні 255 – нулю, тому сума починається з одиниці та загальна кількість коефіцієнтів, що досліджується, становить 65 280.

Гістограма зміни значення функції *WCF*, яка відповідає зміни розподілу спектральних коефіцієнтів Уолша – Адамара, наведена на рис. 5. Цю діаграму отримано при параметрах $start = 0, step = 4, end = 32$.

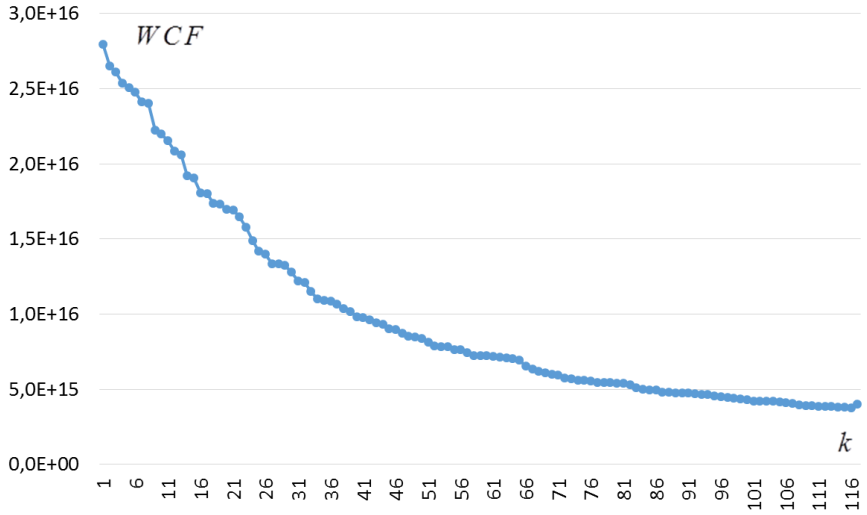


Рис. 5. Діаграма зміни значення функції *WCF*

Функція *WCF* фактично приймає за нульовий вклад значень спектральних коефіцієнтів Уолша – Адамара та враховує лише їх крайні значення, індекси яких за модулем більші ніж значення *end*. Наочно це представлено на рис. 6, який отримано зі значень розподілу, наведених на рис. 3. Тут застосовано обмеження, які використовуються в підрахунку функції *WCF* та представлено у логарифмічному масштабі.

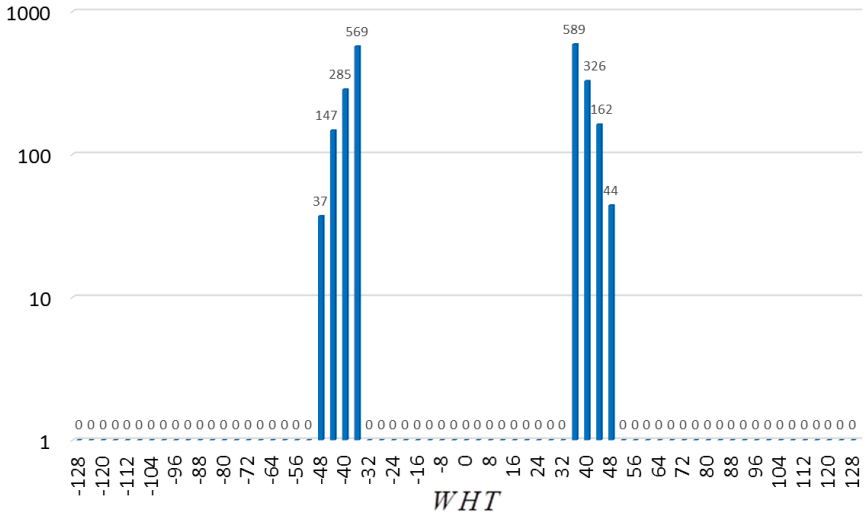


Рис. 6. Розподіл значень спектральних коефіцієнтів Уолша – Адамара які враховуються у функції *WCF* для отриманого бієктивного S-блоку з нелінійністю $N_f = 104$ (приклад)

Розрахунок функції (2) для наведеного прикладу буде проводитися наступним чином:

$$WCF = \sum_{b=1}^{255}\sum_{i=0}^{255}\prod_{\substack{j=start\\ j+=step}}^{end} \| WHT[b,i] | - j | =$$

$$= 37\cdot\left[\left(|-48|-0\right)\cdot\left(|-48|-4\right)\cdot\left(|-48|-8\right)\cdot\left(|-48|-12\right)\cdot\left(|-48|-16\right)\cdot\right.$$
$$\left.\cdot\left(|-48|-20\right)\cdot\left(|-48|-24\right)\cdot\left(|-48|-28\right)\cdot\left(|-48|-32\right)\right]+$$
$$+147\cdot\left[\left(|-44|-0\right)\cdot\left(|-44|-4\right)\cdot\left(|-44|-8\right)\cdot\left(|-44|-12\right)\cdot\left(|-44|-16\right)\cdot\right.$$
$$\left.\cdot\left(|-44|-20\right)\cdot\left(|-44|-24\right)\cdot\left(|-44|-28\right)\cdot\left(|-44|-32\right)\right]+$$
$$+285\cdot\left[\left(|-40|-0\right)\cdot\left(|-40|-4\right)\cdot\left(|-40|-8\right)\cdot\left(|-40|-12\right)\cdot\left(|-40|-16\right)\cdot\right.$$
$$\left.\cdot\left(|-40|-20\right)\cdot\left(|-40|-24\right)\cdot\left(|-40|-28\right)\cdot\left(|-40|-32\right)\right]+$$
$$+569\cdot\left[\left(|-36|-0\right)\cdot\left(|-36|-4\right)\cdot\left(|-36|-8\right)\cdot\left(|-36|-12\right)\cdot\left(|-36|-16\right)\cdot\right.$$
$$\left.\cdot\left(|-36|-20\right)\cdot\left(|-36|-24\right)\cdot\left(|-36|-28\right)\cdot\left(|-36|-32\right)\right]+$$
$$+589\cdot\left[\left(|36|-0\right)\cdot\left(|36|-4\right)\cdot\left(|36|-8\right)\cdot\left(|36|-12\right)\cdot\left(|36|-16\right)\cdot\right.$$
$$\left.\cdot\left(|36|-20\right)\cdot\left(|36|-24\right)\cdot\left(|36|-28\right)\cdot\left(|36|-32\right)\right]+$$
$$+326\cdot\left[\left(|40|-0\right)\cdot\left(|40|-4\right)\cdot\left(|40|-8\right)\cdot\left(|40|-12\right)\cdot\left(|40|-16\right)\cdot\right.$$
$$\left.\cdot\left(|40|-20\right)\cdot\left(|40|-24\right)\cdot\left(|40|-28\right)\cdot\left(|40|-32\right)\right]+$$
$$+162\cdot\left[\left(|44|-0\right)\cdot\left(|44|-4\right)\cdot\left(|44|-8\right)\cdot\left(|44|-12\right)\cdot\left(|44|-16\right)\cdot\right.$$
$$\left.\cdot\left(|44|-20\right)\cdot\left(|44|-24\right)\cdot\left(|44|-28\right)\cdot\left(|44|-32\right)\right]+$$
$$+44\cdot\left[\left(|48|-0\right)\cdot\left(|48|-4\right)\cdot\left(|48|-8\right)\cdot\left(|48|-12\right)\cdot\left(|48|-16\right)\cdot\right.$$
$$\left.\cdot\left(|48|-20\right)\cdot\left(|48|-24\right)\cdot\left(|48|-28\right)\cdot\left(|48|-32\right)\right] = 4\ 003\ 221\ 743\ 861\ 760.$$

Отримали значення $WCF = 4\ 003\ 221\ 743\ 861\ 760$, що відповідає останньому значенні (при $k = 117$) на рис. 5.

З наведеного прикладу розрахунків бачимо:

1) Спектральні коефіцієнти Уолша – Адамара з більш великими абсолютними значеннями мають значно більшу вагу ніж їх «сусідній» менший коефіцієнт. Наприклад, збільшення на одне значенням кількості спектральних коефіцієнтів зі значенням 48 урівноважується зменшенням кількості спектральних коефіцієнтів зі значенням 44 на 4 одиниць, або зі значенням 40 на 22 одиниці, або зі значенням 36 на 220 одиниць;

2) На відміну від функції вартості *WHS*, яку було запропоновано Кларком у роботі [15], функція *WCF* не враховує центральні значення у розподілі спектру. Тобто, навить дуже значні зміни в розподілі WHT, значення яких менш ніж end, не будуть враховані у функції *WCF*;

3) Має значення не лише максимальне значення спектру коефіцієнтів Уолша – Адамара, а й наступні за максимальними значеннями. Так, з двох S-блоків, які мають однакові максимальні значення спектру коефіцієнтів Уолша – Адамара, для наступного пошуку буде обраний той S-блок, який має менші значення інших значень спектру коефіцієнтів;

4) Значення функції *WCF* дуже швидко зростає. Наприклад, при обранні $end = 28$ значення функції *WCF* випадково сформованого S-блоку складає близько $1\cdot10^{15}$, при $end = 32$ близько $2\cdot10^{16}$, при $end = 36$ близько $5\cdot10^{17}$, а вже при $end = 40$ значення функції WCF

перевищує 64-бітне значення (який охоплює діапазон від -9 223 372 036 854 775 808 до 9 223 372 036 854 775 807) та потребує застосування більш довгої арифметики, що потенційно зменшує продуктивність роботи алгоритму пошуку.

Результати дослідження та оптимізації

Модифікація функції WCF

Для зменшення швидкості зростання функції *WCF* та можливість її застосування для $end \geq 40$ з 64-бітними цілими числами, враховуючи кратність спектру коефіцієнтів Уолша – Адамара чотирьом, можна зменшити кожний множник у чотири рази. Програмно це можна виконати побітним зсувом чисел без якісної зміни поводження функції *WCF*. Тобто у подальшому будемо досліджувати модифіковану функцію вартості виду

$$WCF = \sum_{b=1}^{255} \sum_{i=0}^{255} \prod_{\substack{j=start \\ j+=step}}^{end} \frac{1}{4} \cdot \left| \left| WHT[b,i] \right| - j \right|. \qquad (3)$$

Наведена модифікація зменшує значення *WCF* у $4^{(end-start)/step}$ рази. При цьому значення функції (4) для випадково сформованого S-блоку буде складати:

- для параметру $end = 28$ близько $1 \cdot 10^{10}$,
- для параметру $end = 32$ близько $1 \cdot 10^{11}$,
- для параметру $end = 36$ близько $5 \cdot 10^{11}$,
- для параметру $end = 40$ близько $5 \cdot 10^{12}$,
- для параметру $end = 44$ близько $1 \cdot 10^{13}$,
- для параметру $end = 48$ близько $5 \cdot 10^{13}$,
- для параметру $end = 52$ близько $1 \cdot 10^{14}$,
- для параметру $end = 56$ близько $5 \cdot 10^{14}$.

Задавати значення $end > 48$ практичного сенсу немає, так як це буде відповідати $N(S) < 128 - 48/2 = 104$, тобто для $N(S) = 104$ значення функції вартості *WCF*=0.

Дослідження впливу параметру *end*

Для проведення досліджень впливу параметрів на значення функції вартості (3) здійснено тестування. При цьому параметр *end* змінювали у діапазоні від 0 до 48 з шагом 4. Параметри $start = 0$ та $step = 4$ змінювати не має сенсу через значення, які може приймати спектр коефіцієнтів Уолша – Адамара.

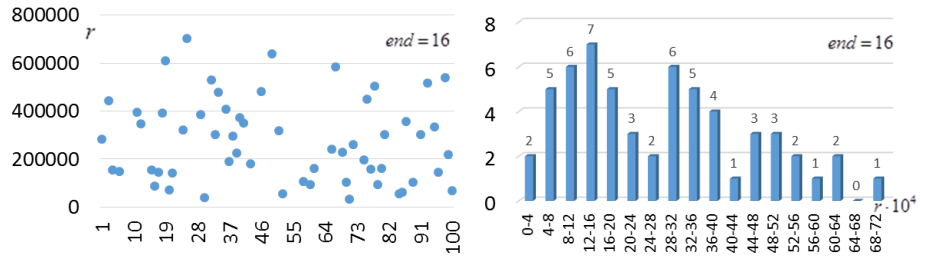
Всього було проведено 100 іспитів (окремих запусків програми для знаходження цільового S-блоку) для кожного значення *end*. Для кожної серії іспитів розраховували:

- кількість вдалих іспитів, тобто випадків знаходження цільового S-блоку (бієктивної 8-бітної підстановки з нелінійністю $N(S) = 104$);
- кількість ітерацій до знаходження цільового S-блоку (що є пропорційним до часу, затраченого на пошук);
- послідовність змін прийнятих значень функції *WCF* у алгоритмі пошуку та поточне значення $N(S)$.

На рис. 7 – 14 наведено результати тестування:

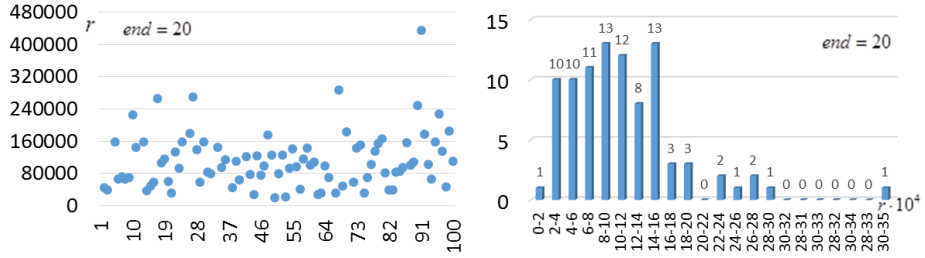
- *а* – кількість ітерацій r, які біло виконано в кожному іспиті, до знаходження цільового S-блоку;
- *б* – розподіл кількості ітерацій r.

Позначимо середнє значення кількість ітерацій символом r^{aver}. Узагальнені результати тестування наведено у табл. 1.



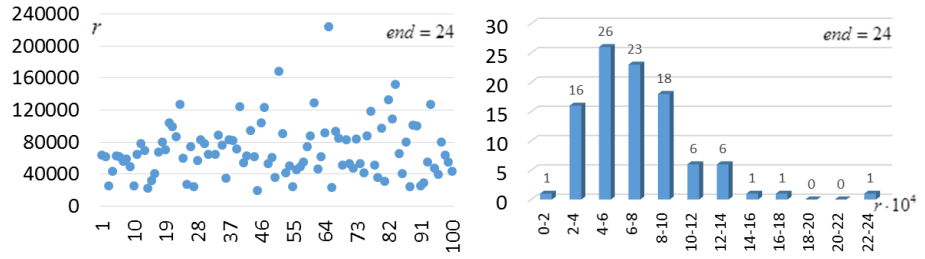
а *б*

Рис. 7. Результати тестування алгоритму Hill climbing з функцією вартості WCF, $end = 16$



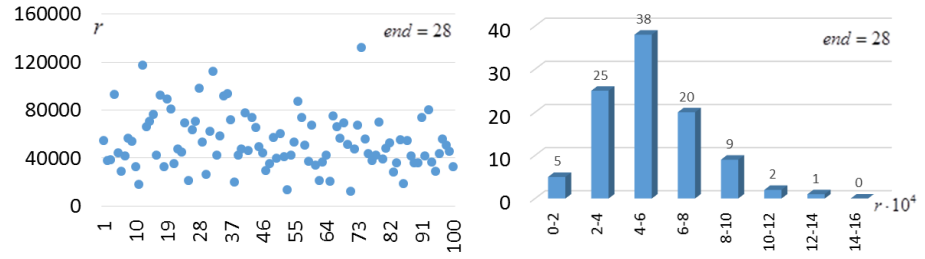
а *б*

Рис. 8. Результати тестування алгоритму Hill climbing з функцією вартості WCF, $end = 20$



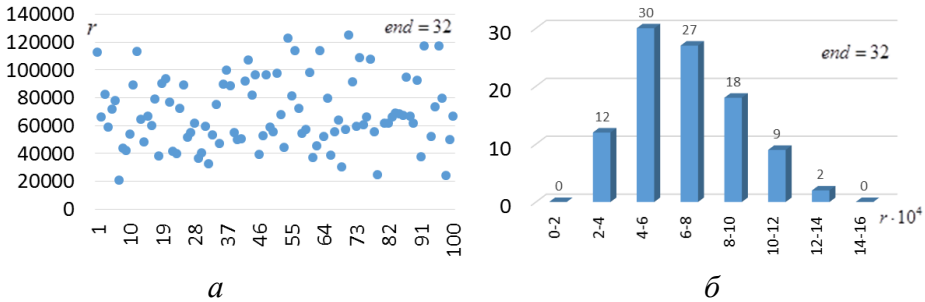
а *б*

Рис. 9. Результати тестування алгоритму Hill climbing з функцією вартості WCF, $end = 24$



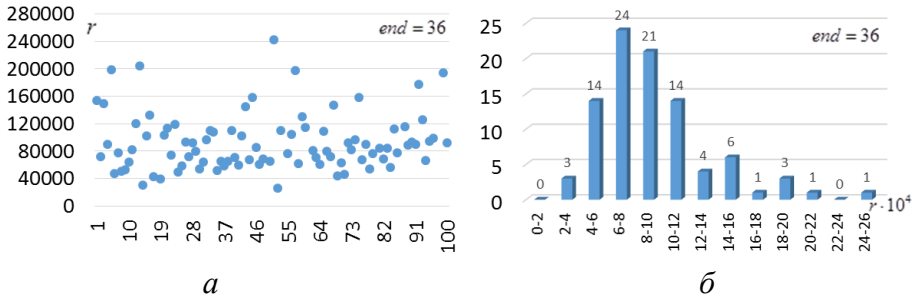
а *б*

Рис. 10. Результати тестування алгоритму Hill climbing з функцією вартості WCF, $end = 28$



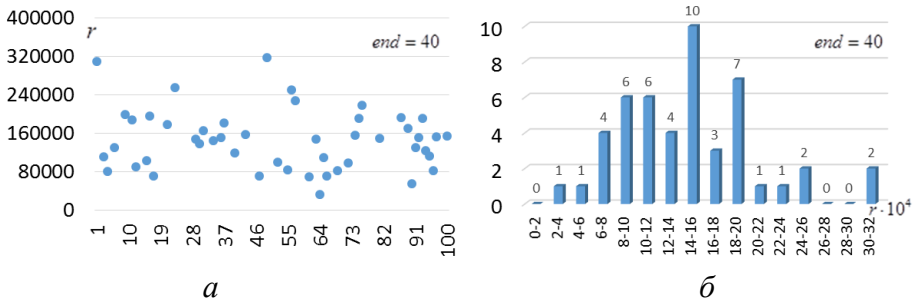
а *б*

Рис. 11. Результати тестування алгоритму Hill climbing з функцією вартості WCF, $end = 32$



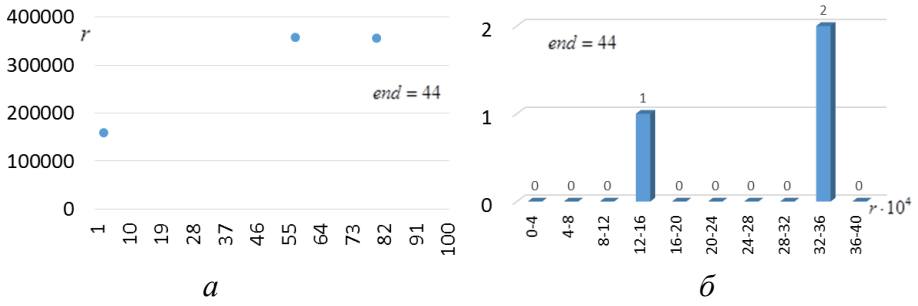
а *б*

Рис. 12. Результати тестування алгоритму Hill climbing з функцією вартості WCF, $end = 36$



а *б*

Рис. 13. Результати тестування алгоритму Hill climbing з функцією вартості WCF, $end = 40$



а *б*

Рис. 14. Результати тестування алгоритму Hill climbing з функцією вартості WCF, $end = 44$

Таблиця 1

Узагальнені результати тестування алгоритму Hill climbing із функцією вартості WCF для різних значень *end*

end	Кількість знайдених S-блоків	Середня кількість ітерацій (r^{aver})
0	0	–
4	0	–
8	0	–
12	0	–
16	58	276 380
20	91	110 770
24	99	69 344
28	100	53 160
32	98	68 855
36	92	92 709
40	48	146 074
44	3	291 568
48	0	–

Обговорення результатів

За результатами тестування отримали суттєве прискорення при формуванні цільових підстановок. Зокрема, у порівнянні із кращим відомим на сьогоднішній день результатом було суттєво зменшено середню кількість ітерацій.

Значення $end = 32$ відповідає випадку функції вартості, яку було запропоновано та досліджено у [8, 9]. За результатом тестування алгоритму Hill climbing у [8] отримано середню кількість ітерацій $r^{aver} = 70{,}596$. В [9] тими ж авторами опубліковано кращий результат, який складає 65,933 ітерацій. Наша оцінка з табл. 1 для $end = 32$ дає середню кількість 68,855 ітерацій, що є близьким до значень із [8, 9]. Отже цей результат вважаємо підтвердженим. Однак з отриманих результатів (табл. 1) бачимо, що найменша кількість виконаних ітерації досягається при $end = 28$. При цьому, в середньому необхідно виконати лише 53,160 ітерації. Це майже на 20 % краще, ніж для результатів із [8, 9]. Крім того, ми значно покращили частоту формування цільових підстановок. За результатами тестування в [8] тільки в 11 випадках із 30 незалежних експериментів було знайдено S-блок з нелінійністю 104. Для наших налаштувань успіх було досягнуто в 100 % випадках.

Аналізуючи другий стовпчик в табл. 1, також бачимо, що для інших значень параметру end кількість знайдених S-блоків зменшується. Однак це відбувається не тому, що алгоритм не спроможний знайти рішення, а тому, що виконується умова виходу при досягненні обраного критерію зупинки у max_frozen_outer_loops=5. На рис. 15 та 16 наведено приклади послідовної зміни значень функції вартості WCF та відповідні значення нелінійності $N(S)$ для $end = 28$ і $end = 40$ під час роботи алгоритму пошуку. Як бачимо, в середньому, під час роботи алгоритму пошуку виконується від 100 до 150 покращень значень функції вартості WCF.

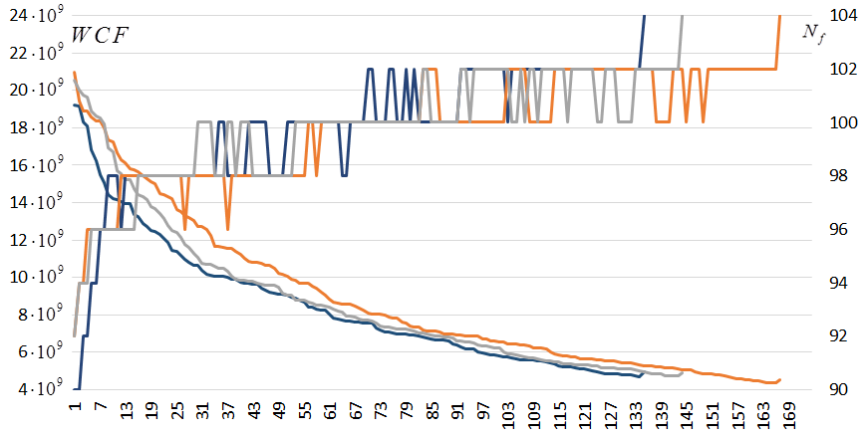


Рис. 15. Послідовність зміни значень WCF та $N(S)$, які фіксувалися при кожному покращенні значенні функції вартості WCF, $end = 28$

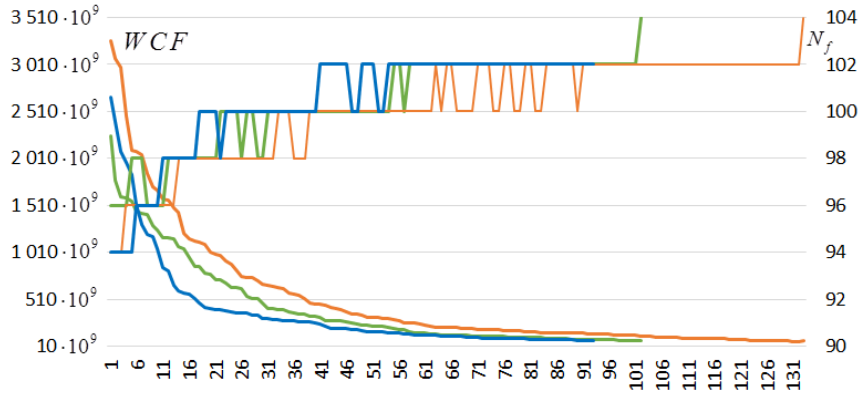


Рис. 16. Послідовність зміни значень WCF та $N(S)$, які фіксувалися при кожному покращенні значенні функції вартості WCF, $end = 40$

Висновки

У цій роботі досліджено можливість формування високонелінійних S-блоків за допомогою простого за реалізацією евристичного алгоритму сходження на пагорб. У якості функції вартості ми застосовували *WCF*.

За результатами тестування перевірено та підтверджено результати, які опубліковано у [8, 9]. Зокрема підтверджуємо, що функція вартості *WCF* дійсно дозволяє значно прискорити формування високонелінійних підстановок. При застосуванні алгоритму Hill climbing нами отримано середнє значення кількості ітерацій 68,855, що є близьким до опублікованих у [8, 9] результатів (65,933 та 70,596 відповідно).

Слід зазначити, що в [8, 9] застосовувався фіксований параметр $end = 32$. В цій роботі було модифіковано функцію вартості *WCF* та проведено розширене тестування для різних значень end. За результатами тестування кращим параметрам було визначено значення $end = 28$, при якому у 100 % (з проведених випробувань) було знайдено бієктивний S-блок з нелінійністю 104. При цьому середня кількість ітерацій алгоритму Hill climbing складала 53 160 ітерацій. Це майже на 20 % покращує відомий із [8, 9] результат.

Список літератури:

1. Freyre Echevarría A. Evolución híbrida de s-cajas no lineales resistentes a ataques de potencia. 2020.
2. McLaughlin J. Applications of search techniques to cryptanalysis and the construction of cipher components: phd. University of York, 2012.
3. Álvarez-Cubero J. Vector Boolean Functions: applications in symmetric cryptography. 2015.
4. Bard G.V. Algebraic Cryptanalysis. Boston, MA: Springer US, 2009.
5. Courtois N.T., Bard G.V. Algebraic Cryptanalysis of the Data Encryption Standard // Cryptography and Coding / ed. Galbraith S.D. Berlin, Heidelberg: Springer, 2007. P. 152–169.
6. Rodinko M., Oliynykov R., Gorbenko Y. Optimization of the High Nonlinear S-Boxes Generation Method // Tatra Mountains Mathematical Publications. Sciendo, 2017. Vol. 70, № 1. P. 93–105.
7. Kuznetsov A.A. et al. Stream Ciphers in Modern Real-time IT Systems. Cham: Springer Nature, 2022. 593 p.
8. Freyre-Echevarría A. et al. An External Parameter Independent Novel Cost Function for Evolving Bijective Substitution-Boxes: 11 // Symmetry. Multidisciplinary Digital Publishing Institute, 2020. Vol. 12, № 11. P. 1896.
9. Freyre Echevarría A., Martínez Díaz I. A new cost function to improve nonlinearity of bijective S-boxes. 2020.
10. Kuznetsov A. et al. Optimizing the Local Search Algorithm for Generating S-Boxes // 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S T). 2021. P. 458–464.
11. Burnett L.D. Heuristic Optimization of Boolean Functions and Substitution Boxes for Cryptography: phd. Queensland University of Technology, 2005.
12. Ivanov G., Nikolov N., Nikova S. Cryptographically Strong S-Boxes Generated by Modified Immune Algorithm // Cryptography and Information Security in the Balkans / ed. Pasalic E., Knudsen L.R. Cham: Springer International Publishing, 2016. P. 31–42.
13. Freyre-Echevarría A. et al. Evolving Nonlinear S-Boxes With Improved Theoretical Resilience to Power Attacks // IEEE Access. 2020. Vol. 8. P. 202728–202737.
14. Kazymyrov O., Kazymyrova V., Oliynykov R. A Method For Generation Of High-Nonlinear S-Boxes Based On Gradient Descent: 578. 2013.
15. Clark J.A., Jacob J.L., Stepney S. The design of S-boxes by simulated annealing // New Gener Comput. 2005. Vol. 23, № 3. P. 219–231.
16. McLaughlin J. Applications of search techniques to cryptanalysis and the construction of cipher components: phd. University of York, 2012.
17. Wang J. et al. Construction Method and Performance Analysis of Chaotic S-Box Based on a Memorable Simulated Annealing Algorithm: 12 // Symmetry. Multidisciplinary Digital Publishing Institute, 2020. Vol. 12, № 12. P. 2115.
18. Kuznetsov A. et al. WHS Cost Function for Generating S-boxes // 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S T). 2021. P. 434–438.
19. Ivanov G., Nikolov N., Nikova S. Reversed genetic algorithms for generation of bijective s-boxes with good cryptographic properties // Cryptogr. Commun. 2016. Vol. 8, № 2. P. 247–276.
20. Kapuściński T., Nowicki R.K., Napoli C. Application of Genetic Algorithms in the Construction of Invertible Substitution Boxes // Artificial Intelligence and Soft Computing / ed. Rutkowski L. et al. Cham: Springer International Publishing, 2016. P. 380–391.

21. Mariot L., Leporati A. Heuristic Search by Particle Swarm Optimization of Boolean Functions for Cryptographic Applications // Proceedings of the Companion Publication of the 2015 Annual Conference on Genetic and Evolutionary Computation. New York, NY, USA: Association for Computing Machinery, 2015. P. 1425–1426.
22. Picek S., Cupic M., Rotim L. A New Cost Function for Evolution of S-Boxes // Evolutionary Computation. 2016. Vol. 24, № 4. P. 695–718.
23. Clark A.J. Optimisation heuristics for cryptology: phd. Queensland University of Technology, 1998.
24. Cusick T., Stănică P. Cryptographic Boolean Functions and Applications: Second edition // Cryptographic Boolean Functions and Applications: Second Edition. 2017. P. 2751 p.

Надійшла до редколегії 05.03.2022

Відомості про авторів:

Кузнецов Олександр Олександрович – 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: kuznetsov@karazin.ua, ORCID: https://orcid.org/0000-0003-2331-6326

Горбенко Юрій Іванович – канд. техн. наук, Харківський національний університет імені В.Н. Каразіна, старший науковий співробітник кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук; Україна; e-mail: gorbenkou@iit.kharkov.ua, ORCID: https://orcid.org/0000-0002-0652-8629

Полуяненко Микола Олександрович – канд. техн. наук, Харківський національний університет імені В.Н. Каразіна, доцент кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук; Україна; e-mail: nlfsr01@gmail.com, ORCID: https://orcid.org/0000-0001-9386-2547

Кандій Сергій Олегович – АТ «Інститут інформаційних технологій», технік-конструктор, Україна; e-mail: sergeykandy@gmail.com, ORCID: https://orcid.org/0000-0003-0552-8341

Матвєєва Євгенія Дмитрівна – Харківський національний університет імені В.Н. Каразіна, студент кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук; Україна; e-mail: belka.j.0507@gmail.com, ORCID: https://orcid.org/0000-0001-9834-2970

УДК 004.056.5 **DOI:10.30837/rt.2022.2.209.03**

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

ПОРІВНЯННЯ ЯКОСТІ АЛГОРИТМІВ СЕМПЛУВАННЯ З ДИСКРЕТНОГО НОРМАЛЬНОГО РОЗПОДІЛУ НА NTRU РЕШІТКАХ

Вступ

Постквантова криптографія є напрямом досліджень, що вивчає криптографічні перетворення, які захищені від атак з використанням квантових комп'ютерів. У 2016 році NIST США оголосив про початок конкурсу NIST PQC, метою якого є створення нових постквантових криптографічних стандартів. Наразі триває третій фінальний етап цього конкурсу. Згідно з аналізом спеціалістів NIST [5], одним з перспективних напрямів у постквантовій криптографії є криптографія на алгебраїчних решітках. У звіті [4] зазначається, що NIST планує стандартизувати хоча б один електронний підпис (ЕП) на решітках. Серед електронних підписів фіналістами, які є представниками криптографії на решітках, є CRYSTALS-Dilithium [2] та Falcon[3].

Falcon є підписом типу Hash-and-Sign [6] на основі решіток. У схемах такого роду ключ підпису є «гарним» уявленням решітки, одностороння функція з підказкою, що дає можливість, враховуючи довільну точку в «навколишньому просторі», знайти точки решітки, які є відносно близькими до неї (тобто розв'язати задачу апроксимації найближчого вектора, ApproxCVP); ключ перевірки, з іншого боку, є «поганим» уявленням: він дозволяє будь-кому перевірити, чи є точка в решітці, але не вирішити ApproxCVP. Для того щоб підписати повідомлення, спочатку обчислюється геш, що відображає повідомлення на випадкову точку в навколишньому просторі, а підпис є точкою решітки, близькою до неї, отриманою за допомогою односторонньої функції з підказкою. Щоб перевірити підпис, перевіряється, що підпис є точкою решітки і достатньо близько до геш значення повідомлення.

Для ранніх конструкцій за цим напрямком, такі як схема підпису GGH та NTRUSign [6, 7] виявилося, що вони є небезпечними через поширену критичну вразливість: точки решітки, отримані як підписи, призводять до витоку інформації про односторонню функцію з лазівкою, що використовувалася для їх обчислення, і ця функція може бути відновлена з використанням статистичних методів [7]. Один із кандидатів у першому раунді NIST був фактично зламаний з використанням такої ж ідеї [5].

Таким чином, для безпеки дуже важливо довести, що вибірка підписів здійснюється відповідно до розподілу, що статистично не залежить від односторонньої функції з лазівкою. Першим підходом до цього залишається фреймворк GPV [6]: генерується вирішення задачі ApproxCVP відповідно до дискретного гаусового розподілу з центром у цільовій точці з коваріацією, незалежною від односторонньої функції з лазівкою (зазвичай сферичної).

Загальна структура підписів GPV може сильно відрізнятися залежно від решіток, над якими вони створюються, конструкцій односторонніх функцій з лазівкою і алгоритмів гаусової вибірки, на які вони спираються. Досягнутий рівень безпеки за такою схемою по суті визначається якістю односторонньої функції з лазівкою і алгоритмом вибірки. Якість визначена як мінімальне стандартне відхилення, досяжне в гаусовій вибірці, при збереженні статистичної незалежності виходу.

Метою цієї статті є порівняння якості алгоритмів семплування на решітках. Зокрема, в роботі розглянуто алгоритми Клейна (його модифікацю – алгоритм Преста та Дукаса [3]), алгоритм Пейкерта [7] та алгоритм семплування без використання арифметики з плаваючою крапкою [8].

1. Попередні визначення

Для будь-якого $a \in \mathbb{R}$ задамо $[a]_q = \lfloor aq \rceil / q \in (1/q)\mathbb{Z}$. Через A^t позначимо транспонування будь-якої матриці A. Нехай $s_1(A) = \max_{x \neq 0} \frac{\|Ax\|}{\|x\|}$ – найбільше сингулярне значення A. Нехай $\Sigma \in \mathbb{R}^{n \times n}$ – симетрична матриця. Матриця є позитивно визначеною якщо для будь-якого $x \in \mathbb{R}^n$ виконується $x^t \Sigma x > 0$. Позитивна матриця позначається як $\Sigma \succ 0$. Якщо $\Sigma_1 - \Sigma_2 \succ 0$, то це позначається як $\Sigma_1 \succ \Sigma_2$. $\Sigma \succ 0$ тоді і тільки тоді, коли $\Sigma^{-1} \succ 0$ та $\Sigma_1 \succ \Sigma_2 \succ 0$ тоді і тільки тоді, коли $\Sigma_2^{-1} \succ \Sigma_1^{-1} \succ 0$. Решітка $\mathbf{\Lambda}$ є дискретною адитивною підгрупою евклідового простору. Коли простір $\mathbb{R}^m$, то решітка може бути задана базисом $\Lambda(B) = \{Bx | x \in \mathbb{Z}^d\}$. Якщо B є повноранговою, то d є рангом решітки. Об'єм решітки $\mathbf{\Lambda}$ – $Vol(\Lambda) = \det(B^t B)^{\frac{1}{2}}$ для будь-якого базиса B.

Нехай $d = 2^l$ для деякого $l \geq 1$ та ζ_d буде $2d$-й примітивний корінь з 1. Тоді для фіксованого d буде $\mathcal{K} := \mathbb{Q}(\zeta_d)$ – d-е циклотомічне кільце та кільце його алгебраїчних цілих $\mathcal{R} := \mathbb{Z}[\zeta_d]$. Автоморфізм поля $\zeta_d \mapsto \zeta_d^{-1} = \overline{\zeta_d}$ відповідає комплексному спряженню та f^* є зображенням f у цьому автоморфізмі. Ми маємо $\mathcal{K} \simeq \mathbb{Q}[x]/(x^d + 1)$, $\mathcal{R} \simeq \mathbb{Z}[x]/(x^d + 1)$, $\mathcal{K}_\mathbb{R} := \mathcal{K} \otimes \mathbb{R} \simeq \mathbb{R}[x]/(x^d + 1)$. Кожне $f = \sum_{i=0}^{d-1} f_i \zeta_d^i \in \mathcal{K}_\mathbb{R}$ може бути ідентифіковане вектором коефіцієнтів $(f_0, \dots, f_{d-1}) \in \mathbb{R}^d$. Операція доповнення може бути розширена на $\mathcal{K}_\mathbb{R}$ та $\mathcal{K}_\mathbb{R}^+$ – підпростір елементів, для яких виконується $f^* = f$.

Циклотомічне поле $\mathcal{K}$ асоційоване з d комплексними вкладеннями $\varphi_i : \mathcal{K} \to \mathbb{C}$, які відображають поліном f до його значення в точках ζ_d з непарними індексами. Це відображення визначає канонічне вкладення $\varphi(f) := (\varphi_1(f), \dots, \varphi_d(f))$. Воно легко узагальнюється на $\mathcal{K}_\mathbb{R}$ та визначає простір $\mathcal{H} = \{v \in \mathbb{C}^d : v_i = \overline{v_{\frac{d}{2}+i}}, 1 \leq i \leq \frac{d}{2}\}$. Зауважимо, що $\varphi(fg) = \left(\varphi_i(f)\varphi_i(g)\right)_{i \leq d}$. За потреби це вкладення поширюється на вектори або матриці над $\mathcal{K}_\mathbb{R}$. Через $\mathcal{K}_\mathbb{R}^{++}$ позначимо підмножину $\mathcal{K}_\mathbb{R}^+$, яка має усі додатні коефіцієнти в канонічному вкладенні.

NTRU решітки є вільними $\mathcal{R}$-модулями ранга 2 в $\mathcal{K}^2$, або іншими словами групи форми $\mathcal{R}x + \mathcal{R}y$, де $x = (x_1, x_2), y = (y_1, y_2)$ натягнуто на $\mathcal{K}^2$. Існує природна білінійна форма над $\mathcal{K}^2$, що визначена як $\langle x, y \rangle_\mathcal{K} := x_1^* y_1 + x_2^* y_2 \in \mathcal{K}$. Може бути показано, що для всіх $x \in \mathcal{K}^2, \langle x, y \rangle_\mathcal{K} \in \mathcal{K}_\mathbb{R}^{++}$. Ця форма супроводжується відповідним поняттям ортогональності. Зокрема, процедура ортогоналізації Грама – Шмідта для пари лінійно незалежних векторів $b_1, b_2 \in \mathcal{K}^2$ визначена наступним чином:

$$\tilde{b_1} := b_1, \tilde{b_2} := b_2 - \frac{(b_1, b_2)_\mathrm{K}}{(b_1, b_1)_\mathrm{K}} \tilde{b_1} \tag{1}$$

Легко перевірити, що $\langle \widetilde{b_1}, \widetilde{b_2} \rangle_\mathcal{K} = 0$. Матриця Грама – Шмідта з стовбцями $\widetilde{b_1}, \widetilde{b_2}$ позначена як $\tilde{B}$ та ми маємо $det\tilde{B} = detB$. Для $\Sigma \in \mathcal{K}_\mathbb{R}^{2 \times 2}$ через Σ^* позначимо комплексно спряжену та транспоновану матрицю у $\mathcal{K}_\mathbb{R}$.

Функція Гауса над $\mathbb{R}^d$ з центром c та матрицею коваріації $\Sigma \succ 0$ визначена як $\rho_{c,\Sigma}(x) = \exp\left(-\frac{1}{2}(x - c)^t \Sigma (x - c)\right)$. Якщо $\Sigma = s^2 I_d$, то $\rho_{c,s} = \exp\left(-\frac{\|x-c\|^2}{2s^2}\right)$ та називається сферичною гаусовською функцією. Нормальний розподіл $\mathcal{N}_\Sigma$ з матрицею коваріації $\mathbf{\Sigma}$ має функцію розподілу $((2\pi)^d det\Sigma)^{-1/2} \rho_{0,\Sigma}$. Під $\mathcal{N}_{\mathcal{K}_\mathbb{R},s}$ мається на увазі розподіл $(z_1, \dots, z_d) \leftarrow \left(\mathcal{N}_{\frac{s}{\sqrt{d}}}\right)^d$. Дискретний розподіл Гауса над решіткою $\mathbf{\Lambda}$ з центром c та матрицею коваріації $\mathbf{\Sigma}$ визначений як

$$\forall x \in \Lambda, \mathrm{D}_{\Lambda,c,\Sigma(x)} = \frac{\rho_{c,\Sigma}(x)}{\rho_{c,\Sigma}(\Lambda)} \tag{2}$$

Параметр згладжування η_ε решітки Λ для деякого ε визначений як

$$\eta_\varepsilon(\Lambda) = \min\left\{ s > 0 : \rho_{\frac{1}{s}}\left(\Lambda^\vee\right) \le 1+\varepsilon \right\}, \tag{3}$$

де $\Lambda^\vee$ – дуальна решітка. Обмеження на параметр зглажування надає наступна лемма:

Лемма 1 ([3,7]) Нехай $B\mathcal{R}^2$ є вільним $\mathcal{R}$-модулем та нехай $\Lambda = M(B)\mathbb{Z}^{2d}$ буде асоційованою решіткою в $\mathbb{R}^{2d}$. Тоді для всіх $\varepsilon > 0$ маємо

$$\eta_\varepsilon(\Lambda) \le |B|_{\mathrm{K}} \sqrt{\frac{\log\left(2d\left(1+\frac{1}{\varepsilon}\right)\right)}{2\pi^2}}. \tag{4}$$

2. Алгоритм семплування Пейкерта

У [6] Пейкертом запропоновано алгоритм для семплування з дискретного гаусовського розподілу для заданої решітки з використанням невеликого гаусовського шуму. Фактично цей алгоритм можливо описати як рандомізовану версію алгоритму округлення Бабаї з використанням випадкового шуму, що розподілений за розподілом Гауса для того, щоб приховати структуру решітки. Алгоритм може бути визначений у термінах алгебри $\mathcal{K}_{\mathbb{R}}$, що показано на рис. 1.

Алгоритм семплування Пейкерта

Вхідні данні: матриця $B \in \mathcal{K}_{\mathbb{R}}^{2\times 2}$ та центральний вектор $c \in \mathcal{K}_{\mathbb{R}}^{2}$
Вихідні данні: $z \in \Lambda$ з розподілом близьким до гаусовсткого
Параметри алгоритма: параметр $r \ge \eta_\varepsilon(\mathcal{R}^2)$ та $\Sigma_0 \in \mathcal{K}_{\mathbb{R}}^{2\times 2}$ для якої $\Sigma_0\Sigma_0^* = \Sigma - r^2 BB^*$
$x \leftarrow \Sigma_0\left(\mathcal{N}_{\mathcal{K}_{\mathbb{R}},1}\right)^2$ $z \leftarrow \lceil B^{-1}(c-x) \rfloor_r$ Повернути Bz

Рис. 1. Алгоритм семплування Пейкерта

Коли $\Sigma \succ r^2 BB^*$, то існування Σ_0 гарантоване. Якість семплування можливо оцінити наступним чином:

Теорема 1 [8]. Позначимо розподіл ймовірностей на виході алгоритму семплування Пейкерта як $\mathcal{D}$. Якщо $\varepsilon \le \frac{1}{2}$ та $\sqrt{\Sigma} \ge s_1(B)\eta_\varepsilon(\mathcal{R}^2)$, то статистична відстань між $\mathcal{D}$ та $\mathcal{D}_{\Lambda,c,\Sigma}$ обмежена 2ε. Більш того,

$$\sup_{x\in B\mathrm{R}^2} \left| \frac{\mathrm{D}(x)}{\mathrm{D}_{\Lambda(B),c,\Sigma}(x)} - 1 \right| \le 4\varepsilon \tag{5}$$

На практиці параметр коваріації є скалярним кратним тотожної матриці або позитивною дійсною константою.

3. Алгоритми семплування Кляйна та Дукаса і Преста.

У роботі [3] запропоновано гібридний алгоритм для семплування з дискретного гаусовського розподілу для заданої решітки. На високому рівні цей гібридний семплер дотримується підходу Кляйна, який є рандомізованою версією алгоритму найближчої площини Бабаї. У контексті кільця виконується підпрограма рандомізації «на рівні кільця», а не «на рівні цілих чисел». Щоб приховати структуру решітки, також використовується шум, але його розподіл тепер залежить від цільового центру. Алгоритм може бути описаний як зображено на рис. 2.

Алгоритм семплування Дукаса і Преста

Вхідні данні: матриця $B \in \mathcal{K}_{\mathbb{R}}^{2\times 2}$, її ортогоралізація Грама-Шмідта $\tilde{B} \in \mathcal{K}_{\mathbb{R}}^{2\times 2}$,центральний вектор $c \in \mathcal{K}_{\mathbb{R}}^{2}$, параметр σ

Вихідні данні: $z \in \Lambda$ з розподілом близьким до гаусовсткого

Параметри алгоритма: $\sigma_i := \sqrt{\frac{\sigma^2}{\langle b_i, b_i \rangle} - r^2}$

$c_2 \leftarrow c, v_2 \leftarrow 0$
$d_2 \leftarrow \frac{\langle \widetilde{b_2}, c_2 \rangle_{\mathcal{K}}}{\langle \widetilde{b_2}, \widetilde{b_2} \rangle_{\mathcal{K}}}$
$u_2 \leftarrow \mathcal{N}_{\mathcal{K}_{\mathbb{R}},1}$
$y_2 \leftarrow \sigma_2 u_2$
$x_2 \leftarrow \lfloor d_2 - y_2 \rceil_r$
$c_1 \leftarrow c_2 - x_2 b_2, v_1 \leftarrow x_2 b_2$
$d_1 \leftarrow \frac{\langle \widetilde{b_1}, c_1 \rangle_{\mathcal{K}}}{\langle \widetilde{b_1}, \widetilde{b_1} \rangle_{\mathcal{K}}}$
$u_1 \leftarrow \mathcal{N}_{\mathcal{N}_{\mathcal{K}_{\mathbb{R}},1}}$
$y_1 \leftarrow \sigma_1 u_1$
$x_1 \leftarrow \lfloor d_1 - y_1 \rceil_r$
$v_0 \leftarrow v_1 + x_1 b_1$
$return\ v_0$

Рис. 2. Алгоритм семплування Дукаса і Преста

Якість семплування можливо оцінити наступним чином:

Т е о р е м а 2 [8]. Позначимо розподіл ймовірностей на виході алгоритму семплування Дукаса і Преста як $\mathcal{D}$. Якщо $\varepsilon \leq 2^{-5}$ та$\sqrt{\Sigma} \geq s_1(B)\eta_\varepsilon(\mathcal{R}^2)$, то статистична відстань між $\mathcal{D}$ та $\mathcal{D}_{\Lambda,c,\Sigma}$ обмежена 7ε. Більш того,

$$\sup_{x\in BR^2} \left| \frac{\mathrm{D}(x)}{\mathrm{D}_{\Lambda(B),c,\Sigma}(x)} - 1 \right| \leq 14\varepsilon \qquad (6)$$

4. Алгоритм семплування без використання обчислень з плаваючою крапкою

Великим недоліком алгоритма семплування Дукаса і Преста є використання обчислень з плаваючою крапкою, що значно ускладнює криптоаналіз та реалізацію. В роботі [8] запропонований алгоритм семплування, що поєднує алгоритми Пайкерта, Дукаса і Преста та дозволяє семплувати значення з гаусовського розподілу без використання обчислень з пла-

ваючою крапкою за допомогою техніки з роботи [9], в якій було показано як генерувати малий шум за допомогою розкладу Холецького виключно за допомогою цілочисельних обчислень. Розклад Холецького полягає у тому, що можливо представити матрицю у вигляді добутку верхньотрикутної матриці з додатніми елементами на діагоналі на її транспоновану версію. Якщо базис деякої решітки заданий у вигляді верхньотрикутної матриці, то можливо спростити процес семплування. На рис. 3 зображено алгоритм для такого випадку на основі алгоритма Пайкерта, що був описаний вище.

USampler (Алгоритм семплування для верхньотрикутних матриць)

Вхідні данні: верхньотрикутна матриця $U = [(1,0),(u,1)], u \in \mathcal{K}$, параметр $r > 0$

Вихідні данні: $z \in \Lambda$ з розподілом близьким до гаусовського $\mathcal{D}_{\Lambda(U),c,r}$

$z_2 \leftarrow PeikertSampler_{\mathbb{Z}}(c_2, r)$
$c_1' \leftarrow c_1 - z_2 u$
$z_1 \leftarrow PeikertSampler_{\mathbb{Z}}(c_1', r)$
$return\ z = U(z_1, z_2)$

Рис. 3. Алгоритм семплування для випадку, коли базис є верхньотрикутною матрицею

Якщо помножити вихідний вектор алгоритму USampler для відповідної матриції U на ортогоналізацію Грама – Шмідта цільового базиса, то отримаємо вектор на цільовій решітці:

$$\tilde{B}z = \tilde{B}U\left(z_1, z_2\right) = BU^{-1}U\left(z_1, z_2\right) = B\left(z_1, z_2\right) \in \Lambda. \tag{7}$$

Оскільки значення векторів після ортогоналізації Грама – Шмідта можуть мати великі знаменники, то, щоб запобігти цьому, можна використовувати апроксимацію $\hat{B} \in (1/(pq)\,\mathcal{R}^{2\times 2}$ б отриману як округлення за модулем p для B. Вплив на розподіл ймовірностей при цьому буде вимірюватися через найбільше сингулярне значення відповідної матриці Грама – Шмідта $s_1(\tilde{B})$. Алгоритм семплування, що реалізує цю ідею наведено на рис. 4.

В алгоритмі на рис. 4 матрицю A, для якої виконується

$$AA^t = p^2\left(\Sigma_p - I\right) \tag{8}$$

можливо отримати за допомогою алгоритма з роботи [9]. Використання цього алгоритма впливає на вибір параметрів алгоритму семплування, зокрема на вибір параметра s.

Алгоритм на рис. 4 використовує процедуру $OfflinePhase$. Ця процедура також пов'язана з алгоритмом генерації матриці A і адаптована для алгоритму семплування. Вона семплує вектор з розподілу $\mathcal{D}_{\mathcal{R}^2,r^2,\Sigma_p}$. Алгоритм $OfflinePhase$ зображено на рис. 5.

Для оцінки якості роботи алгоритму семплування без використання обчислень з плаваючою крапкою можливо скористатись наступною теоремою.

Теорема 3 [8]. Нехай для $\varepsilon \in (0,1)$ задано $s > s_1(\tilde{B})(1+\sqrt{2d/p})+1$ та ціле число $r \geq \eta_\varepsilon(\mathbb{Z}^{2d})$, тоді статистична відстань між $\mathcal{D}$ та $\mathcal{D}_{\Lambda(\mathrm{B}),\mathrm{c},\mathrm{sr}}$ обмежена 15ε. Більше того,

$$\sup_{x\in\Lambda(B)}\left|\frac{\mathrm{D}\left(x\right)}{\mathrm{D}_{\Lambda(B),c,\Sigma}\left(x\right)}-1\right| \leq 30\varepsilon \tag{9}$$

Алгоритм семплування без використання обчислень з плаваючою крапкою

Вхідні данні: Матриця $\hat{B} \in \mathcal{R}^{2\times 2}$, для якої виконується $\hat{B}U_{\hat{u}} = B = \hat{B}U_u$, де $\hat{u} = \lceil u \rfloor_p \in \frac{1}{p}\mathcal{R}$, центр $c \in \mathcal{R}^2$ та параметри $r, s > 0$

Вихідні данні: $z \in \Lambda$ з розподілом близьким до гаусовського $\mathcal{D}_{\Lambda(B),c,rs}$

Параметри алгоритма: $\Sigma_v = s^2 I - \hat{B}\hat{B}^t$ та матриця A, для якої виконується $AA^t = p^2(\Sigma_p - I)$

$p \leftarrow OfflinePhase(p, A)$
$\hat{c} \leftarrow \hat{B}^{-1}(c - p)$
$z' = USampler(\hat{u}, \hat{c}, s)$
$return\ z = \hat{B}z'$

Рис. 4. Алгоритм семплування без використання обчислень з плаваючою крапкою

$OfflineSampler$

Вхідні данні: ціле число $p > 0$, матриця $A \in \mathcal{R}^{2\times m}$

Вихідні данні: $p \in \mathcal{R}$ з розподілом близьким до $\mathcal{D}_{\mathcal{R}^2, r^2\Sigma}$, де $\Sigma = \frac{1}{p^2}AA^t + I$

Параметри алгоритма: цілі числа $r > \eta_\varepsilon(\mathcal{R}^2)$ та L, для якого виконується $Lr \geq \eta_\varepsilon(\Lambda(A)^\perp)$

$x \leftarrow (\lceil 0 \rfloor_{Lr})^m$
$p' \leftarrow \frac{1}{pL}Ax$
$p \leftarrow \lceil p' \rfloor_r$
$return\ p$

Рис. 5. Оффлайн фаза семплування у алгоритмі семплування без використання обчислень з плаваючою крапкою

5. Порівняння якості алгоритмів семплування для NTRU решіток

У випадку NTRU решіток, одностороння функція з лазівкою є секретний базис

$$B_{f,g} = \begin{bmatrix} f & F \\ g & G \end{bmatrix} \tag{10}$$

Стандартне відхилення дискретного гаусовського розподілу σ, що використовується з цією односторонньою функцією може бути різним і значно залежить від алгоритму семплування. У загальному випадку для NTRU решіток [3, 6] σ має вигляд

$$\sigma = \alpha\eta_{\varepsilon}\left(\mathrm{R}^{2}\right)\sqrt{q} \tag{11}$$

де фактор $\alpha \geq 1$, який є показником якості і залежить від алгоритму семплування.

Для алгоритму семплування Клейна (і відповідно Дукаса і Преста), який використовується в Falcon $\alpha\sqrt{q}$ дорівнює нормі від ортогоналізованого за Грамом – Шмідтом базисом $B_{f,g}$ [3]:

$$\alpha\sqrt{q} = \left\|B_{f,g}\right\|_{GS} = \max_{1\leq i\leq 2d}\left\|b_i^{\square}\right\|_2. \tag{12}$$

Для алгоритму семплування Пейкерта над $\mathcal{K}$ маємо [10]:

$$\alpha\sqrt{q} = \mathrm{s}_1\left(B_{f,g}\right). \tag{13}$$

І для алгоритму семплування без використання арифметики з плаваючою крапкою маємо [8]:

$$\alpha\sqrt{q} = \left|B_{f,g}\right|_{\mathrm{K}}. \tag{14}$$

У докторській роботі [10] Прест за допомогою ряду евристик визначив оптимальні асимптотичні значення для параметра α, які можливо досягти на практиці для алгоритму Клейна та алгоритму Пейкерта. Для алгоритму семплування Пейкерта оптимальне значення становить $\alpha = O(d^{\frac{1}{4}}\sqrt{\log d})$. Для алгоритму семплування Клейна (і відповідно Дукаса і Преста) маємо $\sqrt{e/2}$, тобто $\alpha = O(1)$. Для алгоритму семплування без використання аріфметики з плаваючою крапкою [8] маємо $\alpha = O(d^{1/8}\log^{1/4} d)$. У табл. 1 зведені загальні результати для алгоритмів семплування.

Таблиця 1

Порівняння якості алгоритмів семплування

Алгоритм семплування	Стандартне відхілення, що може бути досягнуто	Асимптотична оцінка параметра α
Алгоритм Пейкерта	$\sigma = s_1(B_{f,g})\eta_{\varepsilon}(\mathcal{R}^2)\sqrt{q}$	$\alpha = O(d^{\frac{1}{4}}\sqrt{\log d})$
Алгоритм Клейна (і модифікація Дукаса – Преста)	$\sigma = \left\|B_{f,g}\right\|_{GS}\eta_{\varepsilon}(\mathcal{R}^2)\sqrt{q}$	$\alpha = O(1)$
Алгоритм без використання арифметики з плаваючою крапкою	$\sigma = \left\|B_{f,g}\right\|_{\mathcal{K}}\eta_{\varepsilon}(\mathcal{R}^2)\sqrt{q}$	$\alpha = O(d^{1/8}\log^{1/4} d)$

Висновки

1. Підписи типу Hash-and-Sign на решітках зазвичай розробляються відповідно до фреймворка GPV [20] за допомогою гешування повідомлення до певного вектору та повернення як підпису точки решітки близько до цього вектору. Це робиться за допомогою «гарного» представлення решітки, яке називається односторонньою функцією з лазівкою, що дає можливість підписувачу вирішити проблему ApproxCVP з відносно невеликим фактором апроксимації. Крім того, щоб запобігти витоку інформації про секретний ключ, близькі точки решітки необхідно відбирати відповідно до статистично незалежного розподілу. Зазвичай використовується сферичний дискретний гаусовий розподіл, що заданий на решітці і має

математичне очікування у точці, що відповідає повідомленню. Для того щоб сформувати такий вектор, використовуються алгоритми семплування з гаусівського розподілу.

2. Безпека схем підпису залежить від стандартного відхилення дискретного гаусівського розподілу, який має алгоритм семплування. Чим менше стандартне відхилення, тим ближче відстань до вектора, що кодує повідомлення, і тим складніше відповідна проблема ApproxCVP, а отже, і вищий рівень безпеки. Однак існує нижня межа (залежно від односторонньої функції з лазівкою) до того, наскільки маленького стандартного відхилення може досягти алгоритм семплування, зберігаючи статистику майже близько до бажаного сферичного гаусівського розподілу, нижче якого розподіл може починати відрізнятися від розподілу Гауса способами, які могли б розкрити інформацію про односторонню функцію з лазівкою, і таким чином ставить під загрозу безпеку електронного підпису.

3. В роботі було розглянуто найбільш розповсюджені варіанти алгоритмів семплування. Якість всіх алгоритмів значно залежить від структури решітки, для якої відбувається семплування.

4. Алгоритм семплування Пейкерта був розроблений історично першим. На NTRU решітках він дає найбільш погані результати, проте його можливо використовувати як підпроцедуру у більш складних алгоритмах семплування.

5. Алгоритм семплування Клейна, зокрема його модифікація – алгоритм Дукаса – Преста, дає найменші вектори. З теоретичної точки зору він набагато кращий за алгоритм Клейна на NTRU решітках, проте він вимагає використання арифметики з плаваючою крапкою, що значно ускладнює аналіз його безпеки та створення програмної чи апаратної реалізації. Алгоритм без використання обчислень з плаваючою крапкою з теоретичної точки зору є трохи гіршим, проте завдяки своїй простоті він легше піддається аналізу, що значно підвищує його привабливість для розробників електронних підписів.

6. Компенсувати гіршу якість семплування можливо іншими засобами у електронних підписах, в той час як буде залишатися простота реалізації. Це є безсумнівним плюсом для побудови сучасних постквантових схем. Потенційно це дає можливість вирішити недолік схеми Falcon і значно зменшити складність реалізації.

Список літератури:

1. Gorhan Alagic Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process. NISTIR 8309 / Gorjan Alagic, Jacob Alperin-Sheriff, Daniel Apon, David Cooper, Quynh Dang, John Kelsey, Yi-Kai Liu, Carl Miller, Dustin Moody, Rene Peralta, Ray Perlner
2. Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, Peter Schwabe, Gregor Seiler and Damien Stehlé CRYSTALS-Dilithium: Algorithm Specifications and Supporting Documentation. Access mode: https://pq-crystals.org/dilithium/data/dilithium-specification.pdf
3. Thomas Prest et Al. aFlcon: Fast-Fourier Lattice-basedCompact Signatures over NTRU. Access mode: https://falcon-sign.info/falcon.pdf
4. NISTR 8309. Status Report on the Second Round of the NIST Post-Quantum Cryptography Standartization Process. NIST, 2020. 39 p.
5. NIST Post-Quantum Cryptography Standartization Project : веб сайт. URL: https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization (дата звернення: 27.11.2020)
6. Craig Gentry, Chris Peikert, Vinod Vaikuntanathan How to Use a Short Basis: Trapdoors for Hard Lattices and New Cryptographic Constructions. -Access mode: https://eprint.iacr.org/2007/432.pdf
7. Phong Q. Nguyen, Oded Regev Learning a Parallelepiped: Cryptoanalysis of GGH and NTRU Signatures. Access mode: https://iacr.org/archive/eurocrypt2006/40040273/40040273.pdf
8. Thomas Espitau et all. MITAKA: A Simpler, Parallelizable Maskable Variant of Falcon. Access mode: https://eprint.iacr.org/2021/1486.pdf
9. Ducas L., Galbraith S., Prest T., Yu Y.: Integral matrix gram root and lattice gaussian sampling without floats // Canteaut A., Ishai Y. (eds.) EUROCRYPT 2020, Part II. LNCS, vol. 12106, pp. 608–637. Springer, Heidelberg (May 2020).
10. Thoms Prest Gaussian Sampling in Lattice-Based Cryptography. Access mode: https://tprest.github.io/pdf/pub/thesis-thomas-prest.pdf

11. Garillot F., Kondi Y., Mohassel P., Nikolaenko V. Threshold schnorr with stateless deterministic signing from standard assumptions // Malkin, T., Peikert, C.(eds.) Advances in Cryptology – CRYPTO 2021. pp. 127–156. Springer International Publishing, Cham (2021)

12. Fukumitsu M., Hasegawa S. A lattice-based provably secure multisignature scheme in quantum random oracle model // Nguyen, K., Wu, W., Lam, K.Y.,Wang, H. (eds.) Provable and Practical Security. pp. 45–64. Springer International Publishing, Cham (2020)

13. Esgin M.F., Steinfeld R., Sakzad A., Liu J.K., Liu D. Short lattice-based one-out-of-many proofs and applications to ring signatures. Cryptology ePrint Archive, Report 2018/773 (2018), https://ia.cr/2018/773

14. Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Pornin, Thomas Prest, Thomas Ricosset, Gregor Seiler, William Whyte, Zhenfei Zhang. Falcon: Fast-Fourier Lattice-basedCompact Signatures over NTRU. [Electronic resource]. Access mode: https://falcon-sign.info/falcon.pdf.

15. PQC Standardization Process: Third Round Candidate Announcement. July 22, 2020. [Electronic resource]. Access mode: https://csrc.nist.gov/News/2020/pqc-third-round-candidate-announcement

Надійшла до редколегії 03.03.2022

Відомості про авторів:

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

Кандій Сергій Олегович – Харківський національний університет імені В. Н. Каразіна, аспірант кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук, АТ «Інститут Інформаційних технологій», технік-конструктор, Україна; e-mail: sergeykandy@gmail.com

Острянська Єлизавета Вадимівна – аналітик з систем захисту інформації, АТ «Інститут Інформаційних технологій», Україна; e-mail: antelizza@gmail.com

УДК 004.056.5 **DOI:10.30837/rt.2022.2.209.04**

Я.А. ДЕРЕВ'ЯНКО, Ю.І. ГОРБЕНКО, канд. техн. наук, О.О. КУЗНЕЦОВ, д-р техн. наук

ФАКТОРІАЛЬНА СИСТЕМА ЧИСЛЕННЯ ДЛЯ ГЕНЕРАЦІЇ НЕЛІНІЙНИХ ПІДСТАНОВОК

Вступ

Перестановки є одним із важливих елементів комбінаторики, який повсюдно використовується у різних сферах і реальних задачах. Одним із варіантів використання перестановок у криптографії є шифрування за допомогою цих повідомлень або використання перестановок високого ступеня (2^8) в різних криптографічних перетвореннях. В деяких випадках, наприклад, якщо потрібно мати доступ до певної перестановки, необхідно мати змогу швидко отримати номер перестановки за її значеннями, або навпаки значення перестановки за її номером у загальному просторі. З такою метою доцільним буде використання факторіальної системи числення, оскільки завдяки її використанню можна швидко відтворити перестановку, маючи тільки її номер, а також виконати зворотне перетворення в разі необхідності. При цьому застосовуються спеціальні математичні поняття інверсії підстановок та алгоритми кодування у факторіальній системі числення.

В даній роботі описано загальні принципи використання факторіальної системи числення для роботи з перестановками, наведено основні алгоритми переведення номеру перестановки у її значення, а також зворотного переведення. Зазначені алгоритми реалізовано мовою програмування С. Ми наводимо чисельні приклади для демонстрації та перевірки отриманих результатів. Також в роботі досліджено зміну криптографічних показників та функцій вартості для впорядкованих у факторіальній системі числення підстановок. Такі функції вартості використовуються в евристичних методах пошуку, тобто отримані результати будуть корисними для прискорення генерації нелінійних підстановок.

1. Факторіальна систем числення

У факторіальній системі числення основами є послідовність факторіалів $b_k = k!$. Кожне натуральне число x представляється у вигляді

$$x = \sum_{k=1}^{n} a_k k!, \tag{1}$$

де $0 \le a_k \le k$

Факторіальна система числення використовується при декодуванні перестановок списками інверсій, тобто маючи номер перестановки, можна відтворити її саму наступним чином: номер перестановки (починаючи з 0) записується в факторіальній системі числення, при цьому коефіцієнт при числі $i!$ буде позначати число інверсій для елементу $i+1$ в тій множині, в якій виконуються перестановки (тобто число елементів, менших за $i+1$, але які знаходяться правіше нього в шуканій перестановці).

1.1. Алгоритми представлення цілого числа в факторіальній системі числення

Для представлення цілого числа без знаку (натуральні числа) x у факторіальній системі числення потрібно знайти набір цифр a_k, $k = 1,...,n$ таких, що

$$x = \sum_{k=1}^{n} a_k k! = a_n n! + a_{n-1}(n-1)! + ... + a_2 2! + a_1 1! \tag{2}$$

де $0 \le a_k \le k$

Для такого представлення достатньо виконати послідовність наступних кроків:

Алгоритм 1:

$$\begin{aligned} &x = a_n n! + r_n \\ &r_n = a_{n-1}(n-1)! + r_{n-1} \\ &\dots \\ &r_2 = a_2 2! + r_2; \\ &r_2 = a_1. \end{aligned} \tag{3}$$

Набір $a_n, a_{n-1}, ..., a_2, a_1$ представляє ціле число без знаку в факторіальній системі числення.

Приклад 1. Представимо число 77 в факторіальній системі числення (з використанням алгоритму 1):

$$\begin{aligned} &77 = 3 \cdot 4! + 5;\ a_4 = 3; \\ &5 = 0 \cdot 3! + 5;\ a_3 = 0; \\ &5 = 2 \cdot 2! + 1;\ a_2 = 2; \\ &1 = 1;\ a_1 = 1. \end{aligned} \tag{4}$$

Вихід: число у факторіальній системі має вигляд $\{3,0,2,1,0\}$.

Недоліком такого алгоритму є необхідність обчислення основ – послідовних значень факторіалів $k!$, $k = 1,...,n$. Для великих k та n це буде доволі складною задачею.

Для усунення даного недоліку можна представити факторіальне число x з використанням схеми Горнера:

$$x = a_n n! + a_{n-1}(n-1)! + ... + a_2 2! + a_1 1! = (...(a_n n + a_{n-1})(n-1) + ... + a_2)2 + a_1 \tag{5}$$

При такому записі числа x для знаходження всіх a_k, $k = 1,...,n-1$ достатньо виконати послідовність таких кроків:

Алгоритм 2:

$$\begin{aligned} &x = q_1 2 + a_1; \\ &q_1 = q_2 3 + a_2; \\ &q_2 = q_3 4 + a_3; \\ &\dots \\ &q_{n-3} = q_{n-2}(n-1) + a_{n-2}; \\ &q_{n-2} = q_{n-1} n + a_{n-1}; \\ &q_{n-1} = a_n. \end{aligned} \tag{6}$$

Набір залишків $a_n, a_{n-1}, ..., a_2, a_1$ представляє ціле число без знаку в факторіальній системі числення.

Приклад 2. Представимо число 77 в факторіальній системі числення (з використанням алгоритму 2):

$$\begin{aligned} &77 = 38 \cdot 2 + 1;\ a_1 = 1; \\ &38 = 12 \cdot 3 + 2;\ a_2 = 2; \\ &12 = 3 \cdot 4 + 0;\ a_3 = 0; \\ &3 = 3;\ a_4 = 3. \end{aligned} \tag{7}$$

Вихід: число у факторіальній системі має вигляд $\{3,0,2,1,0\}$.

Алгоритм 2 з використанням схеми Горнера є значно простішим у застосуванні та реалізації, оскільки не вимагає обчислення основ – послідовних значень факторіалів $k!$, $k=1,...,n$.

Для представлення перестановки у факторіальній системі числення можна застосувати декілька споріднених алгоритмів. В основі цих алгоритмів лежить застосування спеціального математичного поняття інверсії.

1.2. Алгоритми представлення підстановки в факторіальній системі числення

Інверсією в дискретній математиці називається послідовність із двох чисел впорядкованих в оберненому порядку. Ми розглядаємо інверсії в перестановках множини $X=\{1,2,...,n\}$. Кожна перестановка π може бути записана як кортеж із n елементів

$$\pi=(y_1,y_2,...,y_n) \tag{8}$$

або у вигляді підстановки, наприклад:

$$\begin{pmatrix} x_1 & x_2 & x_3 & \dots & x_n \\ y_1 & y_2 & y_3 & \dots & y_n \end{pmatrix} \tag{9}$$

де

$$\{x_1,\dots,x_n\}=\{y_1,\dots,y_n\}=X,\ \pi(x_i)=y_i \tag{10}$$

Інверсією в перестановці π називається пара індексів (i,j) для пар елементів $(\pi(i),\pi(j))$ така, що $1\le i<j\le n$ та $\pi(i)>\pi(j)$.

Наприклад, в перестановці $\pi=(4,2,1,3)$ інверсії утворюють пари індексів $(1,2)$, $(1,3)$, $(1,4)$, $(2,3)$ для пар елементів $(4,2)$, $(4,1)$, $(4,3)$, $(2,1)$ відповідно.

Перестановка називається парною, якщо її елементи утворюють у сумі парне число інверсій, і непарною, якщо вони утворюють непарне число інверсій. Наприклад, в перестановці $\pi=(4,2,1,3)$ елементи утворюють чотири інверсії, тобто перестановка парна. В перестановці $\pi=(2,1,3,4)$ інверсію утворює лише пара індексів $(1,2)$, тому перестановка непарна. В перестановці $\pi=(1,2,3,4)$ немає жодної інверсії. Число інверсій дорівнює 0, тому перестановка парна.

Факторіальна система числення використовується при декодуванні перестановок списками інверсій. Тобто маючи номер перестановки, можна відтворити саму підстановку наступним чином: номер перестановки (починаючи з 0) записується в факторіальній системі числення, при цьому коефіцієнт при числі $i!$ буде позначати число інверсій для елементу $i+1$ в тій множині, в якій виконуються перестановки (тобто число елементів, менших за $i+1$, але які знаходяться правіше нього в шуканій перестановці).

Алгоритм отримання факторіального числа $a_n,a_{n-1},...,a_2,a_1$ із перестановки π множини $X=\{1,2,...,n\}$ має таку послідовність кроків.

Алгоритм 3:

$i\leftarrow 1;$
While $i<n$ do
$k\leftarrow 0;$
For $j=i+1$ to n do
If $\pi(i)>\pi(j)$ then $k\leftarrow k+1$ (11)
$a_{\pi(i)}\leftarrow k;$
$i\leftarrow i+1;$
$a_{\pi(n)}\leftarrow 0;$
Return $a_n,a_{n-1},...,a_2,a_1$.

Приклад 3. Покажемо на прикладі як буде відбуватися переведення перестановки $\pi = (3,5,2,1,4)$ множини $X = \{1,2,3,4,5\}$ у факторіальне число:

$i = 1,\ k = 0$

$j = 2;\ \pi(1) = 3 < \pi(2) = 5,\ k = 0;$

$i = 3;\ \pi(1) = 3 > \pi(3) = 2,\ k = 1;$

$i = 4;\ \pi(1) = 3 > \pi(4) = 1,\ k = 2;$

$i = 5;\ \pi(1) = 3 < \pi(5) = 4,\ k = 2;$

$a_3 = 2;$

$i = 2,\ k = 0$

$i = 3;\ \pi(2) = 5 > \pi(3) = 2,\ k = 1;$

$i = 4;\ \pi(2) = 5 > \pi(4) = 1,\ k = 2;$

$i = 5;\ \pi(2) = 5 > \pi(5) = 4,\ k = 3;$ (12)

$a_5 = 3;$

$i = 3,\ k = 0$

$i = 4;\ \pi(3) = 2 > \pi(4) = 1,\ k = 1;$

$a_2 = 1;$

$i = 4,\ k = 0$

$i = 5;\ \pi(4) = 1 < \pi(5) = 4,\ k = 0;$

$a_1 = 0;$

$a_4 = 0;$

Return $3, 0, 2, 1, 0$.

Для переходу від факторіальної до десяткової системи числення треба скористатися формулою (1), тобто кожен з залишків помножити на відповідну йому основу – факторіал $k!$, $k = 1,...,n$.

Отже, маємо наступне:

$$x = \sum_{k=1}^{n} a_k k! = 0 \cdot 0! + 1 \cdot 1! + 2 \cdot 2! + 0 \cdot 3! + 3 \cdot 4! = 0 + 1 + 4 + 0 + 72 = 77 \quad (13)$$

Також для даного алгоритму покажемо алгоритм зворотного переходу:

Алгоритм отримання перестановки з її номеру буде полягати в наступному.

Алгоритм 4:

1. Переводимо число з десяткової системи числення з використанням алгоритму 2.

2. Отримуємо число у факторіальній системі числення.

3. Кожен з залишків числа у факторіальній системі буде означати кількість елементів, які є меншими за $n - i$, де $i = \overline{0, n-1}$ – порядок залишку у факторіальному числі, але стоять правіше нього.

4. Отримуємо перестановку, яка відповідатиме початковому числу у десятковій СЧ і у факторіальній СЧ.

Приклад 4. Покажемо на прикладі як буде відбуватися переведення числа 77 у перестановку:

1. Переводимо число 77 у факторіальну СЧ:

$$\begin{aligned} &77 = 38 \cdot 2 + 1;\ a_1 = 1; \\ &38 = 12 \cdot 3 + 2;\ a_2 = 2; \\ &12 = 3 \cdot 4 + 0;\ a_3 = 0; \\ &3 = 3;\ a_4 = 3. \end{aligned} \quad (14)$$

2. Отримали число у ФСЧ – {3,0,2,1,0}.

3. Отже, виходячи з алгоритму 4, число у факторіальній системі числення буде означати наступне для перестановки довжини 5:

- першим залишком факторіального числа буде число елементів, які є меншими за 5, але стоять правіше нього – 3;
- другим залишком буде число елементів менших за 4, але які стоять правіше нього – 0;
- третім залишком є число елементів менших за 3, які стоять правіше нього – 2;
- четвертим залишком буде число елементів, менших за 2, які стоять правіше нього – 1.
- останній елемент перестановки завжди ставиться на вільне місце, тому значення останнього залишку завжди буде нульовим.

4. Виходячи з наведених вище правил переведення факторіального числа у перестановку, отримуємо наступну перестановку для числа 77 ({3,0,2,1,0} у ФСЧ) – (3,5,2,1,4).

Отже, як можна бачити, перетворення з десяткової системи числення в факторіальну систему числення, з факторіальної системи числення у перестановку і також зворотні дії виконані успішно, отже даний метод дозволяє виконувати такі дії.

Також, варто згадати про схожий за своїм принципом код Лемера, який полягає в наступному.

У математиці і, зокрема, у комбінаториці, код Лемера – це особливий спосіб кодування кожної можливої перестановки послідовності з n чисел. Це приклад схеми перестановок нумерації та приклад таблиці інверсії. Код Лемера використовує той факт, що існує

$$n! = n \times (n-1) \times \cdots \times 2 \times 1 \tag{15}$$

перестановок послідовності з n чисел. Якщо перестановка σ задається послідовністю $(\sigma_1,...,\sigma_n)$ її образів $1,...,n$, то вона кодується послідовністю з n чисел, але не всі такі послідовності є дійсними, оскільки потрібно використовувати кожне число тільки один раз. Отже, вибирають перше число з набору з n значень, наступне число з фіксованого набору з $n-1$ значень і так далі, зменшуючи кількість можливостей до останнього числа, для якого є лише одне фіксоване значення. Переводячи цю свободу вибору на кожному кроці в число, отримуємо алгоритм кодування, який знаходить код Лемера даної перестановки. Відповідне число для кодування кожного об'єкта σ_i – це кількість об'єктів, які були доступні на той момент (тому вони не зустрічаються до позиції i), але які є меншими за об'єкт σ_i. Отже, сам алгоритм матиме такий опис:

Алгоритм 5:

1. Для отримання коду Лемера перестановки необхідно для кожного σ_i, де $i = \overline{0, n-1}$, знайти кількість елементів, які будуть меншими за нього, але знаходитимуться правіше.

2. Отримуємо таким чином код Лемера.

Приклад 5. Покажемо на прикладі як буде відбуватися переведення перестановки {1,5,0,6,3,4,2} у код Лемера:

1. Починаючи з першого числа в перестановці знаходимо числа, які є меншими за обране число і стоять правіше нього: для перестановки {1,5,0,6,3,4,2} наприклад, число елементів, менших за 1, але правіше нього – 1, менших за 5, але правіше – 4, менших на 0, але правіше 0, менших за 6, але правіше – 3, менших за 3, але правіше – 1, менших за 4, але правіше – 1, і останній лишок завжди буде нульовим, оскільки залишається тільки 1 позиція.

2. Таким чином отримуємо код Лемера – (1,4,0,3,1,1,0).

Зворотне перетворення, тобто коду Лемера у перестановку, полягає в наступному.

Алгоритм 6:

1. Береться перестановка довжини n з елементами у чіткому порядку за зростанням – {0,1,2,3,4,5,6}.

2. Далі, згідно з кодом Лемера, ми викреслюємо з даної перестановки елемент, який відповідає числу i в коді Лемера, $i = \overline{0, n-1}$.

3. Отримуємо початкову перестановку.

Приклад 6. Покажемо на прикладі як буде відбуватися перехід від коду Ламера до перестановки:

1. Береться перестановка – {0,1,2,3,4,5,6}.

2. Перше число коду Лемера – 1, тобто починаємо від елементу під номером нуль ідемо направо та викреслюємо елемент під номером, який відповідає числу в коді Лемера – 1. Перестановка матиме вигляд {0,2,3,4,5,6}. Друге число коду дорівнює 4 – викреслюємо елемент під номером 4 в перестановці, що лишилася – це число 5. Перестановка набула вигляду {0,2,3,4,6}. Третє число коду – 0 – викреслюємо число 0. Перестановка набула вигляду {2,3,4,6}. Четверте число коду дорівнює 3 – викреслюємо число 6. Перестановка набула вигляду {2,3,4}. П'яте число коду дорівнює 1 – викреслюємо число під номером 1 в перестановці – 3. Перестановка набула вигляду {2,4}. Шосте число коду – 1. Викреслюємо число 4. Перестановка набула вигляду {2}. Останнім елементом перестановки є число, що лишилося.

3. Таким чином, використовуючи алгоритм 6, ми отримали перестановку {1,5,0,6,3,4,2}.

Отже, як можна бачити, перетворення перестановки до коду Лемера та назад успішно виконується, тому такий код може також використовуватися для кодування перестановок.

2. Програмна реалізація кодування нелінійних підстановок у факторіальній системі числення

Нами було реалізовано методи, які дозволяють виконувати описані вище дії зі звичайними типами даних (int, тощо). Реалізація доступна на сервісі GitHub за посиланням [1]: https://github.com/DereviankoYaroslav/SBoxDereviankoFactorial. Далі буде наведено лістинг коду цих методів та пояснено сутність їх роботи.

Лістинг 1. Метод перетворення числа з десяткової системи до факторіальної системи числення:

Вхідні дані методу: ціле натуральне число в десятковій СЧ, яке необхідно перевести в факторіальну СЧ – int x та значення факторіалу, в межах якого це число знаходиться int n (наприклад, для чисел 0-119 $n = 5$ і т.д.).

Вихідні дані методу: масив, розміру n, кожним елементом якого будуть залишки факторіального числа за відповідною основою $k!$, $k = 1,...,n$, весь масив в цілому представляє число у факторіальному вигляді.

```
int *numberToFactorial(int x, int n){
  int q = 2;
  int counter = n-2;
  int *positions = calloc (n,sizeof(int));
  positions[n-1] = 0;
  while (counter > 0){
    long long temp = floor(x/q);
    long long val = x – (temp*q);
    positions[counter] = val;
    x = temp;
    ++q;
    counter--;
  }
  positions[counter] = x;
  printf("\nPOSITIONS VECTOR\n");
  for (int i = 0; i < n ; ++i){
    printf("%d ",positions[i]);
  }
```

```
    int *positionsRev = calloc (n,sizeof(int));
    for (int r = 0,t = n-1; r < n, t>=0; ++r, t--){
        positionsRev[t] = positions[r];
    }
    free(positions);
    return positionsRev;
}
```

Лістинг 2. Метод перетворення факторіального числа до перестановки (за алгоритмом 3):

Вхідні дані методу: масив, розміру n, кожним елементом якого будуть залишки факторіального числа за відповідною основою $k!$, $k = 1,...,n$, розмір масиву – $size = n$.

Вихідні дані методу: перестановка довжини n, яка відповідатиме вхідному факторіальному числу.

```
    int *numberToSubstitution(int *number, int size){
    int *S = calloc (size,sizeof(int));
    int *result = calloc (size,sizeof(int));
    int newSize = size;
    int counter = 0;
    int coeffNum = 0;
    int innerCounter = 0;
    while(counter < size){
        int *emptyPos = calloc (newSize,sizeof(int));
        for (int i = 0; i < size; ++i){
            if (S[i]==0){
                emptyPos[innerCounter] = i;
                innerCounter++;
            }
        }
        for (int q = 0; q < newSize; ++q){
            if (q==number[newSize-1]){
                S[emptyPos[q]] = 1;
                result[coeffNum] = emptyPos[q];
                ++coeffNum;
            }
        }
        innerCounter = 0;
        ++counter;
        newSize--;
        free(emptyPos);
    }
    int numberInArr = size;
    int *sub = calloc (size,sizeof(int));
    for (int u = 0; u < size; ++u){
        sub[result[u]] = numberInArr;
        numberInArr--;
    }
    free(result);
    int *subRev = calloc (size,sizeof(int));
    for (int r = 0,t = size-1; r < size, t>=0; ++r, t--){
        subRev[t] = sub[r];
    }
```

```
    free(sub);
    free(S);
    return subRev;
}
```

Лістинг 3. Метод зворотного перетворення перестановки у факторіальне число:

Вхідні дані методу: перестановка довжини n ($size = n$), розмір перестановки $size = n$

Вихідні дані методу: масив, розміру n, кожним елементом якого будуть залишки факторіального числа за відповідною основою $k!$, $k = 1,...,n$, весь масив в цілому представляє число у факторіальному вигляді.

```
    int *substitutionToFactorial(int *sub, int size) {
    int *result = calloc(size,sizeof(int));
    int value = size;
    int flag = 0;
    int innerCounter = 0;
    int counter = 0;
    while (counter<size) {
        for (int i = 0; i < size; ++i) {
            if (flag == 1 && sub[i] < value) {
                ++innerCounter;
            }
            if (sub[i] == value) {
                flag = 1;
            }
        }
        result[counter] = innerCounter;
        innerCounter = 0;
        flag = 0;
        ++counter;
        value--;
    }
    return result;
}
```

Лістинг 4. Метод зворотного перетворення факторіального числа у десяткове число:

Вхідні дані методу: масив, розміру n, кожним елементом якого будуть залишки факторіального числа за відповідною основою $k!$, $k = 1,...,n$, розмір масиву $size = n$.

Вихідні дані методу: ціле натуральне число у десятковій СЧ – int result.

```
    long long factorialNumberToNumber(int *number, int size){
    int *numberRev = calloc (size,sizeof(int));
    long long result = 0;
    for (int r = 0,t = size-1; r < size, t>=0; ++r, t--){
        numberRev[t] = number[r];
    }
    for (int i = 0; i < size; ++i){
        result += numberRev[i]*factorialCounting(i);
    }
    free(numberRev);
    return result;
}
```

2.1. Приклади переведення чисел у перестановки і зворотні перетворення

Покажемо результати виконання послідовного перетворення десяткового числа у факторіальне число, факторіального числа у перестановку, перестановку назад у факторіальне число і далі – факторіальне число у десяткове число. Для наочної демонстрації результатів покажемо спочатку переведення у факторіальну систему числення числа з прикладу – 77, а потім перетворення числа 100 з прикладу та ще декількох чисел на перестановки та назад.

Переведення числа 77 з десяткової СЧ у факторіальну буде відбуватися з використанням схеми Горнера, так наприклад, спочатку число буде ділитися на 2, і першим числом факторіального числа буде залишок від такого ділення, далі на 3, і так далі, поки дільник не буде дорівнювати $n-1$. Дільником на кожному кроці буде виступати ціла частина від такого ділення. Така дія матиме наступний вигляд:

```
START NUMBER
77

a_n = 1
a_n = 2
a_n = 0
a_n = 3

POSITIONS VECTOR
3, 0, 2, 1, 0,
```

Рис. 1. Приклад переведення числа 77 у ФСЧ

Перше значення буде залишком від ділення на 2, друге на 3 і т.д. аж до $n-1$. Таким чином, ці залишки будуть утворювати факторіальне число. Останній залишок факторіального числа завжди буде нульовим. Далі буде показано результати перетворення різних чисел з десяткової СЧ у ФСЧ, із ФСЧ у перестановку, і результати зворотних дій. Деталі перетворень описані у коді алгоритмів:

```
START NUMBER
77

FACTORIAL NUMBER
3, 0, 2, 1, 0,

SUBSTITUTION
3, 5, 2, 1, 4,

FACTORIAL NUMBER
3, 0, 2, 1, 0,

FINAL NUMBER
77
```

Рис. 2. Переведення числа 77 у перестановку і назад (n=5)

```
START NUMBER
100

FACTORIAL NUMBER
4, 0, 2, 0, 0,

SUBSTITUTION
5, 3, 1, 2, 4,

FACTORIAL NUMBER
4, 0, 2, 0, 0,

FINAL NUMBER
100
```

Рис. 3. Переведення числа 100 у перестановку і назад (n=5)

```
START NUMBER
2999999

FACTORIAL NUMBER
8, 2, 3, 1, 3, 4, 3, 2, 1, 0,

SUBSTITUTION
5, 10, 4, 6, 3, 8, 2, 9, 7, 1,

FACTORIAL NUMBER
8, 2, 3, 1, 3, 4, 3, 2, 1, 0,

FINAL NUMBER
2999999
```

Рис. 4. Переведення числа 2999999 у перестановку і назад (n=10)

3. Експерименти

Для демонстрації та перевірки правильності застосування розроблених алгоритмів в роботі проведено низку експериментів із представлення нелінійних підстановок відомих стандартів симетричного криптоперетворення. Зокрема, ми розглядаємо найпростіший приклад 4-бітних S-boxes із відомого алгоритму шифрування ГОСТ 28147-89 (приклади підстановок описані в українському стандарті). Також ми розглядаємо 8-бітну підстановку сучасного американського стандарту симетричного шифрування AES.

Ми наводимо приклади переходу від перестановок до факторіальних чисел і від них, до чисел у десятковій системі числення. Також ми наводимо заміри швидкості виконання операцій такого переходу. Для кожного прикладу пораховано нелінійність підстановки та «вартість» з використанням різних цінових функції. Зокрема, ми розглядаємо цінові функції WHS PCF та WCF з [4]. Такі евристичні функції вартості застосовують в ітераційних алгоритмах генерації S-Boxes, наприклад у HC [5], SA [6] та інших евристичних алгоритмах пошуку.

3.1. Аналіз перестановок (S-box'ів), що використовуються в українській версії ГОСТ 28147-89 (приклади з українського стандарту ДСТУ 4145-2002)

Покажемо демонстрацію роботи з нелінійними вузлами заміни на прикладі S-boxes стандарту ГОСТ 28147-89 (приклади підстановок наведено в українському стандарті ДСТУ 4145-2002).

Блоки для українського варіанту ГОСТ 28147-89 мають вигляд, як у табл. 1. Тут і надалі S-boxes подаються у шістнадцятирічному вигляді.

Таблиця 1

Нелінійні вузли заміни алгоритму ГОСТ 28147-89

S-Box	Шістнадцятирічне представлення S-Box'у																NL	Cost
1	A	9	D	6	E	B	4	5	F	1	3	C	7	0	8	2	4	0
2	8	0	C	4	9	6	7	B	2	3	1	F	5	E	A	D	4	0
3	F	6	5	8	E	B	A	4	C	0	3	7	2	9	1	D	4	0
4	3	8	D	9	6	B	F	0	2	5	C	A	4	E	1	7	4	0
5	F	8	E	9	7	2	0	D	C	6	1	5	B	4	3	A	4	0
6	2	8	9	7	5	F	0	B	C	1	D	E	A	3	6	4	4	0
7	3	8	B	5	6	4	E	A	2	C	1	7	9	F	D	0	4	0
8	1	2	3	E	6	D	B	8	F	A	C	5	7	9	0	4	4	0

Тепер покажемо (табл. 2) перехід від такого представлення до числа у факторіальній системі числення за допомогою алгоритму 3, псевдокод якого наведено у лістингу 2.

Таблиця 2

Факторіальне представлення нелінійних вузлів заміни алгоритму ГОСТ 28147-89

S-Box	Факторіальне представлення S-Box'у															
1	7	10	11	4	8	10	9	1	2	6	4	4	2	0	1	0
2	4	2	0	10	5	0	6	8	4	4	0	3	1	1	0	0
3	15	11	0	6	8	7	1	6	2	6	5	4	2	1	0	0
4	9	2	11	4	7	3	7	7	0	5	2	1	3	1	0	0
5	15	13	8	7	3	0	8	8	7	4	2	1	0	2	0	0
6	10	4	4	5	5	3	7	7	6	1	4	0	0	2	0	0
7	2	8	1	4	9	5	1	7	1	4	4	3	3	2	1	0
8	7	11	9	5	7	5	2	4	2	3	2	0	1	1	1	0

Коли всі блоки показані у вигляді факторіальних чисел, отримаємо з них числа у десятковій системі числення, тобто їхні номери у одновимірному просторі перестановок (табл. 3).

Таблиця 3

Представлення нелінійних вузлів заміни алгоритму ГОСТ 28147-89
у вигляді номеру у одновимірному просторі

S-Box	Номерне представлення S-Box'у
1	10096275666829
2	5410046177360
3	20577296088710
4	12014132259884
5	20801725497628
6	13452973260244
7	3321296141615
8	10171418435529

Як видно з таблиць, ми отримали номерне представлення блоків у одновимірній множині усіх блоків і тепер можемо робити будь-які маніпуляції з цими номерами для пошуку,

наприклад, нових блоків з хорошими показниками, але відмінними від тих, що використовуються в стандарті.

Нами проведено заміри швидкодії операцій перетворення перестановки у номер, а також зворотного перетворення. Для цього було проведено тестування, шляхом виконання операцій над одним і тим же блоком 1000000 разів, щоб порахувати середню швидкість виконання операції в мілісекундах, оскільки ця швидкість має дуже маленьке значення і не відображається коректно шляхом меншої кількості тестів.

Лістинг коду для проведення тестування наводиться нижче:

Лістинг 5. Вимірювання швидкодії операцій переходу від перестановки до номеру:

```
long t;
t = mtime();
for (int y = 0 ; y < 100000000; ++y) {
      int *factNum = substitutionToFactorial(sub2, n);
      long long number = factorialNumberToNumber(factNum, n);
      free(factNum);
}
t = mtime() – t;
printf ("%ld milliseconds\n",t);
```

Лістинг 6. Вимірювання швидкодії операцій переходу від номеру до перестановки:

```
t = mtime();
   for (int y = 0 ; y < 100000000; ++y) {
      int *arr = numberToFactorial(a, n);
      int *sub = numberToSubstitution(arr, n);
      free(arr);
      free(sub);
   }
t = mtime() – t;
printf ("%ld milliseconds\n",t);
```

Результати вимірювання швидкодії операції наведено у табл. 4.

Таблиця 4

Результати вимірювання швидкодії операції, в мілісекундах

Перехід від перестановки до номеру	0,001217 мс
Перехід від номеру до перестановки	0,003457 мс

Також для виконання програми з заданими розмірами блоків (4×4) було виміряне використання оперативної пам’яті під час роботи. Показник використання незалежно від кількості блоків коливався від 352Кб до 364 Кб (рис. 5). Тобто, програмі виділяється потрібна їй пам’ять, далі програма виконує необхідні операції і звільняє пам’ять для наступних операцій.



Рис. 5. Результати тестування витрат пам’яті

Отже, виходячи з отриманих результатів, виконання всіх необхідних операцій є доволі швидким (1-2 мікросекунди для переходу від перестановки до номеру і 3-4 мікросекунди – для переходу від номеру до перестановки) і при цьому не навантажує оперативну пам’ять комп’ютера – використання менше ніж половина мегабайта.

3.2. Аналіз S-box алгоритму AES

У даному розділі продемонструємо роботу з нелінійними вузлами заміни на прикладі AES S-box'у. Для роботи з подібними вузлами проект було адаптовано на мову програмування C++ , також було використано бібліотеку NTL для роботи з нескінченно великими числами. Реалізація доступна на сервісі GitHub за посиланнями [2, 3]:

https://github.com/DereviankoYaroslav/FactorialPSO-WHS та
https://github.com/DereviankoYaroslav/FactorialPSO-CUBA.

Таблиця 5

Нелінійний вузол заміни алгоритму AES

63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Показники у даного блоку будуть наступними (табл. 6):

Таблиця 6

Показники AES-Sbox

S-Box	NL	Cost WHS	Cost WCF	Cost PCF
AES	112	4151216	0	7491.62

Тепер покажемо (табл. 7) перехід від такого представлення до числа у факторіальній системі числення за допомогою алгоритму 3, псевдокод якого наведено у лістингу 2.

Таблиця 7

Факторіальне представлення нелінійного вузла заміни алгоритму AES

130	242	221	169	155	231	149	30	212	40	133	67	126	238	203	220
150	99	161	120	182	66	20	52	73	10	193	73	159	175	28	85
15	87	48	93	83	113	23	179	204	152	63	192	72	107	143	130
130	17	105	173	133	189	187	65	164	46	191	96	160	69	27	170
10	126	40	101	1	48	26	73	161	96	33	40	126	137	119	2
157	45	157	58	161	109	49	97	81	39	141	147	93	147	10	117
93	21	87	141	15	125	4	18	77	123	48	14	131	81	47	60
79	14	42	9	27	26	8	53	10	14	77	89	98	119	54	100
73	60	114	123	121	31	37	29	118	111	93	25	51	105	100	22
109	85	32	30	106	73	11	5	100	18	25	46	99	28	14	41
46	35	41	27	61	68	86	57	12	23	8	1	58	61	45	46
34	21	47	48	15	47	23	13	68	27	41	32	41	4	3	35
58	11	27	33	40	20	34	31	16	50	8	48	30	18	45	48
31	12	2	32	42	18	28	3	30	37	10	11	32	15	20	21
8	3	4	6	18	18	11	21	11	0	20	9	9	14	2	9
0	1	0	5	4	3	5	1	4	1	3	3	0	0	1	0

Тепер отримаємо з цього факторіального числа число у десятковій системі числення, тобто номер цієї перестановки у одновимірному просторі перестановок (табл. 8).

Таблиця 8

Представлення нелінійного вузла заміни алгоритму AES у вигляді номеру у одновимірному просторі

AES-SBox	438802080077461506931487886587859279629566435895940576091249389663118690638511176335757277833257114168214620949945405264375192303618393662335277010380153387264179445016571705252302920569441228045303327567040823942746123930949356593784189672702597268903394924732421379919535170324637836064806689559503327871102084486758924065072351307405825431157286059632497461568460660658015651849289360349395308511707577545803238296080881647265855676077166079014716466333599431175990239379323828746367933202518757906752833

Як видно з таблиць, так як і для блоків ГОСТ 28147-89, для блоку AES ми отримали номерне представлення у одновимірній множині усіх блоків і тепер можемо робити будь-які маніпуляції з цими номерами для пошуку, наприклад, нових блоків з хорошими показниками, але відмінними від тих, що використовуються в стандарті. Далі буде показано можливе практичне застосування цього.

Для блоків розміром 256 елементів також було виконано заміри швидкодії переходу до різних систем числення, а також пам’ять, що використовується при роботі програми. Заміри відбувалися так, як показано в пункті 4.1.

Результати вимірювання швидкодії операції наведено у табл. 9.

Таблиця 9

Результати вимірювання швидкодії операції, в мілісекундах, для блоків розміру 256 елементів

Перехід від перестановки до номеру	2,86940 мс
Перехід від номеру до перестановки	0,60700 мс

Також для виконання програми з заданими розмірами блоків (256 елементів) було виміряно використання оперативної пам’яті під час роботи. Показник використання в залежності від кількості блоків, задіяних для пошуку відрізнявся від 10,5 Мб для 10000 блоків до 101 Мб для 100000 блоків (рис. 6 та 7). Тобто програмі виділяється потрібна для роботи з певною кількістю блоків пам’ять, далі програма виконує необхідні операції і звільняє пам’ять для наступних операцій.

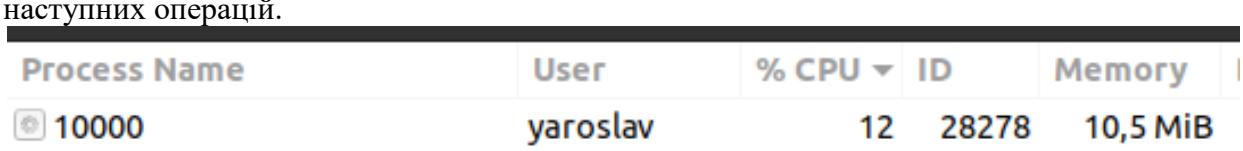


Рис. 6. Результати тестування витрат пам’яті при роботі алгоритму пошуку з кількістю 10000 блоків розміру 256

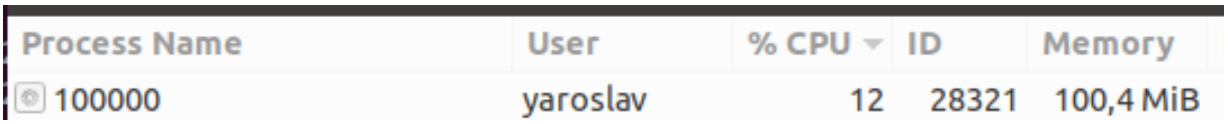


Рис. 7. Результати тестування витрат пам’яті при роботі алгоритму пошуку з кількістю 100000 блоків розміру 256

Нами також було проведено дослідження простору блоків поруч з AES-Sbox для виявлення показників блоків, що знаходяться поруч із ним. Це може допомогти в подальшому краще розуміти простір блоків та оптимізувати пошуки як цим, так і іншими алгоритмами

пошуку. Дані нелінійності та функцій вартості [4] для блоків 100 номерів до та 100 номерів після S-box'у алгоритму AES наводяться у табл. 10.

Таблиця 10

Результати вимірювання нелінійності та функцій вартості блоків у просторі навколо AES-Sbox

AES NUMBER (+/-): -100	Cost WHS	Cost WCF	Cost PCF	NL
AES NUMBER (+/-): -99	4244476	32247990190080	1975.76	108
AES NUMBER (+/-): -98	4249994	54222284390400	2008.22	108
AES NUMBER (+/-): -97	4232112	45565744250880	2003.28	108
AES NUMBER (+/-): -96	4224624	29299058933760	1972.38	108
AES NUMBER (+/-): -95	4278078	36718950481920	1974.98	108
AES NUMBER (+/-): -94	4228678	39001994035200	2002.33	108
AES NUMBER (+/-): -93	4300764	48324421877760	2005.2	108
AES NUMBER (+/-): -92	4196718	41950925291520	1997.79	108
AES NUMBER (+/-): -91	4215350	43853461585920	1998.06	108
AES NUMBER (+/-): -90	4233146	56219947499520	2021.2	108
AES NUMBER (+/-): -89	4251950	67159531192320	1000.43	106
AES NUMBER (+/-): -88	4220900	56029693870080	2028.86	108
AES NUMBER (+/-): -87	4266858	58217610608640	2029.28	108
AES NUMBER (+/-): -86	4218474	65352121712640	1001.52	106
AES NUMBER (+/-): -85	4245628	56600454758400	2023.21	108
AES NUMBER (+/-): -84	4255832	49085436395520	2024.04	108
AES NUMBER (+/-): -83	4312198	64971614453760	1003.94	106
AES NUMBER (+/-): -82	4239532	39192247664640	2001.74	108
AES NUMBER (+/-): -81	4304420	44424222474240	2005.43	108
AES NUMBER (+/-): -80	4223506	69062067486720	1004.6	106
AES NUMBER (+/-): -79	4232028	58407864238080	2029.32	108
AES NUMBER (+/-): -78	4242676	51653860392960	2019.49	108
AES NUMBER (+/-): -77	4280238	56600454758400	2023.04	108
AES NUMBER (+/-): -76	4290560	44614476103680	1998.27	108
AES NUMBER (+/-): -75	4301994	42426559365120	1999.36	108
AES NUMBER (+/-): -74	4276960	65161868083200	2031.77	108
AES NUMBER (+/-): -73	4250832	58027356979200	2029.31	108
AES NUMBER (+/-): -72	4254212	44519349288960	2002.02	108
AES NUMBER (+/-): -71	4200800	30821087969280	1971.74	108
AES NUMBER (+/-): -70	4197658	48704929136640	1995.49	108
AES NUMBER (+/-): -69	4153708	16932573020160	3889.49	110
AES NUMBER (+/-): -68	4219674	43282700697600	1997.28	108
AES NUMBER (+/-): -67	4229136	25208605900800	1971.72	108
AES NUMBER (+/-): -66	4301116	26540381306880	1972.54	108
AES NUMBER (+/-): -65	4240594	16932573020160	3902.09	110
AES NUMBER (+/-): -64	4222232	38621486776320	1996.08	108
AES NUMBER (+/-): -63	4218076	25303732715520	1970.26	108
AES NUMBER (+/-): -62	4247938	47182900101120	2001.29	108
AES NUMBER (+/-): -61	4304304	43472954327040	2002.08	108
AES NUMBER (+/-): -60	4254024	30821087969280	1968.48	108
AES NUMBER (+/-): -59	4196730	11034710507520	3841.33	110
AES NUMBER (+/-): -58	4231694	38716613591040	1998.56	108
AES NUMBER (+/-): -57	4221304	33294385152000	1972.31	108
AES NUMBER (+/-): -56	4210396	28347790786560	1969.27	108
AES NUMBER (+/-): -55	4257300	42711939809280	1995.62	108
AES NUMBER (+/-): -54	4215518	27777029898240	1973.42	108
AES NUMBER (+/-): -53	4218746	17598460723200	3905	110
AES NUMBER (+/-): -52	4203988	45565744250880	2003.24	108
AES NUMBER (+/-): -51	4247010	53841777131520	2007.28	108
AES NUMBER (+/-): -50	4156984	26635508121600	1968.75	108
AES NUMBER (+/-): -49	4196778	45090110177280	1998.77	108
AES NUMBER (+/-): -48	4265426	30440580710400	1974.95	108

AES NUMBER (+/-): -47	4203034	17693587537920	3904.35	110
AES NUMBER (+/-): -46	4168880	34150526484480	1969.22	108
AES NUMBER (+/-): -45	4134586	11034710507520	3841.33	110
AES NUMBER (+/-): -44	4180802	26730634936320	1970.48	108
AES NUMBER (+/-): -43	4208900	16361812131840	3900.12	110
AES NUMBER (+/-): -42	4302216	43092447068160	1997.97	108
AES NUMBER (+/-): -41	4241694	26730634936320	1971.04	108
AES NUMBER (+/-): -40	4215210	42807066624000	1997.84	108
AES NUMBER (+/-): -39	4219576	30440580710400	1971.41	108
AES NUMBER (+/-): -38	4240916	45375490621440	2002.8	108
AES NUMBER (+/-): -37	4305804	49370816839680	2003.29	108
AES NUMBER (+/-): -36	4233768	47373153730560	1992.81	108
AES NUMBER (+/-): -35	4176474	16171558502400	3888.69	110
AES NUMBER (+/-): -34	4243308	43377827512320	1998.41	108
AES NUMBER (+/-): -33	4222804	26540381306880	1970.91	108
AES NUMBER (+/-): -32	4222010	25208605900800	1968.46	108
AES NUMBER (+/-): -31	4258800	39572754923520	1994.41	108
AES NUMBER (+/-): -30	4185168	43948588400640	1996.97	108
AES NUMBER (+/-): -29	4188396	29108805304320	1970.45	108
AES NUMBER (+/-): -28	4206622	53556396687360	2005.33	108
AES NUMBER (+/-): -27	4248510	49465943654400	2005.69	108
AES NUMBER (+/-): -26	4159618	32818751078400	1970.42	108
AES NUMBER (+/-): -25	4198278	43568081141760	1997.31	108
AES NUMBER (+/-): -24	4211454	17408207093760	3904.26	110
AES NUMBER (+/-): -23	4149062	11034710507520	3852.16	110
AES NUMBER (+/-): -22	4129464	27016015380480	1971.95	108
AES NUMBER (+/-): -21	4139788	16361812131840	3900.94	110
AES NUMBER (+/-): -20	4141386	32057736560640	1975.61	108
AES NUMBER (+/-): -19	4214102	27777029898240	1974.82	108
AES NUMBER (+/-): -18	4201340	48039041433600	1999.53	108
AES NUMBER (+/-): -17	4147928	33960272855040	1971.05	108
AES NUMBER (+/-): -16	4151220	45755997880320	1999.98	108
AES NUMBER (+/-): -15	4160410	27396522639360	1970.32	108
AES NUMBER (+/-): -14	4173236	46802392842240	2003.9	108
AES NUMBER (+/-): -13	4235838	42521686179840	2002.73	108
AES NUMBER (+/-): -12	4192066	40428896256000	1996.81	108
AES NUMBER (+/-): -11	4181676	29489312563200	1971.26	108
AES NUMBER (+/-): -10	4223936	28538044416000	1972.34	108
AES NUMBER (+/-): -9	4203432	17598460723200	3902.97	110
AES NUMBER (+/-): -8	4227212	47087773286400	2001.23	108
AES NUMBER (+/-): -7	4217098	47087773286400	2000.85	108
AES NUMBER (+/-): -6	4150576	43187573882880	2000.74	108
AES NUMBER (+/-): -5	4193598	46326758768640	2003.66	108
AES NUMBER (+/-): -4	4183560	35006667816960	1979.26	108
AES NUMBER (+/-): -3	4225448	30440580710400	1979.06	108
AES NUMBER (+/-): -2	4164820	52510001725440	2004.23	108
AES NUMBER (+/-): -1	4163686	44804729733120	2001.12	108
AES NUMBER (+/-): 0	4185510	11700598210560	3848.05	110
AES NUMBER (+/-): 1	4151216	0	7491.62	112
AES NUMBER (+/-): 2	4200066	17598460723200	3909.85	110
AES NUMBER (+/-): 3	4210390	11985978654720	3857.61	110
AES NUMBER (+/-): 4	4143540	11320090951680	3852.37	110
AES NUMBER (+/-): 5	4188158	17408207093760	3902.36	110
AES NUMBER (+/-): 6	4194032	42807066624000	1969.83	108
AES NUMBER (+/-): 7	4150082	11034710507520	3841.33	110
AES NUMBER (+/-): 8	4200466	36338443223040	1976.81	108
AES NUMBER (+/-): 9	4209656	18359475240960	3904.74	110
AES NUMBER (+/-): 10	4175390	17027699834880	3904.83	110
AES NUMBER (+/-): 11	4228530	30821087969280	1971.69	108

AES NUMBER (+/-): 12	4253206	30916214784000	1972.28	108
AES NUMBER (+/-): 13	4249050	17122826649600	3905.77	110
AES NUMBER (+/-): 14	4245084	18549728870400	3907.39	110
AES NUMBER (+/-): 15	4249450	12461612728320	3857.38	110
AES NUMBER (+/-): 16	4248272	37479964999680	1978.98	108
AES NUMBER (+/-): 17	4256794	45185236992000	1978.69	108
AES NUMBER (+/-): 18	4152730	17788714352640	3900.44	110
AES NUMBER (+/-): 19	4192524	35767682334720	1974.61	108
AES NUMBER (+/-): 20	4185714	12461612728320	3857.38	110
AES NUMBER (+/-): 21	4224374	18074094796800	3909.61	110
AES NUMBER (+/-): 22	4213978	50702592245760	1983.7	108
AES NUMBER (+/-): 23	4212844	38336106332160	1980.03	108
AES NUMBER (+/-): 24	4180910	16361812131840	3902.3	110
AES NUMBER (+/-): 25	4209008	11034710507520	3852.16	110
AES NUMBER (+/-): 26	4195466	28347790786560	1977.02	108
AES NUMBER (+/-): 27	4268182	35482301890560	1979	108
AES NUMBER (+/-): 28	4127018	17027699834880	3899.93	110
AES NUMBER (+/-): 29	4171636	29489312563200	1971.7	108
AES NUMBER (+/-): 30	4189432	49085436395520	1996.44	108
AES NUMBER (+/-): 31	4198894	31391848857600	1970.98	108
AES NUMBER (+/-): 32	4195866	49465943654400	2003.76	108
AES NUMBER (+/-): 33	4258468	45185236992000	2004.48	108
AES NUMBER (+/-): 34	4148774	29108805304320	1970.33	108
AES NUMBER (+/-): 35	4201914	42521686179840	1996.52	108
AES NUMBER (+/-): 36	4248606	41094783959040	2000.2	108
AES NUMBER (+/-): 37	4304972	43663207956480	2002.63	108
AES NUMBER (+/-): 38	4240484	29489312563200	1976.59	108
AES NUMBER (+/-): 39	4305372	33009004707840	1978.42	108
AES NUMBER (+/-): 40	4217966	45851124695040	2002.01	108
AES NUMBER (+/-): 41	4226488	46802392842240	2001.4	108
AES NUMBER (+/-): 42	4189620	25208605900800	1969.16	108
AES NUMBER (+/-): 43	4236524	45470617436160	1997.06	108
AES NUMBER (+/-): 44	4221490	16932573020160	3900.06	110
AES NUMBER (+/-): 45	4258280	25779366789120	1971.52	108
AES NUMBER (+/-): 46	4246064	53651523502080	2003.73	108
AES NUMBER (+/-): 47	4235950	42236305735680	2002.47	108
AES NUMBER (+/-): 48	4278342	64781360824320	1003.52	106
AES NUMBER (+/-): 49	4277002	41380164403200	1996.66	108
AES NUMBER (+/-): 50	4243018	70679223336960	1001.67	106
AES NUMBER (+/-): 51	4232336	29013678489600	1969.73	108
AES NUMBER (+/-): 52	4262608	56410201128960	2022.57	108
AES NUMBER (+/-): 53	4253266	38145852702720	1998.79	108
AES NUMBER (+/-): 54	4325246	39097120849920	1998.62	108
AES NUMBER (+/-): 55	4288150	25684239974400	1972.3	108
AES NUMBER (+/-): 56	4289628	53841777131520	2026.6	108
AES NUMBER (+/-): 57	4290094	38621486776320	2001.52	108
AES NUMBER (+/-): 58	4290872	58978625126400	2027.03	108
AES NUMBER (+/-): 59	4328434	57171215646720	2028.27	108
AES NUMBER (+/-): 60	4280580	42997320253440	2000.18	108
AES NUMBER (+/-): 61	4223286	17313080279040	3901.7	110
AES NUMBER (+/-): 62	4280286	51844114022400	2031.31	108
AES NUMBER (+/-): 63	4269896	42616812994560	2001.98	108
AES NUMBER (+/-): 64	4257638	40333769441280	2002.86	108
AES NUMBER (+/-): 65	4304542	56790708387840	2027.87	108
AES NUMBER (+/-): 66	4263074	39192247664640	1999.28	108
AES NUMBER (+/-): 67	4242876	26920888565760	1971.26	108
AES NUMBER (+/-): 68	4280190	57456596090880	2028.1	108
AES NUMBER (+/-): 69	4271140	71630491484160	1004.53	106
AES NUMBER (+/-): 70	4256298	40809403514880	1999.21	108

AES NUMBER (+/-): 71	4267446	67254658007040	1004.04	106
AES NUMBER (+/-): 72	4298478	42331432550400	2001.25	108
AES NUMBER (+/-): 73	4293794	27016015380480	1973.91	108
AES NUMBER (+/-): 74	4287346	48039041433600	1999.52	108
AES NUMBER (+/-): 75	4257306	18739982499840	3904.46	110
AES NUMBER (+/-): 76	4267308	40238642626560	1997.66	108
AES NUMBER (+/-): 77	4241952	26255000862720	1972.68	108
AES NUMBER (+/-): 78	4335268	60595780976640	1002.17	106
AES NUMBER (+/-): 79	4298172	39763008552960	1998.52	108
AES NUMBER (+/-): 80	4326178	58407864238080	2030.25	108
AES NUMBER (+/-): 81	4300516	40714276700160	2003.26	108
AES NUMBER (+/-): 82	4327422	61356795494400	2030.38	108
AES NUMBER (+/-): 83	4338856	64495980380160	1004.64	106
AES NUMBER (+/-): 84	4298780	74389169111040	1002.39	106
AES NUMBER (+/-): 85	4241486	29679566192640	1970.74	108
AES NUMBER (+/-): 86	4300822	66493643489280	1005.79	106
AES NUMBER (+/-): 87	4280318	38906867220480	2002.2	108
AES NUMBER (+/-): 88	4278174	41475291217920	2003.14	108
AES NUMBER (+/-): 89	4314964	58598117867520	1003.49	106
AES NUMBER (+/-): 90	4241646	65352121712640	1001.59	106
AES NUMBER (+/-): 91	4221448	41475291217920	1995.88	108
AES NUMBER (+/-): 92	4297382	73723281408000	1005.72	106
AES NUMBER (+/-): 93	4281562	61451922309120	2029.32	108
AES NUMBER (+/-): 94	4273490	45755997880320	2002.79	108
AES NUMBER (+/-): 95	4277868	57361469276160	2028.12	108
AES NUMBER (+/-): 96	4233710	29489312563200	1971.53	108
AES NUMBER (+/-): 97	4229026	18454602055680	3905.33	110
AES NUMBER (+/-): 98	4224954	38716613591040	2000.18	108
AES NUMBER (+/-): 99	4251712	27491649454080	1974.74	108
AES NUMBER (+/-): 100	4204916	42046052106240	2001.16	108

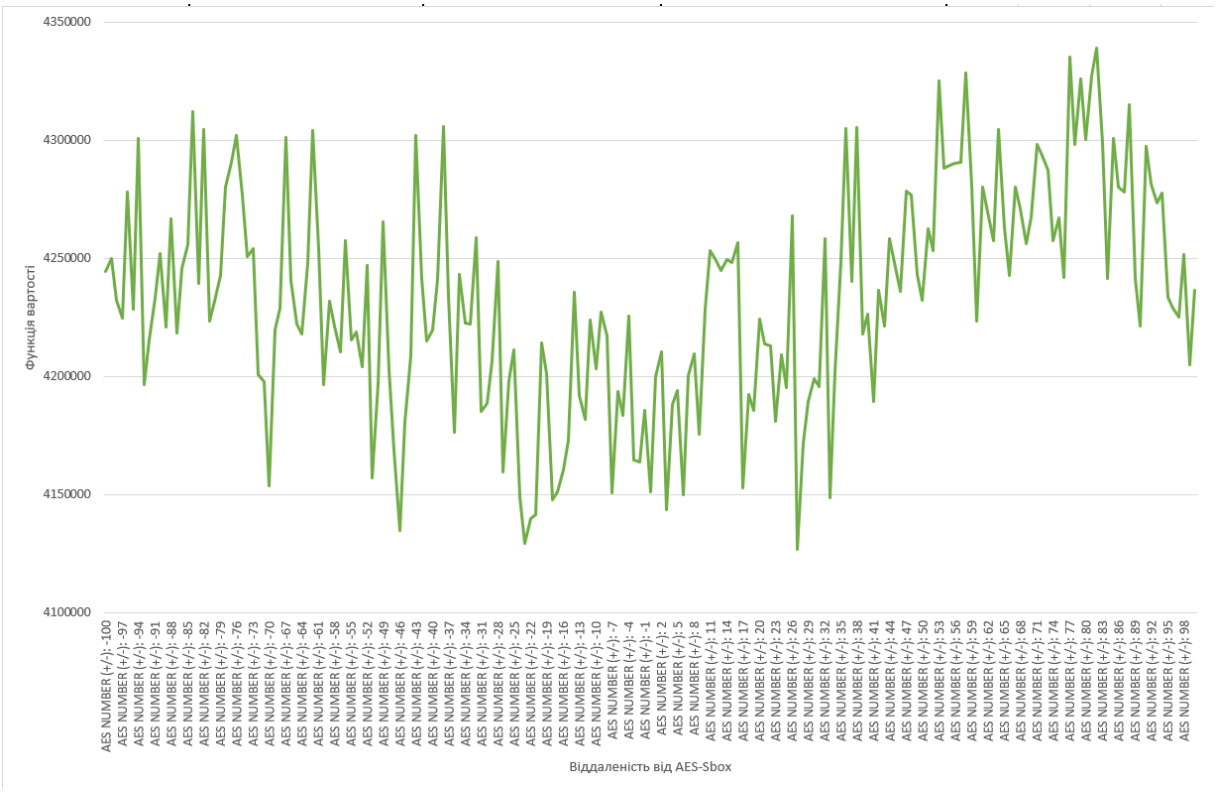


Рис. 8. Графік вартості блок Графік вартості блоків у просторі навколо AES-Sbox для цінової функції WHS

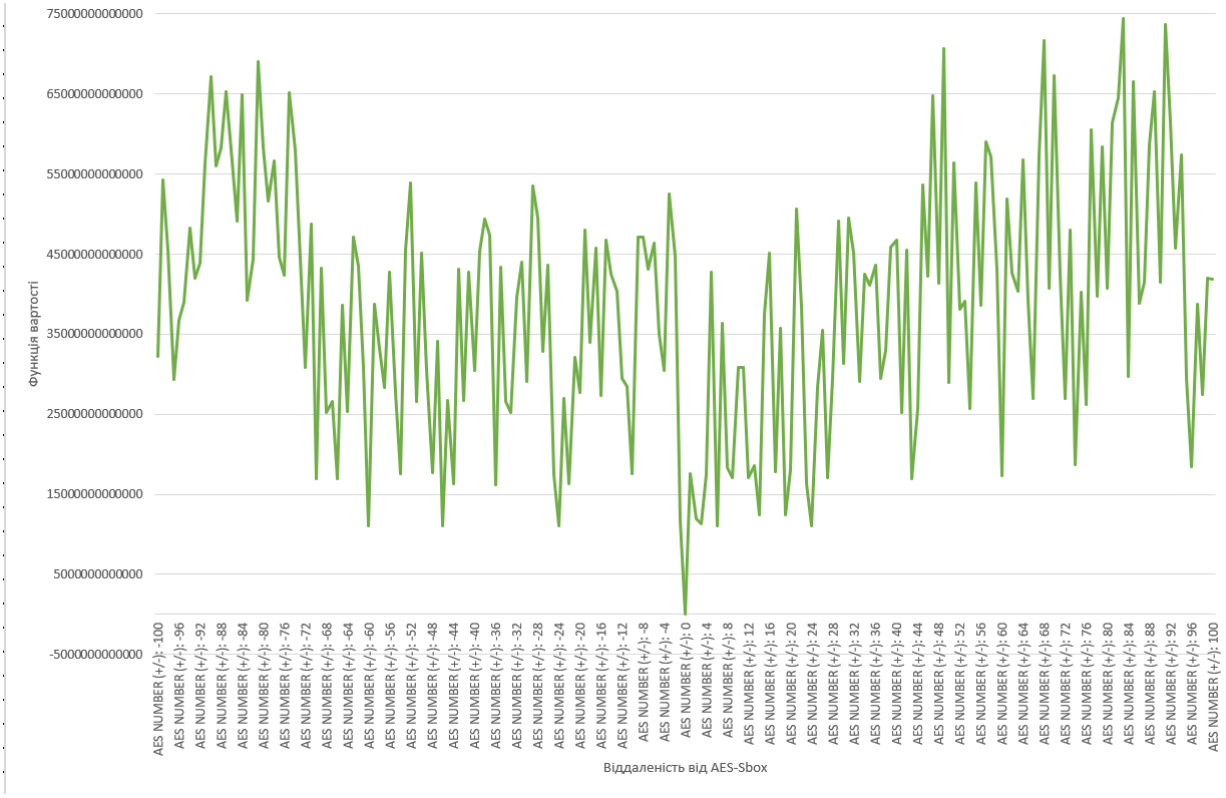


Рис. 9. Графік вартості блоків у просторі навколо AES-Sbox для цінової функції WCF

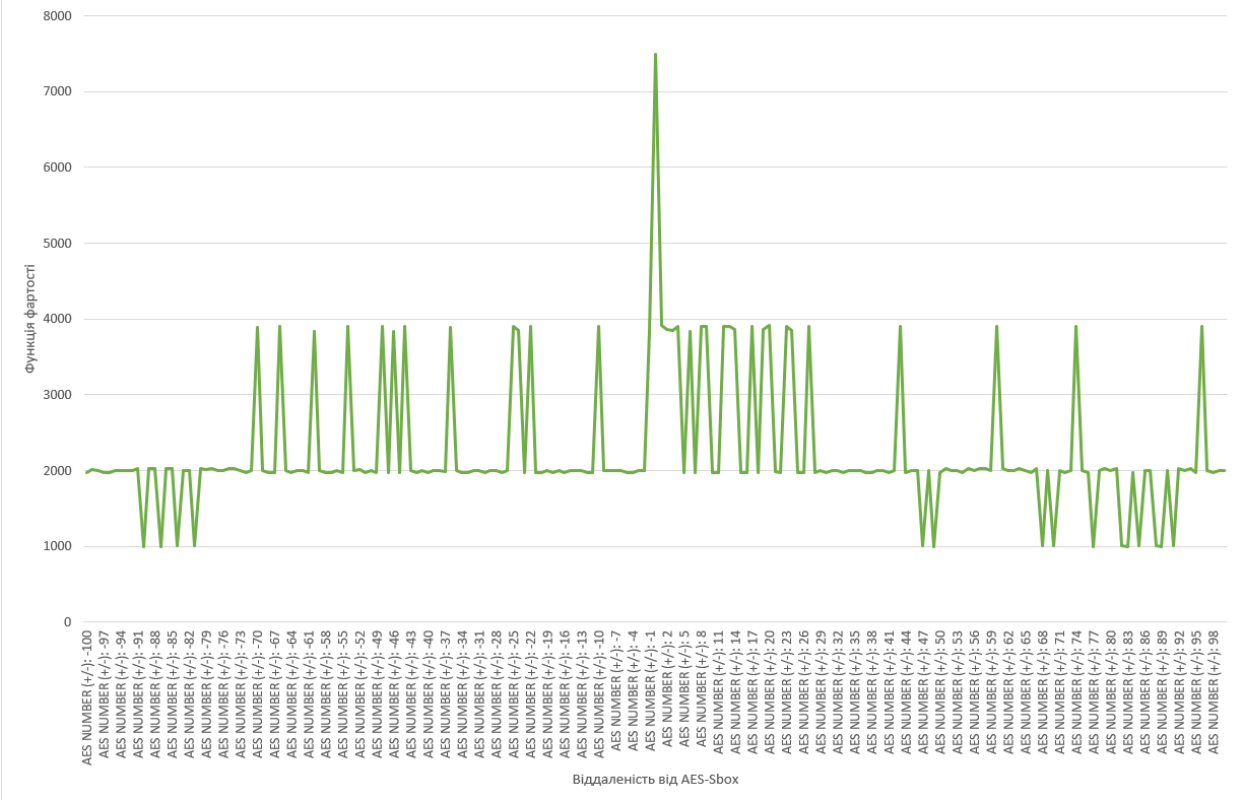


Рис. 10. Графік вартості блоків у просторі навколо AES-Sbox для цінової функції PCF

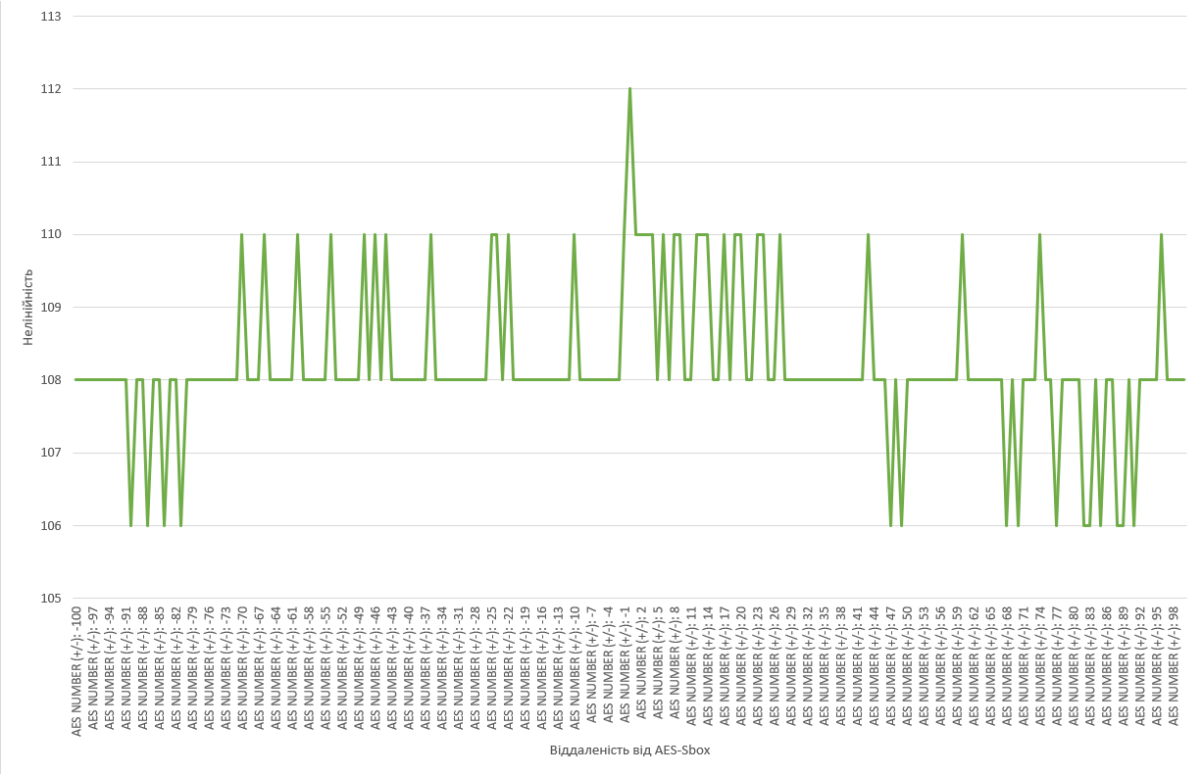


Рис. 11. Графік нелінійності простору блоків навколо AES-Sbox

Як видно з табл. 10 та графіків, простір навколо AES містить у собі блоки з дуже гарними показниками нелінійності, проте всі інші показники, такі як, наприклад, алгебраїчний імунітет, у цих блоків не дуже хороші. Також з результатів видно, що нелінійності блоків несуть в собі дуже малу кількість інформації щодо цінності кожного з блоків, проте при використанні цінових функцій, чітко помітно різницю між «хорошим» та «поганим» блоком, тобто локальні мінімуми чи максимуми (в залежності від функції), в яких і знаходяться «хороші» блоки. Отже, використання цінових функцій має значно покращити пошукові можливості алгоритму, оскільки алгоритм більш чітко «бачитиме» місця, в яких знаходяться «хороші» і «погані» блоки. Це означатиме, що при пошуку він не буде відволікатися на блоки, які є гарними тільки за нелінійністю, тобто враховуватиме тільки блоки, які є кращими за інші за повним спектром, а не тільки за найбільшим з його коефіцієнтів. За результатами тестування можна сказати, що найбільш оптимальною буде функція WHS, оскільки в ній найбільше виражені мінімуми та максимуми простору.

Висновки

1. Оскільки робота з перестановками є важливою задачею в багатьох сферах сучасної діяльності, застосування факторіальної системи числення з метою доступу до певної перестановки за її номером або навпаки отримання номеру за її значеннями є доволі важливою задачею.

2. Детально розглянуто та пояснено загальні принципи використання факторіальної системи числення для роботи з перестановками. В ній пропонуються алгоритми переведення номеру перестановки у її значення, а також зворотного переведення мовою програмування С. Також досліджуються нелінійні перестановки, що використовуються в алгоритмах ГОСТ 28147-89 та AES. Практично отримано номери цих перестановок з використанням факторіальної СЧ, визначено параметри даних блоків, а також надано результати вимірювання швидкодії операцій переходу від перестановок до номерів і зворотних перетворень.

3. Проведено дослідження простору блоків поруч з AES-Sbox, що знаходяться поруч із ним. Це може допомогти в подальшому краще розуміти простір блоків та оптимізувати пошуки як запропонованим, так і іншими алгоритмами пошуку.

4. Визначено показники блоків у просторі – нелінійності та функції вартості. Результати дослідження підтвердили, що простір навколо AES не є оптимальним пошуковим місцем, оскільки блоки тут є «хорошими» тільки за показником нелінійності, тому алгоритм слід адаптувати виключно під випадковий пошук, а не на основі якихось уже відомих блоків.

5. Для ефективного пошуку необхідно застосовувати функцію вартості. Це дозволить в процесі пошуку алгоритму зациклюватися тільки на блоках з повністю «хорошим» спектром, відкидаючи блоки з тільки одним «хорошим» коефіцієнтом.

Список літератури:

1. Програмна реалізація Факторіальної системи числення від Дерев'янка Я. А. URL: https://github.com/DereviankoYaroslav/SBoxDereviankoFactorial.

2. Програмна реалізація алгоритму PSO з використанням факторіальної системи числення та цінової функції WHS від Дерев'янка Я. А. URL: https://github.com/DereviankoYaroslav/FactorialPSO-WHS.

3. Програмна реалізація алгоритму PSO з використанням факторіальної системи числення та цінової функції WCF від Дерев'янка Я. А. URL: https://github.com/DereviankoYaroslav/FactorialPSO-CUBA.

4. Alejandro Freyre-Echevarr´ıa, Ismel Mart´ınez-D´ıaz. A new cost function to improve nonlinearity ofbijective S-boxes. URL: https://www.researchgate.net/publication/343699912_A_new_cost_function_to_improve_nonlinearity_of_bijective_S-boxes.

5. Alexandr Kuznetsov, Luca Romeo, Nikolay Poluyanenko, Sergey Kandiy, Kateryna Kuznetsova. Optimizing Hill Climbing Algorithm Parameters for Generation of Cryptographically Strong S-Boxes. URL: https://assets.researchsquare.com/files/rs-1657863/v1_covered.pdf?c=1653408505.

6. John A. Clark, Jeremy L. Jacob, Susan Stepney. The Design of S-Boxes by Simulated Annealing. URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.123.7114&rep=rep1&type=pdf.

Надійшла до редколегії 15.02.2022

Відомості про авторів:

Дерев'янко Ярослав Андрійович – студент кафедри безпеки інформаційних систем і технологій факультету комп'ютерних наук, Харківський національний університет імені В.Н. Каразіна, Україна; e-mail: yarik0009258@gmail.com; ORCID: https://orcid.org/0000-0002-3290-3373

Горбенко Юрій Іванович – канд. техн. наук, Харківський національний університет імені В.Н. Каразіна, старший науковий співробітник кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук; Україна; e-mail: gorbenkou@iit.kharkov.ua, ORCID: https://orcid.org/0000-0002-0652-8629

Кузнецов Олександр Олександрович – 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: kuznetsov@karazin.ua, ORCID: https://orcid.org/0000-0003-2331-6326

УДК 003.026:004.056 **DOI:10.30837/rt.2022.2.209.05**

Д.В. ГАРМАШ

АЛГОРИТМ RAINBOW ТА ЙОГО ЗДАТНІСТЬ ПРОТИДІЯТИ АТАКАМ RBS ТА 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. Потім впроваджуються схеми, які певний час витримували атаки: Unbalanced Oil and Vinegar (UOV), Rainbow та enTTS. Особлива увага приділяється атакам на алгоритм та його здатність їм протидіяти.

Атака RAINBOW-BAND-SEPARATION (RBS)

Атака Rainbow-Band-Separation відновлює секретний ключ Rainbow, розв'язуючи певні системи квадратичних рівнянь, а його складність оцінюється за відомим показником, який називається ступенем регулярності. Однак, як правило, ступінь регулярності більша, ніж ступінь розв'язання в експериментах, і точної оцінки отримати неможливо. Попередні методи оцінки [1, 4] для складності атаки RBS використовують ступінь регулярності як її показник за припущенням, що система квадратичних рівнянь, розв'язана в атаці, є напіврегулярною. Для напіврегулярної системи ступінь регулярності задається як ступінь D_{reg} першого члена, коефіцієнт якого непозитивний у ряді потужностей

$$\frac{(1-t^2)^m}{(1-t)^n}, \tag{1}$$

де m і n – числа рівнянь і змінних відповідно. Оскільки загальноприйнята квадратична система, що вирішується в прямій атаці, часто є напіврегулярною, то при оцінці складності прямої атаки використовується ступінь регулярності [1].

У роботі [5] запропоновано новий показник складності атаки Rainbow-Band-Separation за допомогою алгоритму F_4, який дає більш точну оцінку порівняно з показником, що використовує ступінь регулярності. Цей показник виводиться двома змінними рядами потужності

$$\frac{\prod_{i=1}^{m}(1-t_1^{d_{i1}}t_2^{d_{i2}})}{(1-t_1)^{n_1}(1-t_2)^{n_2}}, \tag{2}$$

що збігається з однозмінним рядом потужностей при $t_1=t_2$, виводячи ступінь регулярності. Крім того, показано залежність між атакою Rainbow-Band-Separation за допомогою гібридного підходу та атакою HighRank. Розглядаючи це відношення та показник, ми отримали нову оцінку складності для атаки Rainbow-Band-Separation. Отже, завдяки цьому, мож на зрозуміти точну безпеку Rainbow від атаки Rainbow-Band-Separation за допомогою алго ритму F_4.

Опис атаки RBS на схему підпису RAINBOW

Нехай m і n – натуральні числа. Позначимо через F кінцеве поле порядку q. Елемент $(f_1, ..., f_m)$ F $[x_1, ..., x_n]^m$ називається поліноміальною системою і дає відображення $F^n \to F^m$ на $a \to (f_1(a),...,f_m(a))$, яке називають поліноміальним відображенням (картою).

Багатовимірна схема підпису відкритого ключа складається з наступних трьох алгоритмів.

Генерація ключів: будуються дві обернені лінійні карти $S:F^n \to F^n$ і $T:F^m \to F^m$ випадковим чином і легко обернена квадратична карта $F: F^n \to F^m$, яку називають центральною картою, а потім обчислюється $P:=T \circ F \circ S$. Відкритий ключ подається у вигляді P. Кортеж (T, F, S) – секретний ключ.

Генерація підписів: для повідомлення $b \in F^m$ обчислюємо $b'=T^{-1}(b)$. Далі ми можемо обчислити елемент a' з $F^{-1}(\{b'\})$, оскільки F легко обернений. Отже, ми отримуємо підпис

$$a=S^{-1}(a') \in F^n.$$

Перевірка: перевіряється, чи $P(a)=b$ має місце. Для натуральних чисел v, o_1 і o_2, нехай $x=\{x_1, ..., x_v\}$, $y=\{y_1, ..., y_{o1}\}$ і $z=\{z_1, ..., z_{o2}\}$ будуть трьома змінними множинами і $n=v+o_1+o_2$, і $m=o_1+o_2$. Центральна карта $F=(f_1, ..., f_m) \in F[x, y, z]^m$ Rainbow

$$\begin{cases} f_1 = g^{(1)}(\mathbf{x}) + \sum_{i=1}^{o_1} l_i^{(1)}(\mathbf{x}) y_i, \\ \quad \vdots \\ f_{o_1} = g^{(o_1)}(\mathbf{x}) + \sum_{i=1}^{o_1} l_i^{(o_1)}(\mathbf{x}) y_i, \\ f_{o_1+1} = g^{(o_1+1)}(\mathbf{x}, \mathbf{y}) + \sum_{i=1}^{o_2} l_i^{(o_1+1)}(\mathbf{x}, \mathbf{y}) z_i, \\ \quad \vdots \\ f_{o_1+o_2} = g^{(o_1+o_2)}(\mathbf{x}, \mathbf{y}) + \sum_{i=1}^{o_2} l_i^{(o_1+o_2)}(\mathbf{x}, \mathbf{y}) z_i, \end{cases} \tag{3}$$

де $g^{(j)}$ та $l^{(j)}_i$ – випадковим чином обрані квадратичні многочлени та лінійні многочлени відповідно. Тоді за алгоритмом генерації підписів, наведеним вище, ми можемо легко обчислити елемент a' у попередньому зображенні будь-якого елемента $b'=(b'_1, ..., b'_{o1+o2})$ у F^m під F наступним чином.

1. Випадково обрати $a_v{}' = (a_1', ..., a_v')$ як x.
2. Вирішити систему лінійних рівнянь

$$f_1(\mathbf{a}'_v, \mathbf{y}) = b'_1, \ldots, f_{o_1}(\mathbf{a}'_v, \mathbf{y}) = b'_{o_1}.$$

Нехай $\mathbf{a}'_{o_1} = (a'_{v+1}, \ldots, a'_{v+o_1})$ є одним із її рішень, якщо воно існує. В іншому випадку повернутись до кроку 1.

3. Вирішити систему лінійних рівнянь

$$f_{o_1+1}(\mathbf{a}'_v, \mathbf{a}'_{o_1}, \mathbf{z}) = b'_{o_1+1}, \ldots, f_{o_1+o_2}(\mathbf{a}'_v, \mathbf{a}'_{o_1}, \mathbf{z}) = b'_{o_1+o_2}.$$

Нехай $\mathbf{a}'_{o_2} = (a'_{v+o_1+1}, \ldots, a'_{v+o_1+o_2})$ є одним із її рішень, якщо воно існує. В іншому випадку повернутись до кроку 1.

4. Отримати елемент $\mathbf{a}' = (a'_1, \ldots, a'_{v+o_1+o_2})$ у попередньому зображенні b'.

Нехай (v, o_1, o_2) – набір параметрів Rainbow, покладемо $n=v+o_1+o_2$ і $m=o_1+o_2$. Для відкритого ключа Rainbow $P=(p_1, ..., p_m)$ атака RBS відновлює свій секретний ключ (T, F, S) наступним чином. За визначенням (3) центральної карти $F=(f_1, ..., f_m)$ кожна матриця, відповідна f і має такий вигляд:

$$M_{f_i} = \begin{cases} \begin{pmatrix} *_{v\times v} & *_{v\times o_1} & 0_{v\times o_2} \\ *_{o_1\times v} & 0_{o_1\times o_1} & 0_{o_1\times o_2} \\ 0_{o_2\times v} & 0_{o_2\times o_1} & 0_{o_2\times o_2} \end{pmatrix} \text{ if } 1 \le i \le o_1, \\ \begin{pmatrix} *_{v\times v} & *_{v\times o_1} & *_{v\times o_2} \\ *_{o_1\times v} & *_{o_1\times o_1} & *_{o_1\times o_2} \\ *_{o_2\times v} & *_{o_2\times o_1} & 0_{o_2\times o_2} \end{pmatrix} \text{ if } o_1+1 \le i \le o_1+o_2. \end{cases} \tag{4}$$

Тут $*_{k\times l}$ означають k на l матриці над F. Аналогічно, матриці, відповідні S і T, можна записати наступним чином.

Матриці $M_{p1}, ..., M_{pm}$, що відповідають відкритим поліномам $p_1, ..., p_m$, задаються як

$$(M_{p_1}, \ldots, M_{p_m}) = (M_S M_{f_1}{}^t M_S, \ldots, M_S M_{f_m}{}^t M_S) M_T. \tag{5}$$

Існує вектор m на 1 t=(1,0 ...,0, λ_{v+o1+1}, ..., $\lambda_{v+o1+o2}$) такий, що $M_T \cdot {}^t t = {}^t(1,0, ..., 0)$. Потім, помноживши рівняння (5) на ${}^t t$, отримаємо

$$M_{p_1} + \sum_{i=1}^{o_2} \lambda_{v+o_1+i} M_{p_{o_1+i}} = M_S M_{f_1}{}^t M_S, \quad (6)$$

де e_k – це n на 1 вектор (0;...;0;1;0;...;0). Тут вилучаємо випадок $k=n$, оскільки рівняння (6) для $k=n$ випливає з рівняння (5).

Оскільки s = (λ_1, ..., λ_{v+o1}, 0, ..., 0,1), зрозуміло, що рівняння (5) і (7) є $n+m-1$ квадратичними рівняннями в n змінних λ_1,...,λ_n і будуються з відкритого ключа p_1,...,p_m. Вирішивши ці квадратичні системи, зловмисник може відновити частину секретного ключа S і T,а саме – s і t. Атака RBS може відновити S і T, повторюючи подібні обговорення, як описано вище (детальніше див. [2]).

Оскільки складність розв'язання квадратичної системи домінує в одній з атак RBS, достатньо оновити лише систему. Квадратична система, що складається з рівнянь (6) та (7), називається домінуючою системою RBS.

З досліджень [5] можна зробити висновок, що домінуюча система RBS є нерегулярною та дворівневою.

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:

- диференціального аналізу потужності на SFLASH;
- на секретні ключі від модуля SHA-1 схем SFLASH;.
- 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 за допомогою апаратного забезпечення [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 квантовим атакам. Ці задачі розглянуті 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 ; зааг. 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]. 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 07.05.2022

Відомості про автора:

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

УДК 003.026:004.056 **DOI:10.30837/rt.2022.2.209.06**

Г.А. МАЛЄЄВА

АНАЛІЗ АТАКИ ЧАСТКОВОГО ВІДНОВЛЕННЯ КЛЮЧА НА МУЛЬТИВАРІАТИВНІ КРИПТОГРАФІЧНІ ПЕРЕТВОРЕННЯ З ВИКОРИСТАННЯМ РАНГОВИХ СИСТЕМ

Вступ

Схема підпису Rainbow [1], запропонована Дінгом і Шмідтом у 2005 році, є однією з найстаріших і найбільш вивчених схем підпису в багатовимірній криптографії. Rainbow заснована на схемі підпису (unbalanced) Oil and Vinegar [2, 3], яка за правильно обраних параметрів мала необхідну криптостійкість починаючи з 1999 року. В останнє десятиліття збільшився інтерес до багатоваріантної криптографії, оскільки вважається, що вона є квантово стійкою.

Криптоаналіз Rainbow та його попередників активно розвивався на початку 2000-х років. Атаки з цієї епохи включають атаку MinRank, атаку HighRank, атаку Білле – Гілберта, атака погодження UOV та атака розподілу смуги Rainbow [4 – 8]. Після 2008 року криптоаналіз, здавалося, припинився, аж до участі Rainbow у проєкті NIST PQC, що послугувало мотиватором до продовження криптоаналізу. Під час другого раунд NIST, Бардет та інші запропонував новий алгоритм для розв'язування задачі MinRank [9]. Це різко підвищило ефективність атаки MinRank хоча й недостатньо, щоб загрожувати параметрам, поданим до NIST. Менш витратну з точки зору пам’яті версію цього алгоритму запропонувала Баена та ін. [10]. Перлнер і Сміт-Тон глибше проаналізували атаку розподілення смуги Rainbow, що показала, що атака була ефективнішою, ніж до цього вважалося[11]. Це спонукало команду Rainbow дещо збільшити параметри для третього туру. Під час третього раунду Белленс представив нову атаку [12], які знизили рівень безпеки Rainbow у 2^{20} разів для параметрів SL 1. Команда Rainbow стверджувала, що, незважаючи на нові атаки, параметри Rainbow все ще відповідають вимогам NIST [13].

У статті представлені дві нові атаки (часткового) відновлення ключа.

Розв’язування багатовимірних систем

Наші атаки використовують (у режимі чорної скриньки) процедуру, що задана однорідним багатовимірним квадратичним відображенням $\mathcal{P}: F_q^n \to F_q^m$, і знаходить ненульовий розв’язок *x* такий, що $\mathcal{P}(x) = 0$, якщо такий розв’язок існує. Ми розробили цю процедуру за допомогою блокового алгоритму Відемана XL [14 – 17]. Цей алгоритм будує велику, але дуже розріджену систему лінійних рівнянь і вирішує його за допомогою блокового алгоритму Відемана, використовуючи перевагами розрідженості системи.

Для експериментальної перевірки наших атак ми використали оптимізовану реалізацію блокового алгоритму Відеман XL авторів Cheng, Chou, Niederhagen та Yang [17]. Складність цього алгоритму на екземплярі з m випадкових однорідних рівнянь в n змінних можна оцінити як складність

$$3\binom{n-1+D}{D}^2\binom{n+1}{2}$$

множення поля, де D – *робочий ступінь* XL, який обирається найменшим цілим числом, коефіцієнт члена t^D у розкладанні степеневого ряду

$$\frac{(1-t^2)^m}{(1-t)^n}$$

є недодатним.

Приклад 1. Припустимо, що необхідно знайти розв'язок системи з 63 однорідних квадратних рівнянь з 31 змінною. Маємо

$$\frac{(1-t^2)^{63}}{(1-t)^{31}} = 1 + 31t + 433t^2 + 3503t^3 + 17081t^4 + 41447t^5 - 44919t^6 + O(t^7),$$

тож ми можемо запустити XL на ступені D = 6 з орієнтовною складністю

$$3\binom{31-1+6}{6}^2\binom{31+1}{2} \approx 2^{52.3}$$

множень поля.

Проста атака

Нехай $(pk = \mathcal{P}, sk = (O_1, O_2, W))$ – пара ключів Rainbow. Для будь-якого вектора $x \in F_q^n$, і будь-якого вектора $o_2 \in O_2$, за побудовою маємо, що $\mathcal{P}'(x, 2) \in W$. Отже, для будь-якого x ми розглянемо диференціал

$$D_x : F_q^n \to F_q^m : y \to \mathcal{P}'(x, y),$$

яка є лінійним відображенням з F_q^n до F_q^m, що, крім того, надсилає O_2 до W. Для будь-якого фіксованого відмінного від нуля x диференціал $D_x|O_2$, обмежений O_2, є рівномірно випадковим лінійним відображенням O_2 до W (по випадкових бітах алгоритму генерації ключа). Зазначимо що $dim(O_2) = dim(W) = o_2$, тому ймовірність того, що D_x має вектор ядра у O_2 – це саме ймовірність того, що випадкова матриця o_2 на o_2 над F_q є сингулярною. Матриця є не сингулярною, якщо перший рядок відмінний від нуля, і для кожного $i < o_2$, $i + 1 -$ й рядок не знаходиться в проміжку перших i рядків (що трапляється з імовірністю q^{i-1-o_2}), тому ймовірність бути сингулярною для матриці становить

$$1 - \prod_{i=0}^{o_2}\left(1 - q^{i-o_2}\right),$$

що близько до 1/q для достатньо великого q, незалежно від o_2. Наприклад, з q = 16, o_2 = 32, ймовірність приблизно 1/15,06.

Цільова атака тепер полягає в тому, щоб просто обрати випадковий (не нульовий) x, і сподіватися, що ядро D_x перетинає O_2 нетривіально, а потім спробувати знайти вектор o в цій інтерсекції. Оскільки $\mathcal{P}(o) = 0$ для всіх $o \in O_2$, запропоновано зробити це, розв'язавши наступну систему

$$\begin{cases} D_x o = 0 \\ \mathcal{P}(o) = 0 \end{cases}$$

Це система з m однорідних лінійних рівнянь і m однорідних квадратних рівнянь у n змінних o. Якщо ми використовуємо m лінійних рівнянь для усунення m змінних з квадратних рівнянь, ми отримуємо систему m однорідних рівнянь у $n - m$ змінних. Конкретно, нехай $B \in F_q^{n\times(n-m)}$ це матриця, стовпці якої утворюють основу для $ker(D_x)$, то ми шукаємо рішення $x \in F_q^{n-m}$ до $\tilde{\mathcal{P}}(x) = 0$, де $\tilde{\mathcal{P}}(x) := \mathcal{P}(Bx)$.

Атака в полях непарної характеристики. Коли q непарне, $\tilde{\mathcal{P}}$ поводиться як випадкова система з m однорідних квадратне рівняння в $n - m$ змінних в алгоритмі XL. Ранги XL системи точно відповідають рангам XL систем випадкових квадратичних рівнянь на кожному ступені операції D. Зокрема, якщо розв'язок $\mathcal{P}(x) = 0$ існує, ми можемо знайти його з орієнтовною вартістю

$$3\binom{n-m-1+D}{D}^2\binom{n-m+1}{2}$$

множення поля, де D – найменше натуральне число, таке, що t^D коефіцієнт розкладання по степеневому ряду $\frac{(1-t^2)^m}{(1-t)^{m-n}}$.

Атака в полях парної характеристики. Для парних q ранг систем XL не збігається з рангом випадкових систем, і застосування XL як у випадку непарної характеристики іноді не вдається. Причина полягає в тому, що $\mathcal{P}'(x,x) = 2\mathcal{P}(x)$ звертається до нуля в характеристиці 2, тому $x \in ker(D_x)$. Це означає існує $\tilde{x} \in F_q^{n-m}$(відомий зловмиснику) такий, що $\tilde{\mathcal{P}}(\tilde{x} + y) = \tilde{\mathcal{P}}(\tilde{x}) + \mathcal{P}(y)$ для всіх $y \in F_q^{n-m}$, що зазвичай не відбувається для випадкового $\tilde{\mathcal{P}}$. Добре, що це не становить проблеми для атаки, ми навіть можемо використовувати цю властивість, щоб зробити атаку трохи ефективнішою: необхідно знайти x такий, що $\tilde{\mathcal{P}}(x) = 0$. Нехай $Y \subset F_q^{n-m}$ будь-який підпростір розмірності $n - m - 1$, що не містить $\tilde{x}$, такий, що $\langle \tilde{x} \rangle + Y = F_q^{n-m}$. Тоді достатньо знайти $y \in Y$ таке, що $\tilde{\mathcal{P}}(y) = \alpha\tilde{\mathcal{P}}(\tilde{x})$ для деякого $\alpha \in F_q$, оскільки тоді $x = \tilde{x} + \alpha^{-1/2}y$ є рішення $\tilde{\mathcal{P}}(x) = 0$, (нагадаємо, що кожен елемент має квадратний корінь у полях характеристика 2, то $\alpha^{-1/2}$ існує), тому що

$$\tilde{\mathcal{P}}(\tilde{x} + \alpha^{-1/2}y) = \tilde{\mathcal{P}}(\tilde{x}) + \alpha^{-1}\tilde{\mathcal{P}}(y) = 0 .$$

Щоб знайти це $y \in Y$, ми обмежуємо $\tilde{\mathcal{P}}$ до Y і шукаємо рішення для $m - 1$ однорідних квадратних рівнянь

$$\hat{\mathcal{P}} := \{\tilde{p}_1 a_i - \tilde{p}_i a_1\}_{i=2}^{m} ,$$

де $a = \tilde{\mathcal{P}}(\tilde{x})$, і з втратою загальності припустимо, що $a_1 \neq 0$.

Обмеживши Y, ми видалимо проблемний вектор $\tilde{x}$, тому не дивно, що наші рангові експерименти показують, що нова система $\hat{\mathcal{P}}$ веде себе як система $m - 1$ випадкових однорідних квадратних рівнянь з $n - m - 1$ змінною. Тому, якщо рішення існує, можемо знайти його з орієнтовною вартістю

$$3\binom{n-m-2+D}{D}^2\binom{n-m}{2}$$

множення поля, де D – найменше натуральне число, таке, що t^D коефіцієнт розкладання по степеневому ряду $\frac{(1-t^2)^{m-1}}{(1-t)^{m-n-1}}$.

Виконання атаки. Як тільки вектор O_2 буде знайдено, другий шар Rainbow можна видалити, а безпека Rainbow зводиться до безпеки меншої системи UOV $m' = m - o_2$ рівнянь в $n' = n - o_2$ змінних (див. розділ 5.3 [12]). Для єдиного вектора o $\in O_2$ можна спочатку обчислити

$$\langle \mathcal{P}'(o, e_1), \ldots, \mathcal{P}'(o, e_n) \rangle \subset W ,$$

що з великою ймовірністю буде рівнянням. Нехай V — це зміна змінних, яка надсилає W до останніх o_2 координат F_q^m , і розбиває $V \circ \mathcal{P}$ як

$$V \circ \mathcal{P}(x) = \begin{cases} \mathcal{P}_1(x) \\ \mathcal{P}_2(x) \end{cases}$$

де $\mathcal{P}_1 : F_q^n \to F_q^{m-o_2}$ складається з перших $m - o_2$ координат $V \circ \mathcal{P}$ і $\mathcal{P}_2 : F_q^n \to F_q^{o_2}$ решти координат o_2. Тоді O_2 можна знайти як ядро лінійного відображення

$$o \to \begin{pmatrix} \mathcal{P}`_1(e_1, o) \\ \ldots \\ \mathcal{P}`_1(e_n, o) \end{pmatrix}.$$

Простір O_2 знаходиться в цьому ядрі, оскільки $\mathcal{P}`(x, o) \in W$ для всіх x $\in F_q^n$ і з великою долею ймовірності, маємо що ядро в точності дорівнює O_2. Тепер нехай U – зміна змінних, яка надсилає останні o_2 координати F_q^n до O_2, і нехай

$$V \circ \mathcal{P} \circ U(x) = F(x) = \begin{cases} F_1(x) \\ F_2(x) \end{cases},$$

де знову F_1 складається з перших $m - o_2$, а F_2 – з решти o_2 координат $V \circ \mathcal{P} \circ U$. Тоді F_1 залежить лише від перших $n - o_2$ записів x: нехай y – вектор, перші $n - o_2$ записів якого дорівнюють нулю, тоді $U(y) \in O_2$, тому $F_1(x + y) = F_1(x) + \mathcal{P}`_1 (U(x), U(y)) + \mathcal{P}(U(y)) = F_1(x)$. Крім того, F_1 звертається в нуль на $U^{-1} O_1$, оскільки $\mathcal{P}(O_1) \in W$. Отже, ігноруючи останні координати o_2, F_1 має структуру відкритого ключа UOV з $n' = n - o_2$ змінних і масляним простором розмірності $m' = m - o_2$.

Пошук прообразів для $\mathcal{P}$ еквівалентний пошуку прообразів для F, оскільки вони відрізняються трансформацією змінних, відомих зловмиснику. Тепер необхідно довести, що пошук прообразів для F зводиться до пошуку прообразів для F_1: припустимо, дано t = (t_1,t_2) і ми хочемо знайти *x* таке, що $F_1(x) = t_1$ і $F_2(x) = t_2$. Діємо наступним чином:

1. Знайти x таке, що $F_1(x) = t_1$ з деякою атакою на UOV з параметрами $(n', m') = (n - o_2, m - o_2)$,

2. Розв'яжіть для $o \in F_q^n$, у якого перших $n - o_2$ записів дорівнюють нулю так, що $F_2(x + o) = t2$. Це система o_2 лінійних рівнянь у o_2 змінних, оскільки $F_2(x + o) = F_2(x) + F'_2(x, o)$ є лінійною по o, тому o можна ефективно знайти.

3. Вихід $x + o$. Зверніть увагу, що $F_1(x + o) = F_1(x) = t_1$, оскільки F_1 залежить лише від перших $n - o_2$ змінних. Отже, $x + o$ дійсно є рішенням.

П р и м і т к а . Саме так працює справжній алгоритм підписання, за винятком того, що справжній підписувач володіє знаннями про O_1, що дозволяє йому ефективно виконувати перший крок.

Для наборів параметрів SL 1 у другому та третьому раундах NIST, F_1 є відображенням UOV, параметри якої (n', m') = (64,32) і (68,32) відповідно. У цих випадках атака Кіпніса – Шаміра [4], яка виконується за час $q^{n'-2m'} \cdot poly(n')$, може дуже ефективно відновити O_1, тому ми маємо повну атаку відновлення ключа. Для набору параметрів SL 3 і 5 екземпляри UOV можуть протистояти відомим атакам відновлення ключів, тому повна атака відновлення ключів здається недосяжною. Однак, оскільки $m' = m - o_2$ є відносно малим, ми все ще можемо вирішити $F_1(x) = t_1$, тому можливо підробити підписи без відновлення O_1. Для параметрів, поданих до NIST, вартість вирішення $F_1(x) = t_1$ за допомогою алгоритму Відемана XL нижча, ніж складність пошуку O_2 і W, тому складність атаки підробки переважає вартість пошуку O_2 і W .

Приклад 2. Набір параметрів SL1 другого раунду подання NIST дорівнює $q = 16, n = 96, m = 64, o_2 = 32$. Щоб знайти O_2 і W для цього набору параметрів, нам потрібно розв'язати системи $m - 1$ = 63 однорідні квадратні рівняння з $n - m - 1$=31 змінною, тому орієнтовна вартість розв'язання кожної системи становить 252,3 множення (див. приклад 1). У середньому нам потрібно перевірити 15,06 систем. Якщо вартість одного F_{16}-множення становить 36 процедур, то можемо оцінити, що загальна середня вартість елемента пошуку O_2 і W становить 252,3 · 15,06 · 36 ≈ 261,4. Після того як ми знайшли O_2 і W, у нас залишився відкритий ключ UOV з m′ = 32 рівняннями і n′ = 64 змінними. Отже, O_1 можна знайти за поліноміальний час з атакою Кіпніса – Шаміра[4]. У складності атаки переважає перший крок, який має складність ≈ 261,4, як зазначено в табл. 1.

Таблиця 1

Огляд вартості запропонованих атак у порівнянні з відомими атаками для шести наборів параметрів Rainbow які були подані до другого раунду та фіналу NIST PQC. Складність атак наведено у вигляді $\log_2$ прогнозуємої кількості операції. Складності відомих атак взяті з [12]. Для параметрів SL I наведено атаку відновлення ключа (позначено $*$), інші атаки є атаками підробки

Набір параметрів		q, n, m, o_2	Проста атака	Комбінована атака	Відомі атаки
Другий раунд	SL 1	(16, 96, 64, 32)	61*	93*	123*
	SL 3	(256, 140, 72, 36)	186	131	151
	SL 5	(256, 188, 96, 48)	246	164	191
Фіналісти	SL 1	(16, 100, 64, 32)	69*	99*	127*
	SL 3	(256, 148, 80, 48)	160	157	177
	SL 5	(256, 196, 100, 64)	257	206	226

Рангові експерименти

Проста атака. Для деяких наборів параметрів Rainbow над F_{31} створюємо певні $\tilde{\mathcal{P}}(x) = 0$ системи, як наведено у означеній простій атаці, і обчислюємо ранги матриці Маколея цих систем різного ступеня. Ці ранги відображаються в табл. 2. Аналогічно для деяких параметрів веселки над F_{16} ми будуємо певні $\hat{\mathcal{P}}(x) = 0$ системи, і відображаємо ранги матриць Маколея в табл. 3. Ми спостерігаємо в обох випадках, що ранги ідентичні рангам системи рівномірно випадкових квадратних рівнянь відповідних розмірів.

Тобто, якщо $\tilde{\mathcal{P}}(x)$ (або$\hat{\mathcal{P}}(x)$) має m рівнянь і n змінних, то ранг його Матриця Маколея на ступені D дорівнює коефіцієнту t^D в степеневому ряді розширення

$$(1 - t)^n(1 - (1 - t^2)^m),$$

якщо цей коефіцієнт додатний. Інакше система має ядро розмірності 1, що відповідає одномірному простору розв'язків. Це є свідченням того, що системи $\tilde{\mathcal{P}}(x) = 0$ і $\hat{\mathcal{P}}(x) = 0$ не мають конкретних відмінностей, які роблять їх легшими або складнішими для розв'язування в порівнянні з випадковими системами.

Комбінована атака. Табл. 4 надає інформацію про деякі з наших рангових експериментів для комбінованої атаки. Для деяких невеликих наборів параметрів Rainbow була виконана комбінована атака з розділу 4 для отримання екземпляра MinRank $n - m$ матриць з $n - 1$ рядками і m стовпцями (з яких ми зберігаємо m'). Потім були побудовані лінеаризовані системи, як вони рахуються в алгоритмі розв'язування MinRank за авторством Барде та ін. на кількох ступенях (b, 1), і обчислені їхні ранги. Виявилось для непарних характеристик ранг матриць Маколея завжди відповідає випадковим екземплярам MinRank з відповідними параметрами. Натомість, були виявлені невеликі дефекти рангів в двох характеристиках (підкреслені в табл. 4).

Таблиця 2

Ранг і кількість стовпців матриць Маколея для $\tilde{\mathcal{P}}(x) = 0$ система рівнянь простої атаки над F_{31}. Ранги матриці Маколея ступеня *D* виділено жирним шрифтом, якщо систему можна розв'язати на цьому ступені

Параметри Rainbow			Розмір $\tilde{\mathcal{P}}$			Ранг матриці Маколея ступеня *D*		
n	*m*	o_2	*m*	*n*		*D = 2*	*D = 3*	*D = 4*
30	20	10	20	10	Ранг Стовпички	20 55	200 220	**714** 715
45	30	15	30	15	Ранг Стовпички	30 120	450 680	**3059** 3060
60	40	20	40	20	Ранг Стовпички	40 210	800 1540	7620 8855

Таблиця 3

Ранг і кількість стовпців матриць Маколея для $\hat{\mathcal{P}}(\mathrm{x}) = 0$ система рівнянь простої атаки над F_{16} . Ранги матриці Маколея ступеня *D* виділено жирним шрифтом, якщо систему можна розв'язати на цьому ступені

Параметри Rainbow			Розмір $\hat{\mathcal{P}}$			Ранг матриці Маколея ступеня *D*		
n	*m*	o_2	*m*	*n*		*D = 2*	*D = 3*	*D = 4*
30	20	10	19	9	Ранг Стовпички	19 45	**164** 165	
36	24	12	23	11	Ранг Стовпички	23 66	253 286	**1000** 1001
42	28	14	27	13	Ранг Стовпички	27 91	351 455	**1819** 1820

Таблиця 4

Ранг і кількість стовпців матриць Маколея для проблеми MinRank внаслідок комбінованої атаки над F_{31} і F_{16}. Ранги матриці Маколея на бі-ступені (b, 1) виділені жирним шрифтом, якщо систему можна розв'язати на цьому ступені

Параметри Rainbow			Параметри MinRank			Ранг матриці Маколея бі-ступеня (*b*, 1)		
n	*m*	o_2	*k*	*m`*		*b = 1*	*b = 2*	*b = 3*
15	10	5	5	8	Ранг F_{31} Ранг F_{16} Стовпички	**279** **279** 280		
15	10	5	5	7	Ранг F_{31} Ранг F_{16} Стовпички	98 98 105	**314** **314** 315	
14	6	4	8	6	Ранг F_{31} Ранг F_{16} Стовпички	78 78 120	533 527 540	**1799** **1799** 1800

Результати та висновок

1. Вартість і ймовірність успіху атаки на практиці відповідають тому, що передбачає теорія. Очікується, що атака відновлення ключа проти набору параметрів SL 1, що подані Rainbow в третьому раунді, буде складніша лише на коефіцієнт 2^8, що хоч і вимагає від зловмисника більшої, проте все ще помірної кількості ресурсів.

2. Можливо було б перейти до більших параметрів для захисту від атаки, що представлена в цій статті, ціною більшого розміру ключів і підпису. Наприклад, параметри SL 3 подання третього раунду, схоже, забезпечують достатній рівень безпеки для SL 1, але ці параметри мають в 2,5 та 4,4 рази довший підпис та відкритий ключ порівняно з параметрами SL 1. Проте, схоже, також є потенціал для покращення атак, тому необхідно більше досліджень, перш ніж зможемо мати впевненість в безпеці Rainbow. Більше того, отримана схема підпису Rainbow була менш ефективною, ніж схема «Oil and Vinegar».

Список літератури:

1. Jintai Ding and Dieter Schmidt. Rainbow, a new multivariable polynomial signature scheme. In John Ioannidis, Angelos Keromytis, and Moti Yung, editors, ACNS 05, volume 3531 of LNCS, pages 164–175. Springer, Heidelberg, June 2005. 1.
2. Jacques Patarin. The oil and vinegar signature scheme. In Dagstuhl Workshop on Cryptography September, 1997, 1997. 1, 5.
3. Aviad Kipnis, Jacques Patarin, and Louis Goubin. Unbalanced oil and vinegar signature schemes. In Jacques Stern, editor, EUROCRYPT'99, volume 1592 of LNCS, pages 206–222. Springer, Heidelberg, May 1999. 1.
4. Aviad Kipnis and Adi Shamir. Cryptanalysis of the oil & vinegar signature scheme. In Hugo Krawczyk, editor, CRYPTO'98, volume 1462 of LNCS, pages 257–266. Springer, Heidelberg, August 1998. 1, 3, 4.
5. Bo-Yin Yang and Jiun-Ming Chen. Building secure tame-like multivariate public-key cryptosystems: The new TTS. In Colin Boyd and Juan Manuel Gonz´alez Nieto, editors, ACISP 05, volume 3574 of LNCS, pages 518–531. Springer, Hedelberg, July 2005. 1.
6. Olivier Billet and Henri Gilbert. Cryptanalysis of Rainbow. In Roberto De Prisco and Moti Yung, editors, SCN 06, volume 4116 of LNCS, pages 336–347. Springer, Heidelberg, September 2006. 1
7. Louis Goubin and Nicolas Courtois. Cryptanalysis of the TTM cryptosystem. In Tatsuaki Okamoto, editor, ASIACRYPT 2000, volume 1976 of LNCS, pages 44–57. Springer, Heidelberg, December 2000. 1.
8. Jintai Ding, Bo-Yin Yang, Chia-Hsin Owen Chen, Ming-Shing Chen, and Chen-Mou Cheng. New differential-algebraic attacks and reparametrization of Rainbow. In Steven M. Bellovin, Rosario Gennaro, Angelos D. Keromytis, and Moti Yung, editors, ACNS 08, volume 5037 of LNCS, pages 242–257. Springer, Heidelberg, June 2008. 1, 2.
9. Magali Bardet, Maxime Bros, Daniel Cabarcas, Philippe Gaborit, Ray A. Perlner, Daniel Smith-Tone, Jean-Pierre Tillich, and Javier A. Verbel. Improvements of algebraic attacks for solving the rank decoding and MinRank problems. In Shiho Moriai and Huaxiong Wang, editors, ASIACRYPT 2020, Part I, volume 12491 of LNCS, pages 507–536. Springer, Heidelberg, December 2020. 1, 2, 4, 5.
10. John Baena, Pierre Briaud, Daniel Cabarcas, Ray Perlner, Daniel Smith-Tone, and Javier Verbel. Improving support-minors rank attacks: applications to GeMSS and rainbow. Cryptology ePrint Archive, Report 2021/1677, 2021. https://eprint.iacr.org/2021/1677. 1
11. Ray Perlner and Daniel Smith-Tone. Rainbow band separation is better than we thought. Cryptology ePrint Archive, Report 2020/702, 2020. https://eprint.iacr.org/2020/702. 1
12. Ward Beullens. Improved cryptanalysis of UOV and rainbow. In Anne Canteaut and Fran¸cois-Xavier Standaert, editors, EUROCRYPT 2021, Part I, volume 12696 of LNCS, pages 348–373. Springer, Heidelberg, October 2021. 1, 1, 1, 2, 2, 3, 4, 5 14 Ward Beullens.
13. Response to recent paper by Ward Beullens. https://troll.iis.sinica.edu.tw/by-publ/recent/response-ward.pdf, 2020. 1.
14. Daniel Lazard. Gr¨obner bases, Gaussian elimination and resolution of systems of algebraic equations. In European Conference on Computer Algebra, pages 146– 156. Springer, 1983. 2.
15. Nicolas Courtois, Alexander Klimov, Jacques Patarin, and Adi Shamir. Efficient algorithms for solving overdefined systems of multivariate polynomial equations. In Bart Preneel, editor, EUROCRYPT 2000, volume 1807 of LNCS, pages 392–407. Springer, Heidelberg, May 2000. 2.
16. Wael Said Abdelmageed Mohamed, Jintai Ding, Thorsten Kleinjung, Stanislav Bulygin, and Johannes Buchmann. Pwxl: A parallel wiedemann-xl algorithm for solving polynomial equations over gf (2). In Conference on Symbolic Computation and Cryptography, page 89, 2010. 2.
17. Chen-Mou Cheng, Tung Chou, Ruben Niederhagen, and Bo-Yin Yang. Solving quadratic equations with XL on parallel architectures. In Emmanuel Prouff and Patrick Schaumont, editors, CHES 2012, volume 7428 of LNCS, pages 356–373. Springer, Heidelberg, September 2012. 2, 5.

Надійшла до редколегії 02.06.2022

Відомості про автора:

Малєєва Ганна Андріївна – аспірант кафедри безпеки інформаційних технологій, Харківський національний університет радіоелектроніки,Україна, e-mail: hanna.malieieva@nure.ua

УДК 004.056.5 **DOI:10.30837/rt.2022.2.209.07**

О.О. КУЗНЕЦОВ, д-р техн. наук, М.О ПОЛУЯНЕНКО, канд. техн. наук, С.О. КАНДІЙ, О.І. ПЕЛЮХ

ДОСЛІДЖЕННЯ НОВОЇ ФУНКЦІЇ ВАРТОСТІ ДЛЯ ГЕНЕРАЦІЇ ВИПАДКОВИХ ПІДСТАНОВОК СИМЕТРИЧНИХ ШИФРІВ

Вступ

Алгоритми блокового та потокового шифрування із секретним ключем застосовуються у різних додатках інформаційної безпеки [1, 2]. Зокрема, вони є головним компонентом безпеки в інтернеті та в сучасних телекомунікаційних мережах, використовуються для шифрування великих сховищ даних, тощо. Отже проєктування сучасних шифрів, які забезпечують високу швидкість перетворення та криптографічну стійкість, є актуальною та важливою задачею [1 – 3].

Сучасні погляди на проєктування шифрів із секретним ключем базуються на концепції substitution-permutation networks (SPN) [4, 5]. SPN використовує прості для реалізації криптографічні примітиви (підстановки та перестановки), які у сукупності забезпечують властивості confusion та diffusion [6]. Ці властивості перешкоджають застосуванню статистичного, диференціального, лінійного та інших методів криптоаналізу [7 – 10]. Зокрема підстановки (substitutions, S-boxes) вносять нелінійність у співвідношення відкритий текст-шифр текст та забезпечують властивість confusion. Для захищеності від алгебраїчного криптоаналізу S-boxes повинні бути також випадковими [11 – 13], тобто підстановки не повинні містити простих алгебраїчних конструкцій, як, наприклад, в S-box шифрі AES [4, 14, 15].

Слід зазначити, що генерація криптографічно стійких випадкових підстановок є складною обчислювальною задачею. Зазвичай генерацію здійснюють алгоритмами локального пошуку: Hill climbing Algorithm [16 – 19]; Simulated Annealing [20, 21]; Genetic Algorithm [22 – 24] та інші. Це ітеративні алгоритми, пошук цільового рішення якими здійснюється із застосуванням спеціальних функцій вартості. На кожній ітерації алгоритм пошуку змінює поточний стан доки не буде досягнуто умову виходу: знаходження цільового рішення або виконання певної кількості ітерацій. Фактично, пошук цільового S-box здійснюється шляхом мінімізації (інколи максимізації) функції вартості. Однак пошук екстремуму та генерація високонелінійних S-boxes є надзвичайно складним завданням. Наприклад, для найбільш швидкого відомого результату для генерації S-box із нелінійністю 104 необхідно виконати не менше 65 тисяч ітерацій [18, 25].

В статті пропонується нова функція вартості та досліджується ефективність генерації високонелінійних випадкових S-box. Реалізовано Hill climbing алгоритм та проведено серію експериментів з генерації підстановок. Показано, що складність пошуку можна суттєво зменшити. Зокрема, для генерації S-box із нелінійністю 104 необхідно виконати менше 50 тисяч ітерацій.

Пов’язані роботи

Алгоритми локальної оптимізації для генерації високонелінійних підстановок досліджуються багатьма авторами. Зокрема, у [16 – 19] досліджено Hill climbing алгоритм; у [7, 18, 20, 25] розглянуто Local Search Algorithm [7, 18, 20, 25]; у роботах [17, 26 – 28] та [20, 21] вивчено simulated annealing; роботи [22–24] присвячено Genetic Algorithm і т.д.

Ці алгоритми застосовують різні функції вартості. Зокрема, найбільш дослідженою та поширеною є функція вартості Кларка (Clark’s cost functions). Ця функція based on Walsh-Hadamard Spectra (WHS). Вперше її було запропоновано в [26]. Дослідження її поведінки та певну модифікацію виконано в [20, 21].

В роботах [18, 29] Picek та іншими авторами було запропоновано нову функцію вартості. Picek's cost functions для деяких алгоритмів виявилася більш ефективнішою у порівнянні із WHS.

В [18, 25] Freyre-Echevarría та іншими було запропоновано нову функцію WCF (Cost Function of the content of the Walsh-Hadamard spectrum). Як виявилося, вона дозволяє як найшвидше сформувати випадкові бієктивні 8-бітні S-boxes. Кращим алгоритмом пошуку виявився Hill climbing. Наприклад, для генерації S-boxes із нелінійністю 104 йому необхідно в середньому понад 65 тисяч ітерацій. Це кращий відомий результат. Далі показано, що запропонована в цій статті функція вартості дозволяє зменшити кількість ітерацій Hill climbing алгоритму до 50 тисяч.

Передумова

За визначенням S-box є нелінійною підстановкою $S:\{0,1\}^n \to \{0,1\}^m$, яку зазвичай подають у вигляді координатних булевих функцій $F(x)=(f_1, f_2,..., f_m)$ [10, 30]:

$$f_1(x_1, x_2,..., x_n) = y_1,$$
$$f_2(x_1, x_2,..., x_n) = y_2,$$
$$...$$
$$f_m(x_1, x_2,..., x_n) = y_m.$$

В цій роботі розглядаються 8-бітні бієктивні підстановки, тобто $n=m=8$.

Основним криптографічним показником S-box є нелінійність $N(S)$, яку розраховують за формулою [30]:

$$N(S) = \min_{v\in\{0,1\}^m\setminus\{0\}^m}\{N(v\cdot F(x))\} = \frac{1}{2}(2^8 - WHT_{\max}), \quad (1)$$

де

$$WHT_{\max} = \max_{v,u\in\{0,1\}^m\setminus\{0\}^m}\left|WHT(v\cdot F(x),u)\right|,$$
$$WHT(f(x),u) = \sum_{x\in\{0,1\}^n}(-1)^{f(x)\oplus u\cdot x}. \quad 2)$$

Таким чином, нелінійність $N(S)$ визначається через перетворення Уолша – Адамара $WHT(f(x),u)$ булевої функції $f(x)=v\cdot F(x)$. Саме коефіцієнти $WHT(f(x),u)$ визначають $N(S)$. Тому функції вартості повинні враховувати значення $WHT(f(x),u)$ з метою максимізації $N(S)$ з (1), тобто максимізації мінімуму нелінійності за всіма булевими функціями $v\cdot F(x)$.

Для пошуку випадкових S-boxes на сьогодні використовують декілька функцій вартості. Перша та найбільш досліджена функція вартості WHS запропонована у [31], вона базується на врахуванні коефіцієнтів Уолша – Адамара:

$$WHS = \sum_{v\in\{0,1\}^m}\sum_{u\in\{0,1\}^n}\left|\,|WHT(v\cdot F(x),u)| - X\right|^R, \quad (3)$$

де X и R – параметри функції, які потрібно підібрати для мінімізації ітерацій пошуку.

Функція WHS використовувалася в багатьох пов'язаних роботах. Наприклад, в одній з останніх публікацій показано, що із її використанням вдається формувати 8-бітну бієктивну підстановку із $N(S)=104$ [25]. Але складність такого пошуку занадто велика. В середньому генерація вимагає близько 3,8 мільйонів ітерацій. При цьому використовувався варіант генетичного алгоритму пошуку.

В роботі [29] Picek та іншими авторами запропоновано іншу функцію. Вона заснована на врахуванні лише позицій ненульових коефіцієнтів $WHT(f(x),u)$. Функція вартості обраховується за формулою

$$PCF = \sum_{i=1}^{N} 2^{-i} H(S)_{k-i}, \tag{4}$$

де $H(S)$ – вектор значень $|WHT(v \cdot F(x), u)|$, в якому на i-й позиції вказано число коефіцієнтів с значеннями $|4i|$, k – максимальний номер позиції з ненульовим значенням.

В роботі [29] проведено низку експериментів, які показали, що функція вартості (4) є значно ефективнішою за (3). З тим же алгоритмом пошуку вона вимагає лише 167 451 ітерацій для генерації S-boxes із $N(S) = 104$.

Останній варіант функції вартості WCF було запропоновано в [18, 25]. Вона обчислюється за формулою:

$$WCF = \sum_{v \in \{0,1\}^m} \sum_{u \in \{0,1\}^n} \prod_{z \in C} \| WHT(v \cdot F(x), u) | - z |, \tag{5}$$

где $C = \{0, 4, ..., 32\}$.

За результатами експериментів в [18, 25] ця функція вартості виявилася найбільш ефективною. Зокрема, в поєднанні із Hill climbing алгоритмом вона вимагає лише біля 65 тисяч ітерацій для генерації випадкових S-boxes із $N(S) = 104$. Це кращий із відомих на сьогодні результат.

Запропонована функція вартості WCFS

Для обґрунтування нової функції вартості розглянемо розподіл значень (2) для випадково сгенерованого S-box. Приклад такого розподілу наведено на рис. 1.

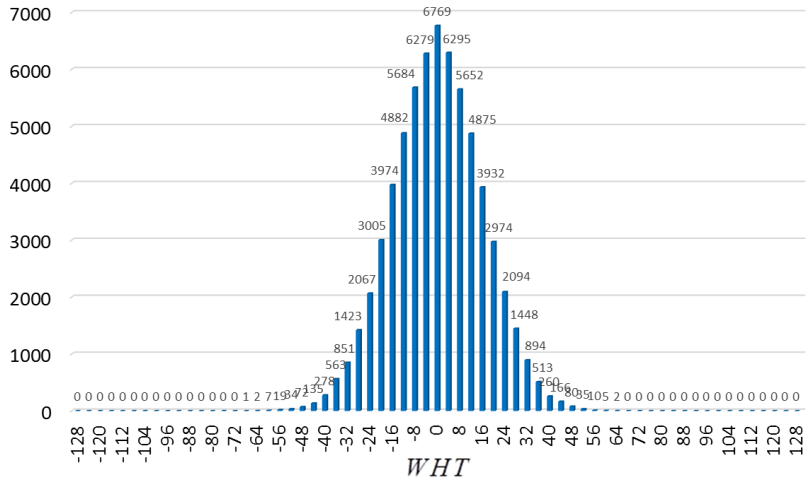


Рис. 1. Приклад розподілу значень спектральних коефіцієнтів Уолша – Адамара для випадково сформованого бієктивного S-блоку

За нашими дослідженнями виявилося, що для підрахунку функції вартості переважним є спосіб урахування окремих коефіцієнтів (2). Оскільки нелінійність (1) обраховується за максимальними значеннями $|WHT(v \cdot F(x), u)|$, то пріоритетними повинні бути крайні значення спектру з рис. 1. По мірі наближення коефіцієнтів $|WHT(v \cdot F(x), u)|$ до центральної частини розподілу їх вплив на функцію вартості повинен значно зменшуватись.

Таким чином, на кожній ітерації алгоритму оптимізації нас у першу чергу цікавить зменшення крайніх коефіцієнтів. Групування інших коефіцієнтів до центру розподілу буде полегшувати підвищення нелінійності на наступних ітераціях алгоритму. Отже, необхідно враховувати кожний спектральний коефіцієнт з деяким ваговим коефіцієнтом. Чим ближче коефіцієнт до нуля – тим нижче його вага. У функції (5) це реалізовано за рахунок добутку, при-

чому, спектральні коефіцієнти від нуля до 32 включно взагалі не ураховуються (внаслідок множення на нуль), а значення добутку зростає пропорційно позиції спектрального коефіцієнта у розподілу.

Схоже вагове урахування реалізовано у функції (3). Наприклад, при $R=12$ та $X=0$ коефіцієнти спектру Уолша – Адамара, які знаходяться на крайніх позиціях, мають більш вагомий внесок у значення функції вартості, ніж коефіцієнти, які знаходяться ближчі до центру у розподілу.

Базуючись на отриманих результатах, можна зробити висновок, що більш швидке знаходження S-блоку відбувається при урахуванні лише деяких крайніх значень спектру Уолша – Адамара. З цього приводу нами пропонується нова цільова функція WCFS, яка є деяким гібридним рішенням між функціями WHS та WCF. В ній враховуються лише коефіцієнти, які більш деякого значення X, що відповідає виразу $|WHT|>X$. Також доцільним є зменшення значень, що враховуються, на X та у 4 рази, що призведе до постійного та рівномірного порядку зростання (1,2,3,…) значень спектральних коефіцієнтів, що враховуються. Вагове урахування позицій спектральних коефіцієнтів у розподілі реалізуємо у вигляді возведення у деяку ступінь R отриманої позиції спектральних коефіцієнтів. Нижче наведено формальний опис запропонованої цільової функції:

$$WCFS=\sum_{\substack{b=1\\ |WHT[b,i]|>X}}^{255}\sum_{i=0}^{255}\left(\frac{|WHT[b,i]|-X}{4}\right)^{R}. \tag{6}$$

Параметри X та R повинні бути підібрані з метою підвищення ефективності генерації підстановок.

Тестування та оптимізація параметрів нової функції вартості

Для підбору оптимального значення параметрів X та R розглянемо, як буде змінюватися вплив запропонованої функції (6) на швидкість пошуку. Швидкість будемо вимірювати в кількості ітерацій.

У якості методу пошуку будемо використовувати Hill climbing алгоритм. Псевдокод цього алгоритму наведено у додатку роботи [18]. Пошук починається із випадково сформованої бієктивної підстановки S_0. Критерієм зупинки алгоритму є досягнення загальної кількості ітерацій N_1. Додатково введено ще два критерії зупинки алгоритму, а саме:

- досягнення максимальної кількості N_2 поспіль виконаних ітерацій, при яких не знайдено жодного покращення функції вартості;
- досягнення цільового значення нелінійності підстановки N_3, розрахованого за формулою (1).

Отже наш варіант Hill climbing алгоритму подаємо у наступному вигляді.

Pseudo-Code of the Hill Climbing Algorithm

Вхід: S_0, N_1, N_2, N_3.

$S \leftarrow S_0$, $n \leftarrow 0$;

While ($N_1 > 0$) and ($n < N_2$) and ($N(S) < N_3$) do:

$S' \leftarrow S$;

Select at random two different positions i and j and swap the outputs on S' corresponding to i and j;

if $WCFS(S') \le WCFS(S)$ then

$S \leftarrow S'$, $n \leftarrow 0$;

else

$n \leftarrow n+1$;

$N_1 \leftarrow N_1 - 1$;

Return S.

Таким чином, на кожній ітерації алгоритму модифікується поточне значення підстановки S, в результаті отримуємо S-box S'. Далі розраховуємо значення функції вартості $WCFS(S')$ за формулою (6) та порівнюємо його із значенням $WCFS(S)$ для поточного S-box S. Якщо значення функції вартості не збільшилося, тоді S' приймається за кращий поточний результат.

Початкова підстановка S_0 формувалася випадковим чином.

Параметри зупинки алгоритму обрано наступні:

$N_1 = 1\,000\,000$,

$N_2 = 100\,000$,

$N_3 = 104$.

При тестуванні параметри X та R змінювались у діапазоні:

$-32 \geq X \geq 32$ з кроком 4;

$5 \geq R \geq 18$ з кроком 1.

Зауважимо, що при $X = 48$ та $N(S) = 104$ маємо значення функції $WCFS = 0$.

Для кожного параметру X та R, з метою усереднення результатів, проводилось 100 запусків Hill climbing алгоритму.

Результати досліджень усередненої кількості ітерацій пошуку наведено у табл. 1 та візуалізовано на рис. 1. Крім наведених даних для кожного вдалого запуску (тобто коли був знайдений S-блок з нелінійністю 104) також фіксуємо кількість ітерації алгоритму пошуку, які було виконано для досягнення нелінійності 100 та 102. Усереднені кількості ітерації наведено у табл. 2 і 3 та візуалізовано на рис. 2 і 3 відповідно.

Символом «–» у табл. 1 – 3 позначено випадки, коли алгоритмом пошуку було знайдено цільовий S-блок менш ніж у 50 % випробувань та отримані результати не можуть характеризувати необхідну для пошуку кількість ітерації. У табл. 4 наведено відсоток окремих запусків, за результатом яких було знайдено бієктивний S-блок з нелінійністю 104.

Таблиця 1

Середньоарифметична кількість ітерацій, які було виконано
до знаходження бієктивного S-блоку з нелінійністю 104 при використанні функції WCFS

X	R													
	5	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**
-32	–	–	–	–	–	231762	155358	119041	103349	75955	69554	61694	54840	55188
-28	–	–	–	–	–	157544	133267	108750	86979	70292	61496	58275	56007	57114
-24	–	–	–	–	184299	174331	113341	90294	74057	62517	58270	61259	**52476**	54384
-20	–	–	–	–	162916	126207	97274	74575	70495	61759	53146	**52547**	53902	**53678**
-16	–	–	–	–	151538	99170	84834	68011	61772	51375	56735	54452	53260	56557
-12	–	–	–	183600	123348	93124	67811	58808	**54800**	50732	**50934**	53289	58196	56962
-8	–	–	197322	157799	104289	77086	60823	53292	56088	**49399**	58393	59345	62675	60460
-4	–	–	179263	119941	92926	70066	52260	**50438**	56295	53192	55211	66722	69403	74278
0	–	–	141912	96838	79239	57095	53509	54924	55990	58531	62098	66465	84083	84002
4	–	184668	111097	77850	65663	56931	**50238**	56603	57259	63593	68088	88000	89250	109897
8	–	148482	90091	63921	56935	**50798**	56814	56123	65781	76237	79544	100726	120771	132152
12	171440	103464	66827	**53062**	**52809**	58960	60873	62813	75322	84133	116092	121023	145128	150432
16	131424	78297	63295	57519	55367	60144	71509	87545	97420	119710	138424	–	–	–
20	86714	60656	**51971**	56974	65052	78869	92354	115900	123319	123864	–	–	–	–
24	65010	**54329**	62361	67914	86958	105767	129225	150163	–	–	–	–	–	–
28	**56280**	63986	70787	95384	111413	146470	–	–	–	–	–	–	–	–
32	67049	80236	108002	134489	–	–	–	–	–	–	–	–	–	–

Таблиця 2

Середньоарифметична кількість ітерацій, які було виконано
до знаходження бієктивного S-блоку з нелінійністю 102 при використанні функції WCFS

X	*R*													
	5	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**
-32	–	–	–	–	–	1985	1726	1476	1407	1195	1092	1075	1019	965
-28	–	–	–	–	–	1805	1574	1388	1199	1137	1064	1018	984	959
-24	–	–	–	–	2342	1794	1482	1267	1188	1096	1072	1036	996	924
-20	–	–	–	–	1919	1607	1333	1165	1130	1032	1007	957	1002	952
-16	–	–	–	–	1867	1475	1262	1162	1092	992	967	953	**905**	**894**
-12	–	–	–	2235	1557	1291	1195	1083	1024	1025	972	991	924	970
-8	–	–	2446	1672	1353	1257	1107	1008	998	949	**896**	**878**	936	958
-4	–	–	2023	1478	1271	1088	1072	**939**	998	964	949	985	974	979
0	–	–	1732	1384	1181	1049	981	964	**922**	**940**	972	983	991	1008
4	–	2127	1484	1193	1067	976	**943**	944	937	948	947	1010	1067	1081
8	–	1785	1346	1137	1024	952	965	960	964	967	1018	1070	1128	1091
12	2274	1336	1172	1037	968	**932**	953	972	1009	1050	1049	1046	1119	1353
16	1703	1289	1101	985	**952**	933	1012	996	1114	1022	1116	–	–	–
20	1446	1096	972	973	997	995	969	1015	1094	1196	–	–	–	–
24	1219	1063	923	**913**	971	1005	1053	1158	–	–	–	–	–	–
28	1020	**945**	**915**	966	1015	1204	–	–	–	–	–	–	–	–
32	**974**	961	1001	1151	–	–	–	–	–	–	–	–	–	–

Таблиця 3

Середньоарифметична кількість ітерацій, які було виконано
до знаходження бієктивного S-блоку з нелінійністю 100 при використанні функції WCFS

X	*R*													
	5	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**
-32	–	–	–	–	–	276	231	208	189	179	178	166	151	157
-28	–	–	–	–	–	246	203	194	191	170	166	161	153	154
-24	–	–	–	–	287	230	213	189	181	169	162	153	153	138
-20	–	–	–	–	252	218	202	186	174	163	166	154	148	150
-16	–	–	–	–	232	200	202	170	164	157	164	161	148	149
-12	–	–	–	250	215	199	183	183	168	153	152	148	147	140
-8	–	–	270	233	207	184	173	161	154	151	146	145	145	147
-4	–	–	255	232	196	175	160	165	143	142	147	143	144	143
0	–	–	235	200	183	159	161	156	155	148	148	149	142	142
4	–	259	232	191	173	161	153	149	145	152	142	145	147	149
8	–	238	201	171	164	151	152	144	150	139	143	146	138	139
12	267	220	193	157	153	145	146	148	145	146	147	151	146	143
16	250	191	176	153	151	134	143	150	140	141	158	–	–	–
20	207	182	163	152	146	144	145	144	144	145	–	–	–	–
24	185	168	150	147	149	140	147	145	–	–	–	–	–	–
28	162	154	143	145	154	141	–	–	–	–	–	–	–	–
32	153	148	145	136	–	–	–	–	–	–	–	–	–	–

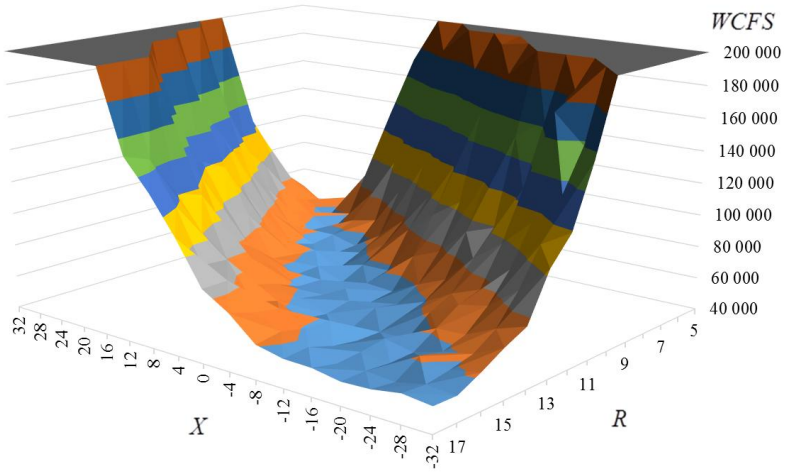


Рис. 2. Середньостатистична кількість ітерацій, які було виконано до знаходження бієктивного S-блоку з нелінійністю 104 при використанні функції $WCFS$ при різних параметрах X та R

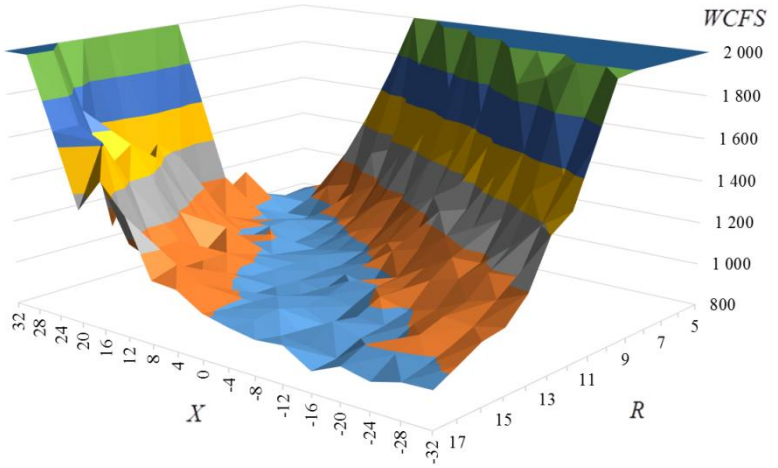


Рис. 3. Середньостатистична кількість ітерацій, які було виконано до знаходження бієктивного S-блоку з нелінійністю 102 при використанні функції $WCFS$ при різних параметрах X та R

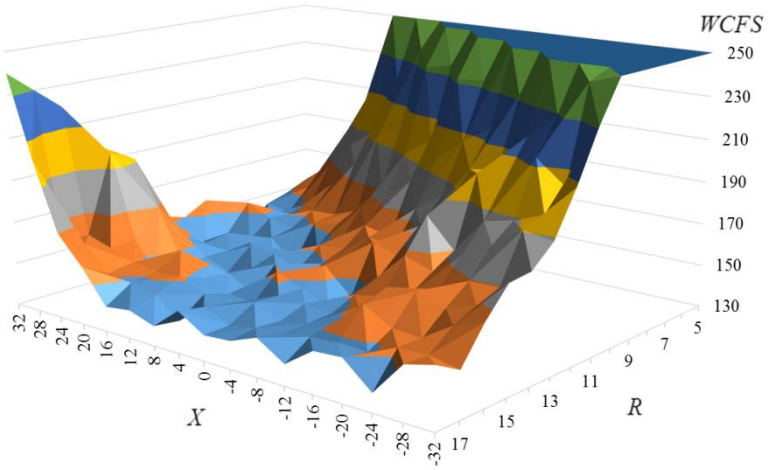


Рис. 4. Середньостатистична кількість ітерацій, які було виконано до знаходження бієктивного S-блоку з нелінійністю 100 при використанні функції $WCFS$ при різних параметрах X та R

Таблиця 4

Кількість знайдених (під час досліджень) бієктивних S-блоків з нелінійністю 104 при використанні функції WCFS

X	R													
	5	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**
-32	1	0	2	10	48	61	86	95	98	99	100	99	100	100
-28	1	1	3	13	35	70	94	99	96	99	99	100	100	100
-24	1	0	7	26	51	87	94	95	100	100	100	100	100	100
-20	0	0	8	36	73	89	98	98	99	100	99	100	100	100
-16	0	3	18	47	84	92	99	100	99	100	100	100	100	100
-12	1	11	34	73	92	98	100	100	100	100	100	99	100	100
-8	2	9	50	85	99	98	100	99	100	100	99	100	99	99
-4	2	34	67	91	100	99	100	100	100	99	100	100	99	100
0	8	47	90	97	98	100	100	99	100	100	100	100	99	95
4	14	56	93	99	100	100	100	100	99	99	99	99	90	92
8	41	85	99	99	100	99	100	99	98	100	97	97	90	80
12	59	97	99	99	100	100	100	100	100	96	88	68	73	55
16	87	97	100	100	99	100	99	98	90	83	72	47	27	19
20	97	100	100	100	99	98	96	82	64	53	35	25	9	7
24	99	100	100	98	98	92	75	60	40	20	17	14	3	2
28	100	99	99	94	84	58	32	13	11	5	1	2	0	1
32	100	98	94	61	35	22	5	3	1	2	3	1	1	3

Обговорення результатів

Отримані результати тестування демонструють високу ефективність запропонованої функції вартості WCFS. Зокрема, для функції (6) існує великий діапазон значень параметрів X та R, для яких генерація підстановок є дуже швидкою. Наприклад, для параметрів $R=14$ та $X=$-8 середньостатистична кількість ітерацій алгоритму пошуку бієктивних S-блоків з нелінійністю 104 склала 49 399 ітерацій. Це суттєво менш ніж при використанні функції WCF (понад 65 тисяч операцій) з [18, 25]. Крім того, як бачимо з наведених результатів, майже при будь-якому значенні X можливо підібрати вагове значення R з дуже швидким знаходженням S-блоку.

Синім кольором у табл. 1 позначено випадки коли середня кількість ітерації скла менш за 60 000, а темно-синім – менш за 55 000 ітерації. Область мінімальних значень середньої кількості ітерації відповідає співвідношенню параметрів X та R, які емпірично можна визначити формулою

$$X = 48 - 4 \cdot R. \tag{7}$$

Значення параметрів X та R, які відповідають співвідношенню (7), у табл. 1 обведені рамкою. Експериментально встановлені мінімальні значення середньої кількості ітерації для кожного R позначено жирним шрифтом. Як бачимо, позиції, які відповідають співвідношенню (7), та знайдені мінімальні значення, у більшості випадках співпадають або знаходяться дуже близько один до одного (у межах обчислювальної похибки). Отже формулу (7) можна використовувати для швидкого підбору найбільш придатних співвідношень X та R.

Слід зазначити, що середня кількість ітерацій для параметрів X та R, яка відповідає співвідношенню (7), також не є однорядною та має мінімальне значення в області $R=12\pm3$. При зменшені або збільшенні значення R від області $R=12\pm3$ середня кількість ітерації починає зростати.

Для мінімізації обчислювальних ресурсів при розрахунку функції вартості необхідним є зменшення значення R. В цій роботі проведено тестування середнього часу обчислення функції *WCFS* в залежності від обраного значення R (при $X=48-4\cdot R$). Отримані результати наведено у табл. 5. Розрахунок виконувався на персональному комп'ютері Intel Core i5-3210M CPU 2.50GHz під керуванням 64-розрядної операційної системи

Windows 7. Компіляція коду, написаного на C++, виконувалась за допомогою Microsoft Visual Studio Community 2022 (64-розрядна версія) у Release конфігурації.

Таблиця 5

Середній час обчислення цільової функції *WCFS* при різних параметрах

Параметр	**Час виконання обчислення функції *WCFS*, с**
$R=5, X=28$	$1{,}06\cdot10^{-3}$
$R=6, X=24$	$1{,}09\cdot10^{-3}$
$R=7, X=20$	$1{,}13\cdot10^{-3}$
$R=8, X=16$	$1{,}22\cdot10^{-3}$
$R=9, X=12$	$1{,}24\cdot10^{-3}$
$R=10, X=8$	$1{,}32\cdot10^{-3}$
$R=11, X=4$	$1{,}30\cdot10^{-3}$
$R=12, X=0$	$1{,}28\cdot10^{-3}$
$R=13, X=-4$	$1{,}30\cdot10^{-3}$
$R=14, X=-8$	$1{,}32\cdot10^{-3}$
$R=15, X=-12$	$1{,}37\cdot10^{-3}$
$R=16, X=-16$	$1{,}38\cdot10^{-3}$
$R=17, X=-20$	$1{,}39\cdot10^{-3}$
$R=18, X=-24$	$1{,}41\cdot10^{-3}$

Наші дослідження показують, що при дотриманні вимоги (7) ймовірність знаходження бієктивного S-блоку з $N(S)=104$, при обраних параметрах алгоритму пошуку, близька до 1 (див. табл.4). Зі збільшенням значення R відповідно збільшується діапазон значень X, при яких ймовірність і середня кількість ітерації знаходяться у своїх кращих значень для обраних R.

В табл. 2 та 3 наведено результати генерації S-блоків з $N(S)=102$ та $N(S)=100$ відповідно.

У табл. 2 синім кольором позначено випадки, коли середня кількість ітерації скла менш за 1 000, а темно-синім – менш за 950 ітерації. Спостерігається схожий характер розподілу з областю мінімальної кількості ітерацій до розподілу з $N(S)=104$. Однак область мінімальних значень буде відповідати співвідношенню

$$X=52-4\cdot R. \tag{8}$$

Чарунки, які відповідають цьому співвідношенню, позначені рамкою. Мінімальні значення для кожного R виділені жирним шрифтом. Також спостерігається добрий збіг мінімальних значень з емпіричним співвідношенням (8).

Для генерації бієктивних S-блоків з $N(S)=100$ (див. табл. 3) також можна виділити область мінімальних значень які будуть відповідати емпіричному співвідношенню

$$X=56-4\cdot R. \tag{9}$$

Узагальнюючи область мінімальної кількості ітерації для різних значень нелінійності найкраще співвідношення параметрів X та R буде відповідати емпіричній залежності:

$$X=2\cdot(128-N(S))-4\cdot R \tag{10}$$

та імовірно найкраще обрати

$$R = \frac{128 - N(S)}{2}. \quad (11)$$

При обранні рекомендованих формулами (10) та (11) параметрів функції *WCFS* середньо-арифметична кількість ітерацій до знаходження цільового S-блоку буде складати:

- близько 52 200 ітерацій при $N(S) = 104$;
- близько 950 ітерацій при $N(S) = 102$;
- близько 148 ітерацій при $N(S) = 100$.

Кращий результат генерації S-блоків з $N(S) = 104$ дає функція *WCFS* з параметрами $X = -8$ and $R = 14$. При цьому Hill climbing алгоритму необхідно в середньому 49399 ітерацій.

Для порівняння отриманих результатів в табл. 6 наведено кращі відомі результати з генерації нелінійних підстановок з $N(S) = 104$.

Таблиця 6

Порівняння отриманих результатів з генерації нелінійних підстановок з $N(S) = 104$

Parameters	[31]	[29]	[18]	[25]	Our work
Generation Method	«Genetic and Tree»	«Genetic and Tree»	Hill climbing	Hill climbing	Hill climbing
Cost function, parameters	WHS, $X = 21$ and $R = 7$	PCF, $N_p = 10$	WCF	WCF	WCFS, $X = -8$ and $R = 14$
Average number of iterations	3 239 000	167 451	70 596	65 933	49 399

Як бачимо, запропонована функція вартості в наших експериментах показує значне покращення. Зокрема, середню кількість ітерацій зменшено на понад 20 % в порівнянні з кращим відомим результатом.

Висновки

Запропоновано та досліджено нову функцію вартості WCFS. Використання WCFS дозволяє підвищити ефективність евристичного пошуку нелінійних підстановок. Крім того, частка успішних запусків алгоритму генерації досягає 100 %. В наших тестуваннях застосовувався Hill climbing алгоритм. В порівнянні з кращим відомим результатом генерації S-блоків з $N(S) = 104$ нам вдалося більше ніж на 20 % скоротити кількість ітерацій.

Проведені тестування дозволили виділити область параметрів функції вартості, для якої спостерігається найменша кількість ітерацій. Введено емпіричну залежність між параметрами X та R. Результати тестування майже повністю збігаються із цією емпіричною залежністю. Отже маємо змогу швидко підбирати параметри нової функції вартості WCFS для генерації S-блоків.

Використання функції WCFS в алгоритмі Hill climbing дало кращі результати в порівнянні з функціями вартості *WCF* або *WHS*. Отримано такі результати:

- для знаходження бієктивного S-блоку з $N(S) = 104$ алгоритм генерації потребує в середньому 49 399 ітерацій (при $R = 14$ та $X = -8$), що на 23 % менш ніж кращий відомий результат (65 933 ітерацій);
- для знаходження бієктивного S-блоку з $N(S) = 102$ алгоритм генерації потребує в середньому 878 ітерацій (при $R = 16$ та $X = -8$);
- для знаходження бієктивного S-блоку з $N(S) = 100$ алгоритм генерації потребує в середньому 134 ітерації (при $R = 10$ та $X = 16$).

Список літератури:

1. Menezes A.J. et al. Handbook of Applied Cryptography. CRC Press, 2018.
2. Delfs H., Knebl H. Introduction to Cryptography. Berlin, Heidelberg: Springer Berlin Heidelberg, 2015.
3. Kuznetsov A.A. et al. Stream Ciphers in Modern Real-time IT Systems: Analysis, Design and Comparative Studies. Springer International Publishing, 2022. XVI. 611 p.
4. Daemen J., Rijmen V. Specification of Rijndael // The Design of Rijndael: The Advanced Encryption Standard (AES) / ed. Daemen J., Rijmen V. Berlin, Heidelberg: Springer, 2020. P. 31–51.
5. Daemen J., Rijmen V. AES proposal: rijndael. 1999.
6. Shannon C.E. Communication theory of secrecy systems // The Bell System Technical Journal. 1949. Vol. 28, № 4. P. 656–715.
7. Freyre Echevarría A. Evolución híbrida de s-cajas no lineales resistentes a ataques de potencia. 2020.
8. Gorbenko I. et al. Random S-Boxes Generation Methods for Symmetric Cryptography // 2019 IEEE 2nd Ukraine Conference on Electrical and Computer Engineering (UKRCON). 2019. P. 947–950.
9. Moskovchenko I. et al. HEURISTIC METHODS FOR THE DESIGN OF CRYPTOGRAPHIC BOOLEAN FUNCTIONS: 3 // International Journal of Computing. 2019. Vol. 18, № 3. P. 265–277.
10. Cusick T., Stănică P. Cryptographic Boolean Functions and Applications: Second edition // Cryptographic Boolean Functions and Applications: Second Edition. 2017. P. 2751 p.
11. Bard G.V. Algebraic Cryptanalysis. Boston, MA: Springer US, 2009.
12. Courtois N.T., Bard G.V. Algebraic Cryptanalysis of the Data Encryption Standard // Cryptography and Coding / ed. Galbraith S.D. Berlin, Heidelberg: Springer, 2007. P. 152–169.
13. Courtois N.T., Pieprzyk J. Cryptanalysis of Block Ciphers with Overdefined Systems of Equations // Advances in Cryptology — ASIACRYPT 2002 / ed. Zheng Y. Berlin, Heidelberg: Springer, 2002. P. 267–287.
14. Technology N.I. of S. and. Advanced Encryption Standard (AES): Federal Information Processing Standard (FIPS) 197. U.S. Department of Commerce, 2001.
15. Daemen J., Rijmen V. Rijndael/AES // Encyclopedia of Cryptography and Security / ed. van Tilborg H.C.A. Boston, MA: Springer US, 2005. P. 520–524.
16. Burnett L.D. Heuristic Optimization of Boolean Functions and Substitution Boxes for Cryptography: phd. Queensland University of Technology, 2005.
17. Ivanov G., Nikolov N., Nikova S. Cryptographically Strong S-Boxes Generated by Modified Immune Algorithm // Cryptography and Information Security in the Balkans / ed. Pasalic E., Knudsen L.R. Cham: Springer International Publishing, 2016. P. 31–42.
18. Freyre-Echevarría A. et al. An External Parameter Independent Novel Cost Function for Evolving Bijective Substitution-Boxes: 11 // Symmetry. Multidisciplinary Digital Publishing Institute. 2020. Vol. 12, № 11. P. 1896.
19. Freyre-Echevarría A. et al. Evolving Nonlinear S-Boxes With Improved Theoretical Resilience to Power Attacks // IEEE Access. 2020. Vol. 8. P. 202728–202737.
20. Kuznetsov A. et al. Optimizing the Local Search Algorithm for Generating S-Boxes // 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S T). 2021. P. 458–464.
21. Kuznetsov A. et al. WHS Cost Function for Generating S-boxes // 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S T). 2021. P. 434–438.
22. Ivanov G., Nikolov N., Nikova S. Reversed genetic algorithms for generation of bijective s-boxes with good cryptographic properties // Cryptogr. Commun. 2016. Vol. 8, № 2. P. 247–276.
23. Kapuściński T., Nowicki R.K., Napoli C. Application of Genetic Algorithms in the Construction of Invertible Substitution Boxes // Artificial Intelligence and Soft Computing / ed. Rutkowski L. et al. Cham: Springer International Publishing, 2016. P. 380–391.
24. Mariot L., Leporati A. Heuristic Search by Particle Swarm Optimization of Boolean Functions for Cryptographic Applications // Proceedings of the Companion Publication of the 2015 Annual Conference on Genetic and Evolutionary Computation. New York, NY, USA: Association for Computing Machinery. 2015. P. 1425–1426.
25. Freyre Echevarría A., Martínez Díaz I. A new cost function to improve nonlinearity of bijective S-boxes. 2020.
26. Clark J.A., Jacob J.L., Stepney S. The design of S-boxes by simulated annealing // New Gener Comput. 2005. Vol. 23, № 3. P. 219–231.
27. McLaughlin J. Applications of search techniques to cryptanalysis and the construction of cipher components: phd. University of York, 2012.
28. Wang J. et al. Construction Method and Performance Analysis of Chaotic S-Box Based on a Memorable Simulated Annealing Algorithm: 12 // Symmetry. Multidisciplinary Digital Publishing Institute, 2020. Vol. 12, № 12. P. 2115.
29. Picek S., Cupic M., Rotim L. A New Cost Function for Evolution of S-Boxes // Evolutionary Computation. 2016. Vol. 24, № 4. P. 695–718.
30. Carlet C. Vectorial Boolean functions for cryptography // Boolean Models and Methods in Mathematics, Computer Science, and Engineering. 2006.
31. Tesar P. A New Method for Generating High Non-linearity S-Boxes. Společnost pro radioelektronické inženýrství, 2010.

Надійшла до редколегії 11.05.2022

Відомості про авторів:

Кузнецов Олександр Олександрович – 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: kuznetsov@karazin.ua; ORCID: https://orcid.org/0000-0003-2331-6326

Полуяненко Микола Олександрович – канд. техн. наук, Харківський національний університет імені В.Н. Каразіна, доцент кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук; Україна; e-mail: nlfsr01@gmail.com; ORCID: https://orcid.org/0000-0001-9386-2547

Кандій Сергій Олегович – АТ «Інститут інформаційних технологій», технік-конструктор, Україна; e-mail: sergey.kandy@gmail.com, ORCID: https://orcid.org/0000-0003-0552-8341

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

УДК 004.056.55 **DOI:10.30837/rt.2022.2.209.08**

О.Г. КАЧКО, канд. техн. наук, М.В. ЄСІНА, канд. техн. наук, К.О. КУЗНЕЦОВА

АНАЛІЗ МЕТОДІВ ТА АЛГОРИТМІВ ГЕНЕРАЦІЇ КЛЮЧОВИХ ДАНИХ ДЛЯ FALCON ПОДІБНИХ АЛГОРИТМІВ ЕЛЕКТРОННОГО ПІДПИСУ

Вступ

Алгоритм Falcon [2] є фіналістом конкурсу постквантових алгоритмів електронного підпису [1] завдяки задовільному значенню суми довжин відкритого ключа |pk| та |sig|, але алгоритм генерації ключових даних застосовує багато методів та важкий для реалізації. Автори [2] застосовують цей алгоритм для поліномів розміром n=512, 1024. Для збільшення шостого рівня криптостійкості цей алгоритм може бути розширено для n=2048. Саме дослідженню алгоритму Falcon з урахуванням його розширення для n=512, 1024, 2048 в частині генерації ключових даних присвячена ця робота.

У роботі застосовуються позначення, що прийняті в [2].

1. Алгоритм генерації ключових даних

Параметрами алгоритму є значення n, q.

Значення n визначає степінь поліномів (n=512, 1024, 2048) та відповідне поле $\phi = x^n + 1$. Значення q визначає модуль, за яким обчислюється відкритий ключ і виконуються перетворення при обчисленні електронного підпису, q=12289 для усіх n.

Результатом роботи алгоритму генерації ключових даних є:

– Поліноми f, g – випадкові поліноми.

– Поліноми F, G, що обираються згідно рівнянню:

$$f \cdot G - g \cdot F = q \bmod \phi . \tag{1}$$

Алгоритм генерації ключових даних включає наступні кроки:

Крок 1. Генерація випадкових поліномів f, g в полі $x^p + 1$, $(p = n)$.

Крок 2. Перетворення поліномів f, g в полі $x^p + 1$, $(p = n)$ в поліноми f', g' для поля $x^p + 1$, $(p = 1)$.

Крок 3. Рішення діафантового рівняння $f' \cdot G' - g' \cdot F' = 1$ відносно F', G' для поля $x^p + 1$, $(p = 1)$.

Крок 4. Якщо рішення є, то обчислення $G' = q \cdot G$, $F' = q \cdot F$; інакше повернутися на Крок 1.

Крок 5. Перетворення F', G' для поля $x^p + 1$, $(p = 1)$ в поліноми F, G для поля $x^p + 1$, $(p = 1)$.

2. Генерація випадкових поліномів f, g, які задовільняють розподілу Гауса

Для отримання коротких поліномів обираються параметри розподілу Гауса $\sigma = 1.17 \cdot \sqrt{\frac{q}{2n}}$, $\mu = 0$.

Квадратична норма поліномів обчислюється за формулою

$$norma(f, g) = \sum_{i=0}^{n-1} \left(f_i^2 + g_i^2 \right). \tag{2}$$

Для поліномів $f' = \frac{qf^*}{ff^* + gg^*}$, $g' = \frac{qg^*}{ff^* + gg^*}$ (f^*, g^* – комплексно спряжені поліноми) квадратична норма обчислюється за формулою

$$norma(f', g') = \sum_{i=0}^{n-1} \left(f_i'^2 + g_i'^2 \right). \quad (3)$$

$norma(f, g)$ та $norma(f', g')$ не повинні перевищувати значення *max_norma*=1.172*q*:

Для поліному *f* повинна існувати інверсія f^{-1}, тобто

$$f \cdot f^{-1} = 1 \bmod (\bmod \phi,\ q). \quad (4)$$

Автори Falcon [2] для генерації поліномів з розподілом Гауса застосовують генератори випадкових чисел і накопичувальну таблицю розподілу, яку передобчислюють заздалегідь. Для згенерованих поліномів порівнюють норми, обчислені за формулами (1), (2), з максимальною нормою (3). Поліном *g* приймається, якщо норми не перевищують максимальну норму. Для поліному *f* виконується додаткова перевірка на наявність інверсії. У разі, якщо хоч одна перевірка для жодного поліному не проходить, поліноми генеруються знову. У табл. 1 наведено результати аналізу поліномів з урахуванням обох критеріїв за нормою та наявності інверсії для поліному *f*. Задано кількість відбракованих поліномів за різними критеріями, а також загальний процент відбракованих поліномів.

Таблиця 1

Результати аналізу поліномів з урахуванням обох критеріїв за нормою та наявності інверсії для поліному

Розмір поліному	*N*=512	*N*=1024	*N*=2048
int	4942	4950	4987
double	4079	4364	4671
f^1	49	51	49
Common *g* (%)	90.21	93.14	96.58
Common *f* (%)	90.7	93.64	97.07

У рядку int наведена кількість поліномів, які не пройшли перевірку, пов'язану з квадратичною нормою згідно (1).

У рядку doudle наведена кількість поліномів, які не пройшли перевірку, пов'язану з квадратичною нормою згідно (2).

У рядку f^{-1} наведена кількість ключів, які не пройшли перевірку, пов'язану з наявністю інверсії (4). Виконується тільки для поліному *f*. У рядках *Common g* (%) та *Common f* (%) наведено % пар поліномів, які не пройшли усіх перевірок.

Як видно з табл. 1, з поліномів, які генеруються за методикою авторів [2], не менше, ніж 90 % пар поліномів треба відбракувати, кількість відбракованих пар поліномів збільшується зі збільшенням *n* разом з часом генерації для цих поліномів. Подалі цей спосіб будемо називати Спосіб 1.

Пропонується інший спосіб (Спосіб 2) генерації поліномів із застосуванням формули імовірності для розподілу Гауса:

$$P(k) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{k^2}{2\sigma^2}}. \quad (4)$$

Розраховуємо ймовірність $0, \pm1, \pm2, \ldots$ і далі з урахуванням значення *n*. У результаті отримаємо поліном, який задовольняє вимогам розподілу Гауса та досягаємо непарності суми коефіцієнтів за модулем 2. За допомогою алгоритму випадкової перестановки [3] отримаємо поліноми *f*, *g*. В табл. 2 наведено норми для таких поліномів в залежності від *n*.

Таблиця 2

Норми для поліномів *f, g* в залежності від *n*

n	512	1024	2048
$\sum_{i=0}^{n-1}\left(f_i^2+g_i^2\right)$	16270	16642	16750

Значення максимальної норми згідно з (2) дорівнює 16822.4121, тобто усі поліноми, згенеровані таким чином, задовольняють цій нормі.

Результати порівняння кількості коефіцієнтів з різними значеннями для алгоритмів згідно [2] та алгоритму, розглянутому вище, наведено в табл. 3.

У табл. 3 для кожного значення *n* наведено дві колонки. Ліва колонка відповідає середній кількості значень коефіцієнтів поліному (*k*) для прийнятних ключів, розрахованих першим способом, а права – для ключів, розрахованих другим способом.

Таблиця 3

Результати порівняння кількості коефіцієнтів з різними значеннями для алгоритмів згідно [2] та алгоритму, розглянутому вище

K	*n*=512		*n*=1024		*n*=2048	
	Cnt1	Cnt2	Cnt1	Cnt2	Cnt1	Cnt2
0	51.02	52	143.37	144	404.48	404
±1	98.42	98	271.40	268	716.59	714
±2	90.21	90	224.24	224	496.50	496
±3	77.34	76	163.95	164	268.25	270
±4	62.00	62	106.80	108	113.15	114
±5	46.69	48	61.28	62	36.92	38
±6	33.18	34	30.85	32	9.81	10
±7	22.12	22	13.87	14	1.89	1
±8	13.93	14	5.64	6	0.33	1
±9	8.13	8	1.80	1	0.04	
±10	4.61	4	0.58	1		
±11	2.36	2	0.16			
±12	1.14	1	0.04			
±13	0.49	1	0.01			
±14	0.21					
±15	0.09					
±16	0.03					
±17	0.01					
	511.98	512	1023.99	1024	2047.96	2048

Загальна кількість коефіцієнтів для першого варіанту задається не цілими значеннями, тому що отримали середнє для усіх поліномів, які пройшли необхідні перевірки.

Результати порівняння показують, що для більшості значень кількість співпадає; для значень, для яких вона відрізняється, значення різниці незначне.

Визначимо простір ключів для другого способу формування коефіцієнтів поліному:

$$C=\frac{n!}{\prod_{i=0}^{18} Cnt2_i!}\cdot \tag{4}$$

Це практично не відрізняється від простору ключових даних для першого варіанту, про що свідчить практичне співпадіння даних в табл. 3.

Застосування другого варіанту замість першого дозволяє генерувати поліноми *f, g* без відбракування їх. Перший варіант передбачав відбракування не менше, ніж 90 % поліномів, а для n=2048 навіть більше, ніж 97 %.

Результати подальшого аналізу алгоритму генерації ключових даних будуть представлені у майбутніх роботах.

Список літератури:

1. Post-Quantum Cryptography. Round 3 Submissions. [Електронний ресурс]. Режим доступу: https://csrc.nist.gov/Projects/post-quantum-cryptography/round-3-submissions.

2. Falcon: Fast-Fourier Lattice-based Compact Signatures over NTRU. [Електронний ресурс]. Режим доступу: https://falcon-sign.info/.

3. Donald E. Knuth The Art of Computer Programming. Seminumerical algorithms. Vol. 2 (3rd ed.). Boston: Addison–Wesley, 1998. 774p.

Надійшла до редколегії 05.05.2022

Відомості про авторів:

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

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

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

УДК 003.026:004.056 **DOI:10.30837/rt.2022.2.209.09**

Є.Ю. КАПТЬОЛ

АНАЛІЗ СТАНУ ПОСТКВАНТОВОГО АЛГОРИТМУ ЕЛЕКТРОННОГО ПІДПИСУ RAINBOW ТА АТАК НА НЬОГО НА ПЕРІОД ЗАВЕРШЕННЯ ТРЕТЬОГО РАУНДУ NIST PQC

Вступ

Через поступове покращення існуючих та винайдення нових квантових комп'ютерів існує потреба в стандартизації постквантових електронних підписів. В межах конкурсу NIST PQC до третього раунду було відібрано три електронних підписи, що претендують на стійкість до класичного та квантового криптоаналізу та можливість їх застосування в постквантовий період. Згідно з [1, 2] до третього раунду в якості основних фіналістів увійшли такі електронні підписи: CRYSTALS-DILITHIUM, FALCON, Rainbow. Також окрім основних кандидатів було відібрано три альтернативних: Picnic, SPHINCS+, GeMSS. Так як Rainbow є одним з фіналістів, варто розглянути атаки на нього, зокрема ті, що використовують переваги квантового комп'ютера. Разом зі звичайним алгоритмом Rainbow було також представлено CZ-Rainbow та стислий алгоритм Rainbow. Також слід зазначити, що в ході доповіді в рамках NIST PQC щодо особливостей прийняття перших постквантових стандартів, що відбулася 8 – 11 березня 2022 р., було згадано про деяке занепокоєння щодо безпеки обох мультиваріативних підписів (Rainbow як основний кандидат та GeMSS як альтернативний).

1. Сутність алгоритму Rainbow

Згідно з [3], генерація та верифікація підпису за алгоритмом Rainbow мають вигляд, наведений далі.

Генерація підпису. Маємо документ d, що необхідно підписати, використовується хеш-функція $\mathrm{H}:\{0,1\}\to\mathrm{F}^m$ для обчислення хеш-значення $\mathrm{h}=\mathrm{H}(d)\in\mathrm{F}^m$. Далі підпис $\mathrm{z}\in\mathrm{F}^n$ документа d обчислюється наступними послідовними кроками: обчислюється $\mathrm{x}=\mathrm{S}^{-1}(\mathrm{h})\in\mathrm{F}^m$; обчислюється прообраз $\mathrm{y}\in\mathrm{F}^n$ від x над центральною мапою F; обчислюється підпис $\mathrm{z}\in\mathrm{F}^n$ з $\mathrm{z}=\mathrm{T}^{-1}(\mathrm{y})$.

Верифікація підпису. Маємо документ d та підпис $\mathrm{z}\in\mathrm{F}^n$, справжність підпису перевіряється наступними кроками: використовується хеш-функція H для обчислення хеш-значення $\mathrm{h}=\mathrm{H}(d)\in\mathrm{F}^m$; обчислюється $\mathrm{h}'=\mathrm{P}(\mathrm{z})\in\mathrm{F}^m$. Якщо виконується рівність $\mathrm{h}'=\mathrm{h}$, підпис z приймається, в іншому випадку він відхиляється.

2. Набори параметрів Rainbow

Спочатку потрібно розглянути параметри електронного підпису. У зв'язку з тим, що на конкурс NIST PQC було представлено три варіанти схеми електронного підпису та кожен з них має свої набори параметрів для різних категорій безпеки, їх варто розглядати окремо. Згідно з [3] було представлено такі варіанти схеми електронного підпису Rainbow: звичайний алгоритм Rainbow, CZ-Rainbow та стислий алгоритм Rainbow.

Набори параметрів для зазначених варіантів електронного підпису відповідають різним категоріям безпеки NIST. Так, кожен варіант Rainbow має три набори параметрів: I, III та V. Відповідність наборів параметрів категоріям безпеки NIST наступна [3]: набір параметрів I відповідає категоріям безпеки I та II, набір параметрів III відповідає категоріям безпеки III та IV, набір параметрів V відповідає категорії безпеки V.

Табл. 1 – 3 містять набори параметрів для звичайного алгоритму Rainbow, CZ-Rainbow та стислого алгоритму Rainbow відповідно [3] (так ми маємо параметри (F, v_1, o_1, o_2), розміри відкритого та закритого ключів, розмір гешу та розмір підпису).

Таблиця 1

Розміри ключів та підписів для звичайного алгоритму Rainbow

Набір параметрів	Параметри (F, v_1, o_1, o_2)	Відкритий ключ (кВ)	Закритий ключ (кВ)	Розмір гешу (біт)	Розмір підпису (біт)
I	(GF(16), 36, 32, 32)	157.8	101.2	256	528
III	(GF(256), 68, 32, 36)	861.4	611.3	576	1,312
V	(GF(256), 96,36, 64)	1,885.4	1,375.7	768	1,696

Таблиця 2

Розміри ключів та підписів для CZ-Rainbow

Набір параметрів	Параметри (F, v_1, o_1, o_2)	Відкритий ключ (кВ)	Закритий ключ (кВ)	Розмір гешу (біт)	Розмір підпису (біт)
I	(GF(16), 36, 32, 32)	58.8	101.2	256	528
III	(GF(256), 68, 32, 48)	258.4	611.3	576	1,312
V	(GF(256), 96,36, 64)	523.6	1,375.7	768	1,696

Таблиця 3

Розміри ключів та підписів для стислого алгоритму Rainbow

Набір параметрів	Параметри (F, v_1, o_1, o_2)	Відкритий ключ (кВ)	Закритий ключ (кВ)	Розмір гешу (біт)	Розмір підпису (біт)
I	(GF(16), 36, 32, 32)	58.8	0.06	256	528
III	(GF(256), 68, 32, 48)	258.4	0.06	576	1,312
V	(GF(256), 92,36, 64)	523.6	0.06	768	1,696

3. Атаки на Rainbow

Як зазначено в [3], всі відомі атаки на Rainbow на даний момент є, в основному, класичними атаками, деякі з котрих можуть бути прискореними за рахунок використання алгоритму Гровера. До атак на Rainbow можна віднести [3]: атаки знаходження колізій на геш-функції, прямі атаки, атаки MinRank, атаки HighRank, атаки "Rainbow-Band-Separation" (RBS), атаки UOV, атаки на диференціальне поле та квантові атаки «грубої сили».

Серед наведених атак передбачається використання квантових методів (а саме, алгоритму Гровера) в наступних атаках: прямі атаки, атаки HighRank, атаки UOV та квантові атаки «грубої сили». Розглянемо атаки, що можуть використовувати квантові методи.

Прямі атаки. Згідно з [3] найбільш прямолінійною атакою на Rainbow як на мультиваріативну схему є пряма алгебраїчна атака, що розглядає рівняння $\mathrm{P}(\mathbf{z}) = \mathbf{h}$ як приклад задачі MQ. Через те, що відкрита система Rainbow є невизначеною системою з $n \approx 1.5 \cdot m$, найефективнішим вважається отримання визначеної системи, що має рівно одне рішення, шляхом фіксації $n - m$ змінних перед застосуванням такого алгоритму, як алгоритм обчислення базисів Гробнера (F_4) [4]. Для досягнення кращих результатів використовують «гібридний підхід» (відгадують додаткові змінні перед вирішенням системи), як в [5]. В [3] складність вирішення такої системи оцінюється як

$$\mathrm{Complexity}_{\mathrm{direct;\ classical}} = \min_k \left(q^k \cdot 3 \cdot \binom{m-k+d_{\mathrm{reg}}}{d_{\mathrm{reg}}} \cdot \binom{m-k}{2} \right)$$

множень у полі, де d_{reg} – це так звана ступінь регулярності системи.

Застосування квантового комп'ютера дозволяє використати алгоритм Гровера для прискорення вгадування додаткових змінних при використанні «гібридного підходу». В [3] складність такої атаки оцінюється як

$$\mathrm{Complexity}_{\mathrm{direct;\ quantum}} = \min_k \left(q^{k/2} \cdot 3 \cdot \binom{m-k+d_{\mathrm{reg}}}{d_{\mathrm{reg}}}^2 \cdot \binom{m-k}{2} \right)$$

множень у полі.

Атаки HighRank. Згідно з [6] метою атаки HighRank є виявлення змінних, що з'являються найменшу кількість разів у центральних поліномах (вони відповідають Oil-змінним останнього рівня Rainbow).

Складність цієї атаки в [3] оцінюється як

$$\text{Complexity}_{\text{HighRank; classical}} = q^{O_u} \cdot \frac{n^3}{6}.$$

Застосування квантового комп'ютера дозволяє використати алгоритм Гровера для прискорення пошуку. У такому випадку складність атаки становить

$$\text{Complexity}_{\text{HighRank; quantum}} = q^{O_u/2} \cdot \frac{n^3}{6}$$

множень у полі.

Атаки UOV. Оскільки Rainbow можна розглядати як продовження добре відомої схеми підписів Oil and Vinegar [7], її можна атакувати, використовуючи всі відомі атаки UOV. Наприклад, атака UOV «Oil Subspace» Кіпніса та Шаміра [8].

Можна розглядати Rainbow як екземпляр UOV з $\upsilon = \upsilon_1 + o_1$ та $o = o_2$. Метою цієї атаки є пошук попереднього зображення так званого Oil підпростору O афінного перетворення T, де $\mathrm{O} = \left\{ \mathrm{x} \in \mathrm{F}^n : x_1 = \cdots = x_\upsilon = 0 \right\}$. Знаходження цього простору дозволяє відокремити Oil від змінних Vinegar та відновити закритий ключ.

Складність цієї атаки оцінюється як

$$\text{Complexity}_{\text{UOV-Attack; classical}} = q^{n-2_{o_2}-1} \cdot o_2^4$$

множень у полі.

Застосування квантового комп'ютера та алгоритма Гровера зменшує складність до

$$\text{Complexity}_{\text{UOV-Attack; classical}} = q^{\frac{n-2_{o_2}-1}{2}} \cdot o_2^4$$

множень у полі [3].

Квантові атаки «грубої сили». За наявності квантових комп'ютерів атаку грубої сили проти схеми можна різко прискорити за допомогою алгоритму Гровера.

У роботі [9] було показано, що можливо розв'язати систему $m-1$ двійкових квадратних рівнянь з $n-1$ двійкових змінних, використовуючи $m+n+2$ кубітів та обчислюючи схему з $2^{n/2} \cdot \left(2m\left(n^2+2n\right)+1\right)$ квантових логічних елементів.

Також було наведено інший варіант, який вирішує систему, використовуючи менше кубітів, але з більшою схемою, що має приблизно в два рази більше квантових логічних елементів. Наприклад, коли $n = m$, то може бути вирішена двійкова система з m рівнянь у m змінних, використовуючи $2^{m/2} \cdot 2 \cdot m^3$ бітових операцій. Загалом, завдяки алгоритму Гровера очікується квадратичне прискорення атаки грубої сили.

У табл. 4 – 6 наведено складність різних атак для наборів параметрів I, III та V відповідно [3]. У першому рядку наведено кількість необхідних для здійснення атаки класичних логічних елементів, а у другому – кількість необхідних для здійснення атаки квантових логічних елементів.

Таблиця 4

Складність атак на підпис з набором параметрів I

Набір параметрів	Параметри (F, v_1, o_1, o_2)	$\log_2$ (#гейтів)		
		прямі	HighRank	UOV
I	(GF(16), 36, 32, 32)	164	150	157
		122	86	91

Таблиця 5

Складність атак на підпис з набором параметрів III

Набір параметрів	Параметри (F, v_1, o_1, o_2)	$\log_2$ (#гейтів)		
		прямі	HighRank	UOV
III	(GF(256), 68, 32, 48)	234	410	437
		200	218	233

Таблиця 6

Складність атак на підпис з набором параметрів V

Набір параметрів	Параметри (F, v_1, o_1, o_2)	$\log_2$ (#гейтів)		
		прямі	HighRank	UOV
V	(GF(256), 96, 36, 64)	285	539	567
		243	283	299

4. Сумніви в безпеці мультиваріативних схем

В ході доповіді в рамках NIST PQC щодо особливостей прийняття перших постквантових стандартів було згадано про занепокоєння щодо безпеки обох мультиваріативних підписів (Rainbow як основний кандидат та GeMSS як альтернативний). Зокрема було зроблено посилання на атаку, котра повертає ключ для набору I параметрів Rainbow в середньому за 53 години обчислень «на стандартному ноутбуці». Разом із цим було зазначено, що це слугує нагадуванням того, що не потрібно поспішати додавати схеми-кандидати до застосунків-продуктів до завершення процесу прийняття стандартів.

Зокрема під «стандартним ноутбуком» в [11] малася на увазі машина з 8-ядровим CPU n Intel i9-10885H з тактовою частотою 2,5 GHz. Також було згадано, що вирішення системи (котре потрібно повторити приблизно 15 разів) потребує 1.1 GB пам'яті.

Також слід зазначити, що такі параметри часу атака досягає з варіантом параметрів з другого раунду NIST PQC, тоді як параметри третього раунду потребують більших ресурсів (згідно до розрахунків авторів атаки на факторіал 2^8).

В [11] було наведено дві атаки на підпис (одна є модифікацією іншої), які вказують на недостатність визначених наборів параметрів: проста атака та, як її більш ефективна версія, комбінована з прямокутною атакою MinRank.

Як наведено в табл. 7, проста атака виграє в інших атак не у всіх випадках, в той час як комбінована показує кращі результати для всіх наборів параметрів. Варто зауважити, що для набору параметрів I проводиться атака відновлення ключа, в той час як для інших – атаки підробки.

Таблиця 7

Порівняння складності запропонованих в [11] атак з аналогічними відомими атаками на Rainbow

Набір параметрів	Проста атака ($\log_2$ (#гейтів))	Комбінована атака ($\log_2$ (#гейтів))	Інші відомі атаки ($\log_2$ (#гейтів))
I	69	99	127
III	160	157	177
V	257	206	226

Згідно з [11] проста атака спрямована на те, щоб зменшити рівень безпеки Rainbow до рівня меншого UOV, з $m' = m - o_2$ та $n' = n - o_2$ змінних. Це стає можливим завдяки усуненню другого шару Rainbow шляхом знаходження вектора в O_2 (при $o_2 \in O_2$ та $O_2 \subset \mathrm{F}_q^n$), що можливо ціною

$$3\binom{n-m-1+D}{D}^2\binom{n-m+1}{2}$$

множень в полі за умови непарного q та ціною

$$3\binom{n-m-2+D}{D}^2\binom{n-m}{2}$$

множень в полі за умови парного q.

Комбінована з прямокутною атакою MinRank атака в свою чергу застосовує просту атаку для того, щоб зменшити кількість матриць для вирішення задачі MinRank від звичайних для оригінальної прямокутної атаки MinRank $n-o_2+1$ до $n-m$ матриць. Хоча також слід зауважити, що це призводить до необхідності повтору атаки в середньому q разів (поки $\ker(D_x)\cap O_2 \neq \{0\}$, де $D_x : \mathrm{F}_q^n \to \mathrm{F}_q^m : y \mapsto \mathrm{P}'(x,y)$).

З варіантів уникнення можливості цих атак можна виділити збільшення параметрів, що призведе до збільшення розмірів ключа та підпису. Якщо брати до уваги [10] та інші джерела щодо NIST PQC, можна помітити, що розміри ключа Rainbow і так вважаються великими (хоча й альтернатива у вигляді GeMSS не сильно відрізняється за цим параметром).

Висновки

Конкурс NIST PQC підходить до моменту демонстрації результатів шляхом формування проектів стандартів для постквантового періоду. З врахуванням цього та трьох раундів цікавим є те, що з мультиваріативних електронних підписів залишилися лише Rainbow в якості основного кандидату та GeMSS – в якості альтернативного. Логічним було б припустити, що в них найменша вразливість до криптоаналізу з усіх поданих мультиваріативних, але це не означає, що в них немає проблем та не може бути виявлено нових можливостей для проведення криптоаналізу.

З попередньо відомих атак можна було зробити висновок, що Rainbow певною мірою готовий до постквантового періоду. Особливо цікавим було те, що атаки були класичними та могли використовувати квантовий комп'ютер для пришвидшення певних кроків (окрім цілком квантової атаки «грубої сили»).

Проте також слід зауважити, що пришвидшення атак за допомогою квантового комп'ютера є нерівномірним. Через це для різних наборів параметрів оптимальними є різні атаки. Так, наприклад для набору параметрів I найкращою атакою з використанням квантового комп'ютера була атака HighRank, а для наборів параметрів III та V – пряма атака.

Також важливим моментом є те, що повністю квантовою атакою з наведених є лише квантова атака «грубої сили». Інші атаки використовують квантовий комп'ютер лише для виконання певного кроку атаки.

Ситуація змінилася з появою атаки, що здатна здійснити криптоаналіз електронного підпису Rainbow «за допомогою ноутбука на вихідних» для одного з наборів параметрів. Про це навіть було згадано в ході доповіді в рамках NIST PQC щодо особливостей прийняття перших постквантових стандартів, що відбулася 8 – 11 березня 2022 р.

Але згадано про це було доволі коротко та у поєднанні з нагадуванням про те, що не варто вбудовувати схеми-кандидати до продуктів заздалегідь до завершення розробки стандартів.

Також не було згадано про те, що такі оцінки криптоаналізу Rainbow (53 години обчислень на машині з 8-ядровим CPU n Intel i9-10885H з тактовою частотою 2.5 GHz) дійсні лише для набору параметрів I з тих наборів параметрів, що було надано на другий раунд NIST PQC. Для набору параметрів, поданого для третього раунду, ситуація виглядає дещо кращою (приблизно на 2^8, за словами авторів атаки). Цієї атаки можна уникнути збільшенням параметрів Rainbow. Хоча просто збільшення параметрів призведе до збільшення ключа та підписа, що не є цілком вірним виходом через те, що розмір ключа і так вважаєтьтся великим та подальше його збільшення робить застосування Rainbow менш вигідним.

Список літератури:

1. Post-Quantum Cryptography PQC. Round 3 Submissions. NIST Computer Security Resource Center (CSRC). URL: https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions (last accessed on 16.06.2022).
2. PQC Standardization Process: Third Round Candidate Announcement. NIST Computer Security Resource Center (CSRC). July 22, 2020. URL: https://csrc.nist.gov/News/2020/pqc-third-round-candidate-announcement (last accessed on 15.06.2022).
3. Jintai Ding. Rainbow – Algorithm Specification and Documentation. The 3d round Proposal. Department of Mathematical Sciences, University of Cincinnati.
4. J.-C. Faugere. A new efficient algorithm for computing Grobner Bases (F4). Journal of Pure and Applied Algebra, 139 (1999) 61-88. DOI: https://doi.org/10.1016/S0022-4049(99)00005-5 (last accessed on 13.06.2022).
5. L. Bettale, J.-C. Faugere, L. Perret. Hybrid approach for solving multivariate systems over finite fields. Journal of Mathematical Cryptology, 3, pp. 177-197, 2009.
6. D. Coppersmith, J. Stern, S. Vaudenay. Attacks on the birational signature scheme. CRYPTO 1994, pp. 435-443. Springer, 1994.
7. A. Kipnis, J. Patarin, L. Goubin. Unbalanced Oil and Vinegar schemes. EUROCRYPT 1999, pp. 206-222. Springer, 1999.
8. A. Kipnis, A. Shamir. Cryptanalysis of the Oil and Vinegar signature scheme. CRYPTO 1998, pp. 257-266. Springer,1998.
9. P. Schwable, B. Westerbaan. Solving Binary MQ with Grover's Algorithm. SPACE 2016, pp. 303-322. Springer 2016.
10. Post-Quantum Cryptography PQC. The Beginning of the End: The First NIST PQC Standards. NIST Computer Security Resource Center (CSRC). URL: https://csrc.nist.gov/Presentations/2022/the-beginning-of-the-end-the-first-nist-pqc-standa (last accessed on 13.06.2022).
11. W. Beullens. Breaking Rainbow Takes a weekend on a Laptop. Cryptology ePrint Archive 2022/214. URL: https://eprint.iacr.org/2022/214 (last accessed on 17.06.2022).

Надійшла до редколегії 11.05.2022

Відомості про автора:

Каптьол Євгеній Юрійович – аспірант кафедри безпеки інформаційних систем і технологій; Харківський національний університет імені В. Н. Каразіна, , Україна; email: kaptevg@gmail.com

УДК 004.056.5 **DOI:10.30837/rt.2022.2.209.10**

О.О. КУЗНЕЦОВ, д-р техн. наук, М.О ПОЛУЯНЕНКО, д-р техн. наук,
С.О. КАНДІЙ, Є.О. ЛОГАЧОВА

ОБҐРУНТУВАННЯ ПАРАМЕТРІВ АЛГОРИТМУ ІМІТАЦІЇ ВІДПАЛУ ДЛЯ ПОШУКУ НЕЛІНІЙНИХ ПІДСТАНОВОК СИМЕТРИЧНИХ ШИФРІВ

Вступ

Нелінійні підстановки (S-boxes) відігріють вирішальну роль у забезпеченні певних криптографічних властивостей сучасних шифрів із секретним ключем [1 – 3]. Зокрема, вони забезпечують confusion та вносять нелінійність у зв'язок вхід-вихід шифру. Отже генерація S-boxes із потрібними криптографічними властивостями є важливим завданням.

В цій роботі розглядаємо генерацію випадкових 8-бітних бієктивних підстановок, які зазвичай застосовуються в сучасних алгоритмах шифрування із симетричним ключем [4 – 6]. Досліджуємо алгоритм імітації відпалу (SA) та оптимізуємо його параметри за критерієм мінімізації обчислювальних ресурсів на генерацію цільового S-box. Зокрема досліджуємо вплив початкової температури та «коефіцієнта охолодження» на ефективність пошуку. Далі показуємо, що при обранні рекомендованих параметрів ймовірність знайти цільовий S-блок дорівнює 56,4 % а середній час пошуку складає 14,2 с. Це кращий відомий результат при застосуванні алгоритму імітації відпалу.

Пов’язані роботи

Методи імітації відпалу досліджуються в різних практичних застосуваннях математичної оптимізації [7]. В роботі [8] було запропоновано реалізацію цього алгоритму для пошуку нелінійних підстановок. Також в цій роботі запропоновано функцію вартості based on Walsh-Hadamard Spectra (WHS). Згодом ця функція вартості досліджувалася в різних роботах, наприклад у [9 – 12] та багатьох інших. Слід відмітити, що у [8] авторам не вдалося сформувати S-блок із нелінійністю >102 через високу обчислювальну складність пошуку. Кращий результат, якого вони досягли, це підстановки із нелінійністю 102. В роботі [9] проведено дослідження налаштувань функції вартості WHS та сформовано S-блок із нелінійністю 104. Але для цього було застосовано інший алгоритм пошуку (використовувався новий алгоритм «Genetic and Tree»). Складність пошуку також виявилася занадто високою (понад 3 мільйони ітерацій). Подальші дослідження були спрямовані на як на розробку нових функцій вартості [10, 12, 13], так і на застосування нових алгоритмів пошуку [3, 14 – 16]. Зокрема в роботах [17 – 20] досліджені різні варіанти алгоритму імітації відпалу. Однак в цих та інших роботах застосування імітації відпалу для генерації S-блоків виявилося надзвичайно складним. Наприклад, в [19] повідомлялося про генерацію бієктивних 8-бітних S-блоків із нелінійностю 104, але для цього виконувалися експерименти із понад 30,000,000 ітераціями. В роботі [18] також проведено чисельні експерименти, але авторам не вдалося сформувати підстановку із нелінійністю вище 100. В одній з останніх робіт [20] авторами досліджено нові методи на основі імітації відпалу. Але згенерований ними S-блок (наведений в статті) має нелінійність лише 92. Отже обчислювальна складність відомих застосувань методу імітації відпалу до задачі генерації нелінійних підстановок є дуже високою. В статті пропонуємо власну реалізацію алгоритму імітації відпалу та показуємо, що генерація бієктивних 8-бітних S-блоків із нелінійностю 104 виконується значно швидше.

Методи

Алгоритм імітації відпалу відносять до класу ітеративних алгоритмів математичної оптимізації та до більш широкого класу евристичних методів рішення комбінаторних задач. Такі алгоритми використовують існуючу сукупність рішень (популяцію) для внесення деякі-

лькох поступових змін і створення (оновлення) нової популяції. Більш детально ці методи описані у [7].

Перше застосування алгоритму імітації відпалу до задачі генерації S-блоків наведено у [8]. В роботах [19, 21] наведено сучасну версію алгоритму (див. рис. 1), яку адаптовано до задачі пошуку нелінійних S-блоків. В цій роботі застосовуємо цей алгоритм з невеликими змінами. У базовому алгоритмі як критерій прийняття нового рішення S_n застосовується покращення функції вартості $C(S_n)$:

$$C(S_n) < C(bestsol). \quad (1)$$

Ми приймаємо всі нові рішення, для яких функція вартості не погіршується:

$$C(S_n) \le C(bestsol). \quad (2)$$

Застосування критерію (2) замість (1) суттєво збільшує коло можливих рішень. Крім того, нами було виконано адаптацію роботи SA алгоритму у багатопоточному режимі пошуку.

$S \leftarrow S_0$
$bestsol \leftarrow S_0$
$T \leftarrow T_0$
$ZERO_ACCEPT_LOOPS \leftarrow 0$
for $x \leftarrow 0, MAX_OUTER_LOOPS - 1$ **do**
  $ACCEPTS_IN_THIS_LOOP \leftarrow false$
  for $y \leftarrow 0, MAX_INNER_LOOPS - 1$ **do**
    Choose some S_n in the 1-move neighbourhood of S.
    $cost_diff \leftarrow C(S_n) - C(S)$
    if $cost_diff < 0$ **then**
      $S \leftarrow S_n$
      $ACCEPTS_IN_THIS_LOOP \leftarrow true$
      if $C(S_n) < C(bestsol)$ **then**
        $bestsol \leftarrow S_n$
      end if
    else
      $u \leftarrow Rnd(0, 1)$
      if $u < exp(-cost_diff/T)$ **then**
        $S \leftarrow S_n$
        $ACCEPTS_IN_THIS_LOOP \leftarrow true$
      end if
    end if
  end for
  if $ACCEPTS_IN_THIS_LOOP = false$ **then**
    $ZERO_ACCEPT_LOOPS \leftarrow ZERO_ACCEPT_LOOPS + 1$
    if $ZERO_ACCEPT_LOOPS = MAX_FROZEN_OUTER_LOOPS$ **then**
      ▷ Algorithm terminates early.
      return $bestsol$
    end if
  end if
  $T \leftarrow T \times \alpha$
end for
return $bestsol$

Рис. 1. Псевдокод алгоритму імітації відпалу з [19, 21]

В роботі розглядаємо лише випадок генерації 8-бітної бієктивної підстановки S_n. В якості функції вартості підстановки S_n використовуємо функцію з [13, 16]:

$$\max WHS = \sum_{i=1}^{255} \left| \max\left(WHT\right) - X \right|^R, \tag{3}$$

де WHT – спектральні коефіцієнти Уолша–Адамара (англ. Walsh–Hadamard transform);

- X та R – деякі параметрів цільової функції WHS.
- В якості оптимальних параметрів функції (3) обрано [13, 16]:
- $X = 36$ як максимально допустиме значення, яке зменшує $\max WHS$, але не приводить до суттєвого впливу на її адекватне взаємозв'язок з нелінійністю S-блоку;
- $R = 4$ як максимально допустиме значення, яке збільшує діапазон значень функції $\max WHS$, що може покращити «чутливість» алгоритмів формування S-блоків.

Зазначимо, що під час обчислення функції вартості $\max WHS$ одночасно розраховувалася нелінійність S-блоку:

$$N_f = \frac{1}{2} \cdot \left(2^n - \max\left(WHT\right)\right) = 128 - \frac{1}{2} \cdot \max\left(WHT\right). \tag{4}$$

Для зниження температури з плином часу застосовувався коефіцієнт охолодження α.

Пошук починається з деякого випадково згенерованого S-блоку S_0. Процес пошуку розбивається на два цикли: зовнішній та внутрішній.

Зовнішній цикл виконується до того моменту, коли один із згенерованих S-блоків S_n буде відповідати заданим параметрам або виконується інший критерій зупинки.

У внутрішньому циклі на кожній ітерації генерується деяке поточне рішення шляхом випадкової перестановки двох значень S-блоку. Далі розраховується функція вартості для поточного рішення та порівнюється з вже найденим кращим рішенням. Якщо значення не гірше попереднього кращого S-блоку, то попереднє краще рішення замінюється поточним. Якщо значення є гіршим, тоді в залежності від температури з деякою ймовірністю приймається гірше рішення.

Умови тестування

При реалізації алгоритму імітації відпалу для генерації S-блоків ми застосовували наступні вихідні параметри:

- COST_FUNCTIONS – функція вартості, яка застосовується в алгоритмі пошуку. В цій статті застосовували COST_FUNCTIONS = $\max WHS$;
- THREADS_COUN – кількість потоків, у яких проходить одночасний пошук. В нашому випадку THREADS_COUN =30, що відповідало максимальної кількості потоків, який підтримував процесор комп'ютера;
- T_0 – початкове значення "температури". У [21] зазначено, що T_0 повинна забезпечувати початкову ймовірність прийняття гіршого рішення на рівні 50 – 80 %. В роботі досліджуємо ефективність пошуку при різних значеннях T_0;
- α – «коефіцієнт охолодження», який визначає, наскільки температура знижується на кожній ітерації алгоритму. В роботі досліджуємо ефективність пошуку при різних значеннях α;
- MAX_INNER_LOOPS, що визначає кількість внутрішніх циклів, які може здійснити локальний алгоритм пошуку при кожній температурі. В статті застосовували MAX_INNER_LOOPS=650 (тобто, загальна кількість внутрішніх тестувань становила $30 \cdot 650 = 19\ 500$);
- Критерії зупинки. В якості критеріїв зупинки використовувались наступні:

- N_f – цільове значення нелінійності (3) S-блоку. В наших експериментах обмежилися значенням $N_f = 104$, тобто пошук припиняється коли знайдено S_n із нелінійністю 104;
- MAX_OUTER_LOOPS – максимальна кількість зовнішніх циклів, тобто скільки разів SA алгоритму дозволялося знижувати температуру та продовжувати пошук до того, як він зупиниться. В дослідженнях застосовували MAX_OUTER_LOOPS =50;
- MAX_FROZEN_OUTER_LOOPS – кількість поспіль виконаних зовнішніх циклів при яких не знайдено жодного покращення функції вартості. В роботі ми застосовували MAX_FROZEN_OUTER_LOOPS = 5.

Окремі параметри алгоритму (MAX_INNER_LOOPS, MAX_OUTER_LOOPS, MAX_FROZEN_OUTER_LOOPS) обирались з міркувань, наведених у [16].

Початкова температура змінювалась від значення, де ймовірність прийняття гіршого рішення майже дорівнювала нулю до більш високої, де ймовірність становила близькою до одиниці.

Збільшення T_0 проводилось за правилом

$$T_0^{i+1} = 1{,}13 \cdot T_0^i . \tag{5}$$

Для кожного T_0^i з (5) проведено 100 запусків алгоритму імітації відпалу.

Параметр α змінювався від 0,6 до 0,95:

- для $\alpha = 0{,}6$ було проведено 10 100 запусків алгоритму пошуку;
- для $\alpha = 0{,}7$ було проведено 7 600 запусків;
- для $\alpha = 0{,}8$ було проведено 5 700 запусків;
- для $\alpha = 0{,}9$ було проведено 8 200 запусків;
- для $\alpha = 0{,}95$ було проведено 8 200 запусків.

Обмеження max_frozen_outer_loops=5 призводило до втрачання частки рішень, щодо яких алгоритм ще міг знайти цільовий S-блок. Але доцільність подальшого пошуку вважалась за малу у порівнянні з затраченим часом.

Отримані результати

Під час тестування проводилась оцінка кількості запусків SA алгоритму за максимальним значенням кортежу, протягом якого були відсутні покращення функції вартості у зовнішньому циклі, але потім було знайдено краще рішення стану S-блоку. Нагадаємо, якщо зазначений кортеж перевищував значення max_frozen_outer_loops, то алгоритм пошуку припинявся.

Результати щодо відносної кількісті запусків алгоритмів пошуку в залежності від довжини максимальних кортежів для $\alpha = 0{,}6$; 0,7; 0,8 0,9 та 0,95, а також разом з абсолютними значеннями наведено у табл. 1. Для порівняння наведено аналогічні значення, які було отримано алгоритмом локального пошуку (рядок позначено при α символом « – ») [16].

Як бачимо, тенденція розподілу кортежів для алгоритму імітації відпалу для перших значень α зберігається так само як і для алгоритму локального пошуку. З ростом параметру α зростає кількість кортежів більшого розміру. Дане зростання пояснюється зростанням кількості прийнятих погіршень, що підвищує ймовірність виходу системи зі стану локального мінімуму.

Таблиця 1

Розподіл кількості запусків алгоритмів пошуку від максимальної кількості поспіль зовнішніх циклів (кортежу), при яких не знайдено жодного покращення, однак потім покращення мали місце

α	Максимальна довжина кортежу											
	0		1		2		3		4		5	
–	720	48%	534	36%	148	10%	57	4%	24	2%	4	0,3%
0,6	4 281	42%	3 042	30%	1 509	15%	725	7%	402	4%	141	1,4%
0,7	2 722	36%	2 510	33%	1 245	16%	641	8%	355	5%	127	1,7%
0,8	1 362	24%	2 060	36%	1 244	22%	592	10%	322	6%	120	2,1%
0,9	2 168	26%	1 671	20%	1 634	20%	1 466	18%	955	12%	306	3,7%
0,95	2 299	28%	1 684	21%	1 333	16%	1 163	14%	1 167	14%	554	6,8%

Основним з показників ефективності алгоритму пошуку можна вважати ймовірність формування цільового S-блоку. Відповідні результати тестування наведені на рис. 2 та 3 (відповідно для $\alpha = 0{,}6$ та 0,9). Ймовірність обчислювалась як відношення кількості знайдених цільових S-блоків до загальної кількості запусків алгоритму пошуку. Також вимірювали середній час формування S-блоку. Отримані результати наведено на рис. 4 та 5 (відповідно для $\alpha = 0{,}6$ та 0,9). Середній час обчислювався як інтервал часу між початком пошуку та знаходженням цільового S-блоку включаючи час затрачений на невдалі запуски алгоритму пошуку.

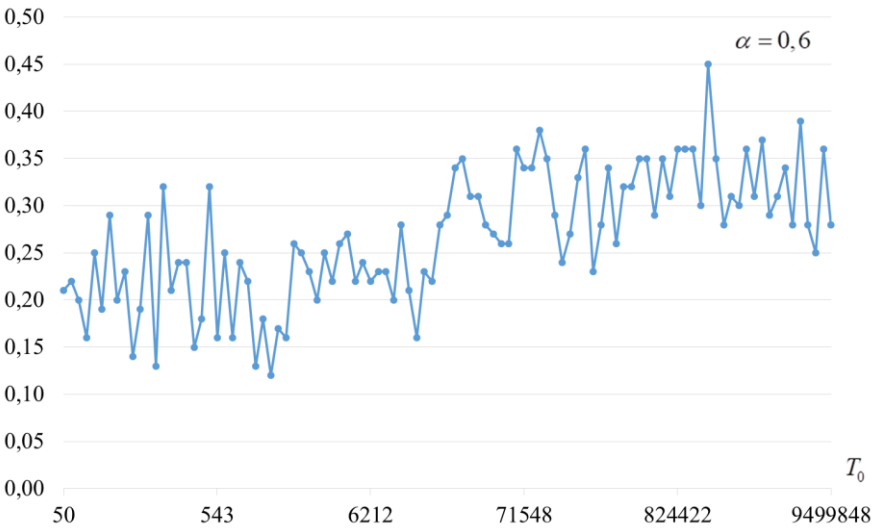


Рис. 2. Ймовірність формування цільового S-блоку при $\alpha = 0{,}6$

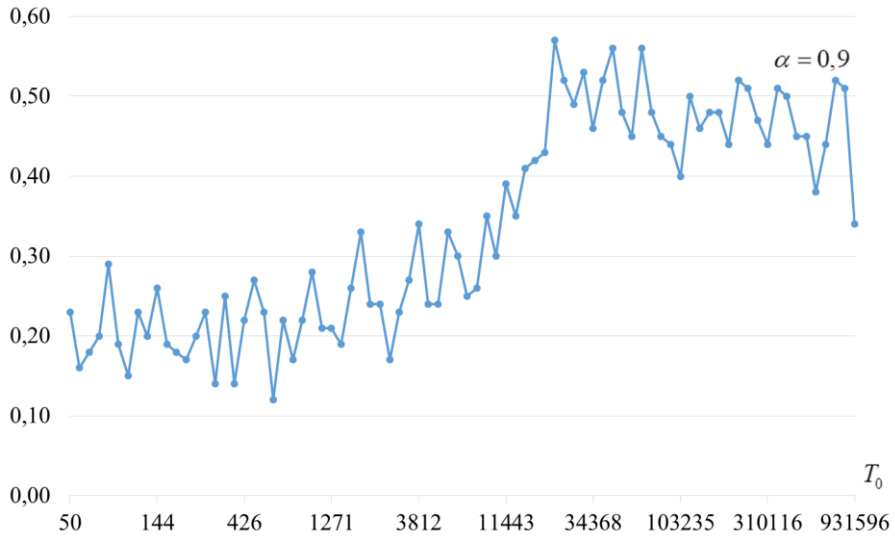


Рис. 3. Ймовірність формування цільового S-блоку при $\alpha = 0,9$

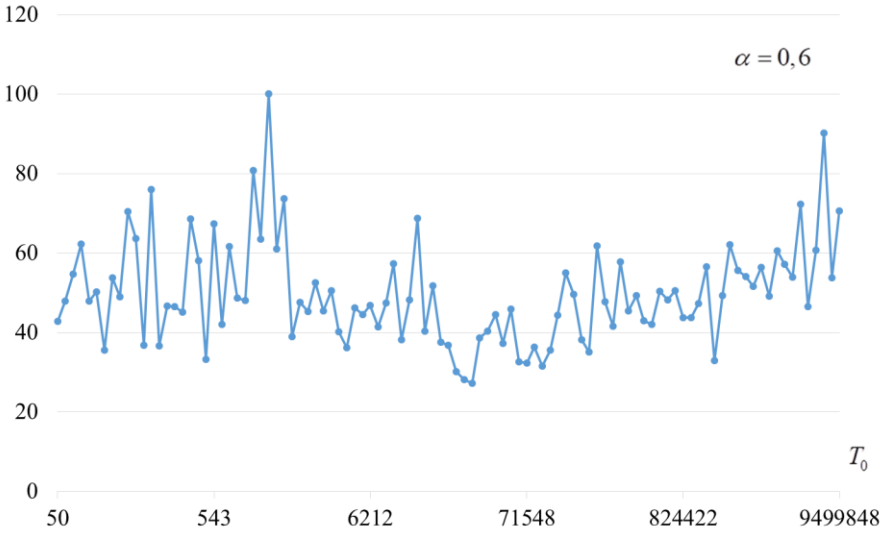


Рис. 4. Середній час (с) формування цільового S-блоку при $\alpha = 0,6$

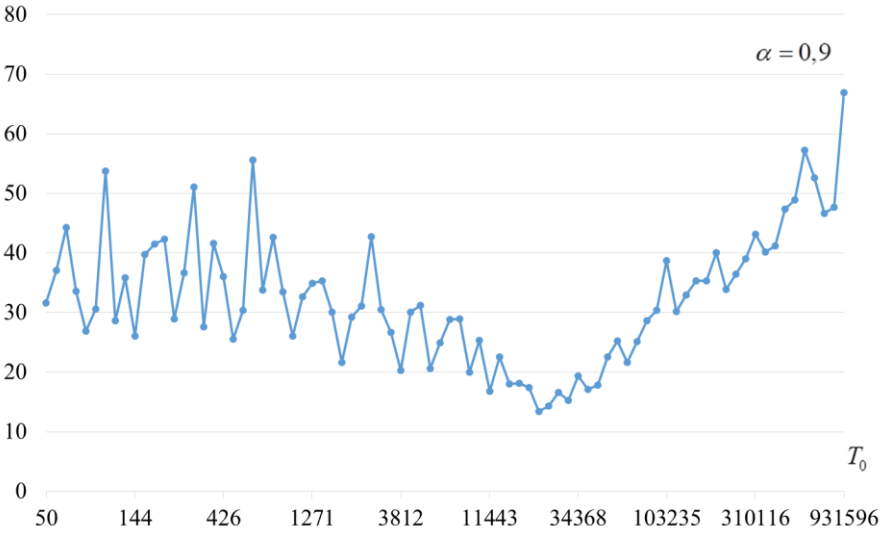


Рис. 5. Середній час (с) формування цільового S-блоку при $\alpha = 0,9$

При аналізу середнього часу необхідно обумовити, що обчислювання проходили на двох різних комп'ютерах, тому більш коректно аналізувати загальний характер поведінки зміни часу, ніж абсолютні значення.

Умовно, графіки ймовірності формування цільового S-блоку можливо поділити на три частини: ліва, середня та права.

- Ліва частина (від $T_0 = 50$ до 6 000), відповідає частині графіку, де значення ймовірності майже не змінюється або спостерігається невелике зростання.
- Середня частина ($T_0 = 6\,000 \ldots 50\,000$), де спостерігається значний ріст ймовірності формування цільового S-блоку зі зростанням значення T_0. Зі збільшенням параметру α ріст відбувається більш швидко.
- Права частина (від $T_0 = 50\,000$ та вище), де, як і у лівій частини, ймовірність фіксується у деякого значення (зі збільшенням α це значення також збільшується), після чого майже не змінюється.

Аналогічним чином можливо умовно розділити графік середнього часу формування цільового S-блоку на дві частини.

- Ліва частина відповідає значенням T_0 від мінімальних до 20 000 – 40 000. Вона відповідає поступовому зниженню середнього часу пошуку цільового S-блоку. Значення $T_0 = 20\,000$ – 40 000 відповідає досягненням області мінімальних значень часу пошуку.
- Права частина – від $T_0 = 20\,000$ –. 40 000 та вище, характеризується зростанням середнього часу пошуку цільового S-блоку, при збільшені значення α швидкість зростання також збільшується.

Значною мірою на час пошуку впливає кількість виконаних ітерації зовнішнього циклу.

На рис. 6 та 7 (відповідно для $\alpha = 0{,}6$ та 0,9) наведена кількість ітерацій зовнішнього циклу до виконання умов зупинки з усієї множини запусків алгоритму для фіксованого значення T_0. Верхня крива відповідає максимальному значенню, нижня крива – мінімальному значенню, середня – середній арифметичній кількості ітерацій зовнішнього циклу з усіх запусків при фіксованому T_0.

На рис. 8 та 9 (відповідно для $\alpha = 0{,}6$ та 0,9) аналогічні показники, але лише з тих запусків, у яких було знайдено цільовий S-блок.

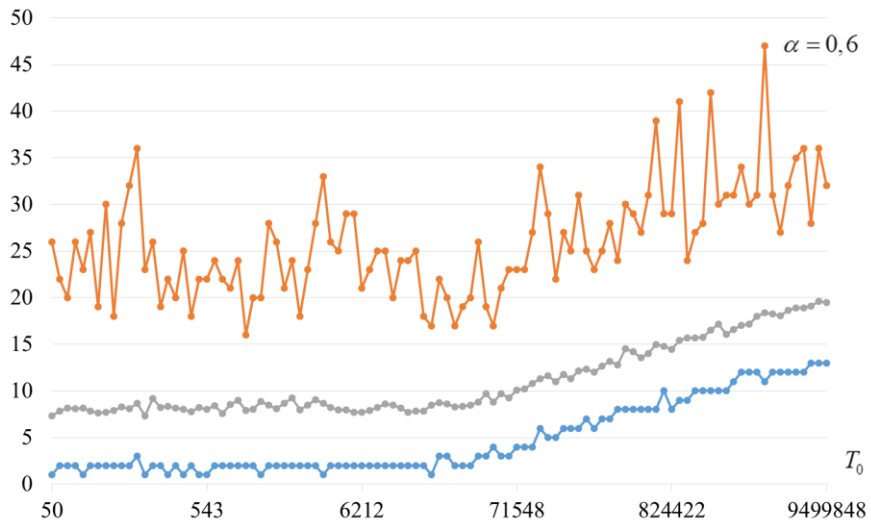


Рис. 6. Максимальна (верхня крива), середньоарифметична (посередині), мінімальна (нижня крива) кількості ітерацій зовнішнього циклу до виконання умов зупинки при $\alpha = 0{,}6$

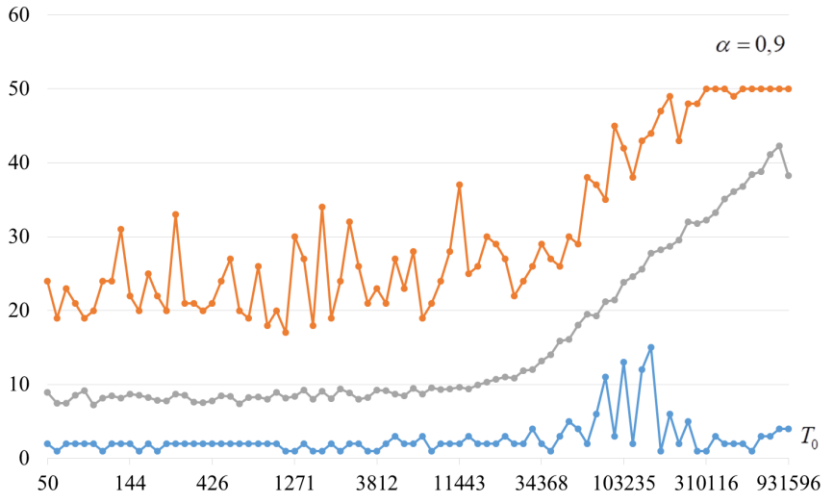


Рис. 7. Максимальна (верхня крива), середньоарифметична (посередині), мінімальна (нижня крива) кількості ітерацій зовнішнього циклу до виконання умов зупинки при $\alpha = 0,9$

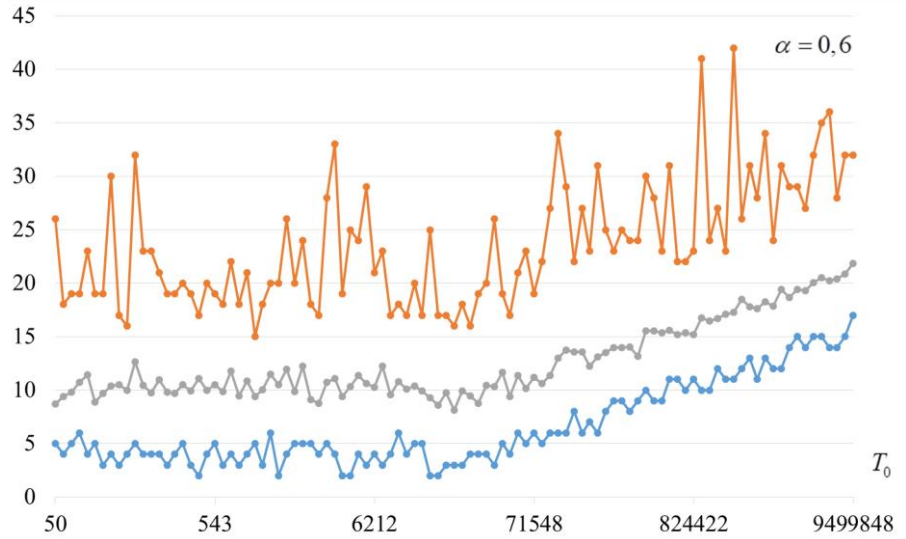


Рис. 8. Максимальна (верхня крива), середньоарифметична (посередині), мінімальна (нижня крива) кількості ітерацій зовнішнього циклу, за умови знайденого цільового S-блоку, до виконання умов зупинки при $\alpha = 0,6$

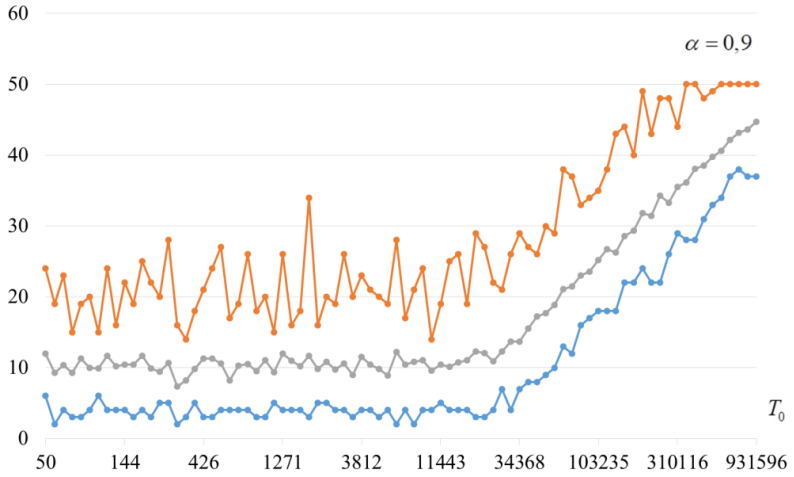


Рис. 9. Максимальна (верхня крива), середньоарифметична (посередині), мінімальна (нижня крива) кількості ітерацій зовнішнього циклу, за умови знайденого цільового S-блоку, до виконання умов зупинки при $\alpha = 0,9$

Поведінка кривих на наведених графіках відповідає умовним частинам графіків середнього часу формування цільового S-блоку. Ліва частина характеризується майже повною відсутністю зростання кількості ітерацій зовнішнього циклу до виконання умов зупинки. Після відмітки у $T_0 = 20\,000 - 40\,000$ спостерігається зростання у лінійному виді, з коефіцієнтом нахилу пропорційному параметру α.

Більш докладно дослідити процеси, які відбуваються у системі під час виконання пошуку, можна за допомогою дослідження окремих подій. Будемо досліджувати такі події як зміни нелінійності N_f та кількості прийнятих окремих рішень при кожному значенні T_0 та у кінці кожної ітерації зовнішнього циклу.

Прогрес зміни значення N_f будемо оцінювати як середньоарифметичне значення N_f всіх поточних рішень які тестуються при пошуку. Приклад прогресу зміни значення N_f наведено на тривимірних графіках рис. 10.

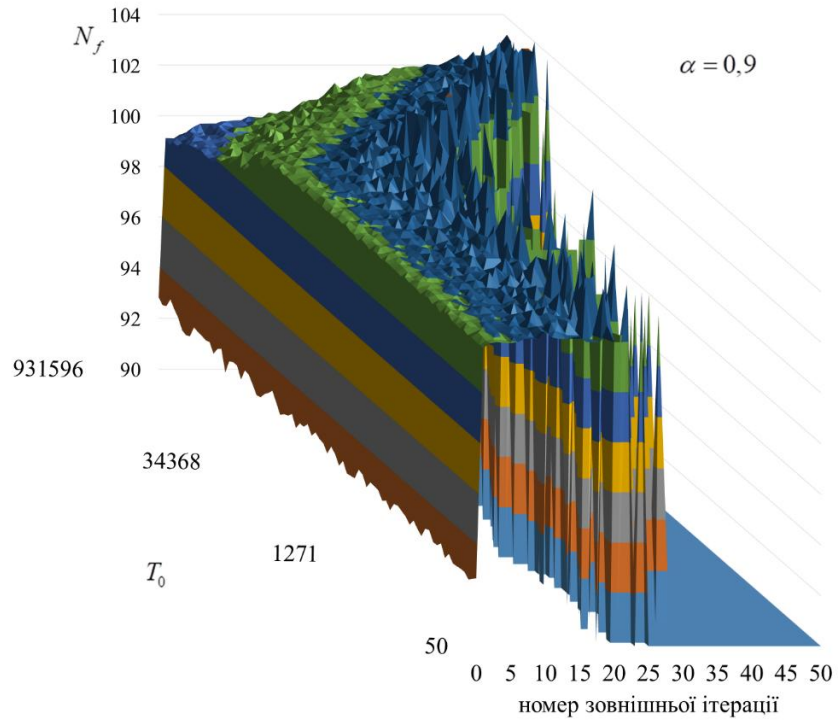


Рис. 10. Середньоарифметичне значення N_f у ітераціях при $\alpha = 0,9$

Середньоарифметичне значення N_f на початку роботи алгоритму відповідає випадково сформованим S-блокам (на графіку їх приведено під нульовою ітерацією зовнішнього циклу). Зі збільшенням номеру ітерації зовнішнього циклу збільшується й середньоарифметичне значення N_f. Однак темп збільшення відбувається по-різному в різних частинах графіку. Додержуючись раніше введеного умовного поділу графіку на ліву (при T_0 від мінімальних значень до 20 000 – 40 000) та праву (при T_0 від 20 000 – 40 000 та максимальних значень) частини, можна охарактеризувати темп збільшення середньоарифметичного значення N_f. У лівій частині після першої ітерації зовнішнього циклу середньоарифметичне значення N_f складає близько 101,8 та у продовж ще 15 – 25 циклів досягає значення 104 (або досягає інших критеріїв зупинки). У правій частині графіку зростання спостерігається значно повільніше. Наприклад, при $\alpha = 0,9$ і $T_0 = 931\,596$ після першої ітерації зовнішнього циклу

середньоарифметичне значення N_f дорівнює 99,1 та лінійно підвищується до 101,8 лише на 34 ітерації (що відповідає температурі $T = 931\,596 \cdot 0{,}9^{34} \approx 25\,910$).

Зі збільшенням номеру ітерації зовнішнього циклу зменшується загальна кількість S-блоків, що перевіряється (S-блоки, які досягли критеріїв зупинки алгоритму, далі в пошуку участь не беруть), тому зі зменшенням загальної кількості S-блоків підвищується девіація значень.

Приклад для випадку $\alpha = 0{,}9$ зміни загальної кількості ітерації, яка складається з кількості ітерації у внутрішньому циклі та кількість виконаних ітерації зовнішнього циклу, наведена на рис. 11.

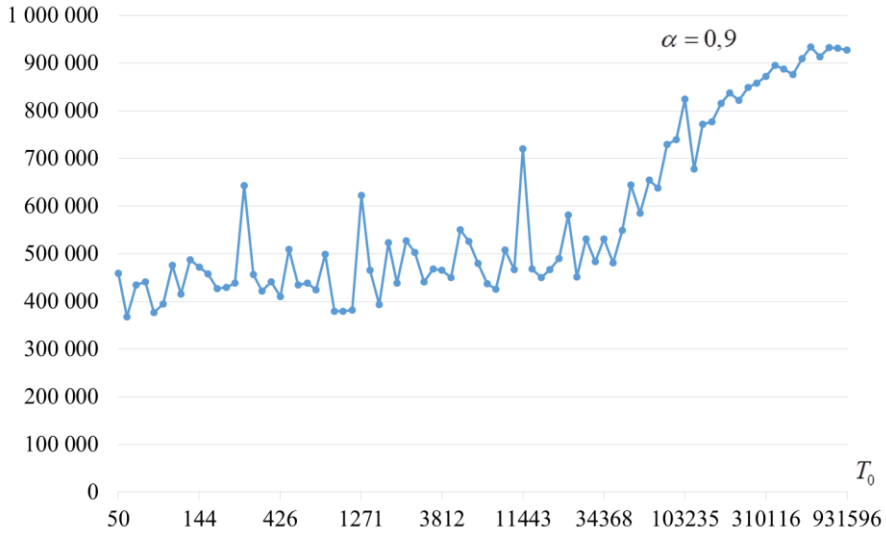


Рис. 11. Сумарне число середньоарифметичної кількості ітерації при пошуку цільового S-блоку при $\alpha = 0{,}9$

З ростом значення T_0 загальна кількість ітерації майже не змінюється до деякого значення ($T_0 = 30\,000 \ldots 70\,000$, в залежності від α) та потім починає швидко зростати, що обумовлює значне підвищення часу на виконання кожного запуску алгоритму.

Для з'ясування факторів, що впливають на підвищення загальної кількості ітерації, розглянемо окремі події, що відбуваються у процесі виконання алгоритму:

- Середньоарифметичне значення (усереднене по 100 запускам) кількості прийнятих погіршень функції вартості, за окремий запуск алгоритму імітації відпалу, зображено на тривимірному графіку – рис. 12. На рис. 13 наведено сумарне значення середньоарифметичної кількості прийнятих погіршень функції вартості за всіма ітераціями впродовж одного запуску алгоритму. Двовимірний графік отримано з тривимірного шляхом підсумовування всіх значень у кожній ітерації для окремого значення температури;
- Приклад середньоарифметичного значення (усереднене по 100 запускам) кількості не прийнятих погіршень функції вартості, за окремий запуск, зображено на тривимірному графіку – рис. 14. На рис. 15 наведено сумарне значення середньоарифметичної кількості неприйнятих погіршень функції вартості за всіма ітераціями впродовж одного запуску алгоритму. Двовимірний графік отримано з тривимірного шляхом підсумовування всіх значень у кожній ітерації для окремого значення температури. Стан найкращого з найдених поточних рішень в обох випадках залишається незмінним;
- Середньоарифметичне значення (усереднене по 100 запускам) кількості прийнятих покращень функції вартості, за окремий запуск алгоритму, зображено на три-

вимірному графіку – рис. 16. На рис. 17 наведено сумарне значення середньоарифметичної кількості прийнятих покращень функції вартості за всіма ітераціями впродовж одного запуску алгоритму. Двовимірний графік отримано з тривимірного шляхом підсумовування всіх значень у кожній ітерації для окремого значення температури;

- Середнєьоарифметичне значення (усереднене по 100 запускам) кількості неприйнятих покращень функції вартості, за окремий запуск алгоритму, зображено на тривимірному графіку – рис. 18. На рис. 19 наведено сумарне значення середньоарифметичної кількості неприйнятих покращень функції вартості за всіма ітераціями впродовж одного запуску алгоритму. Двовимірний графік отримано з тривимірного шляхом підсумовування всіх значень у кожній ітерації для окремого значення температури.

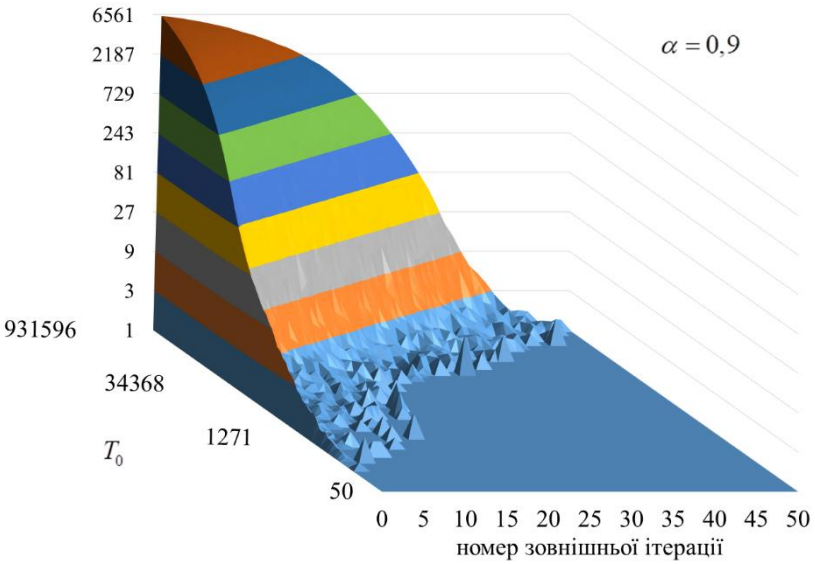


Рис. 12. Середньоарифметичне значення кількості прийнятих погіршень функції вартості у ітераціях при $\alpha = 0,9$

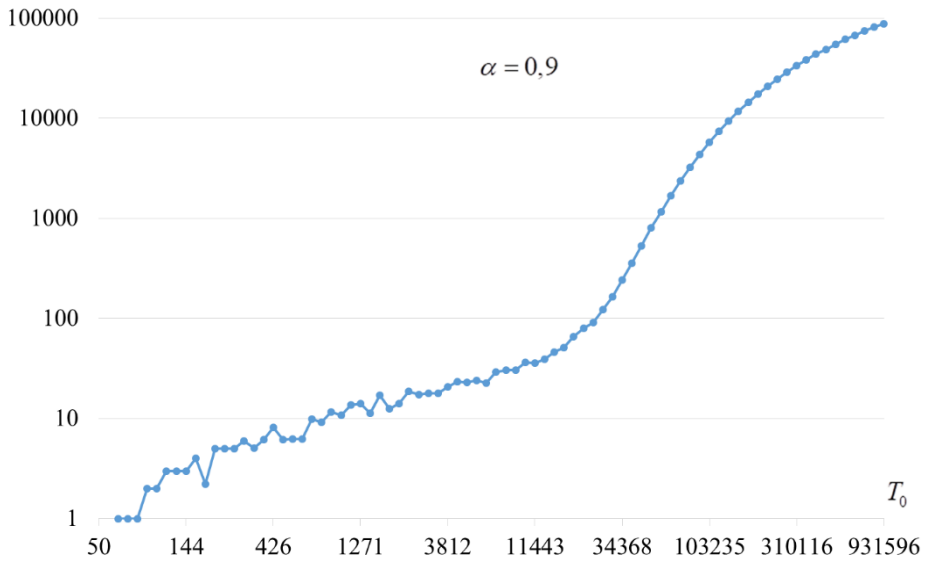


Рис. 13. Сумарне число середньоарифметичної кількості прийнятих погіршень функції вартості у ітераціях при $\alpha = 0,9$

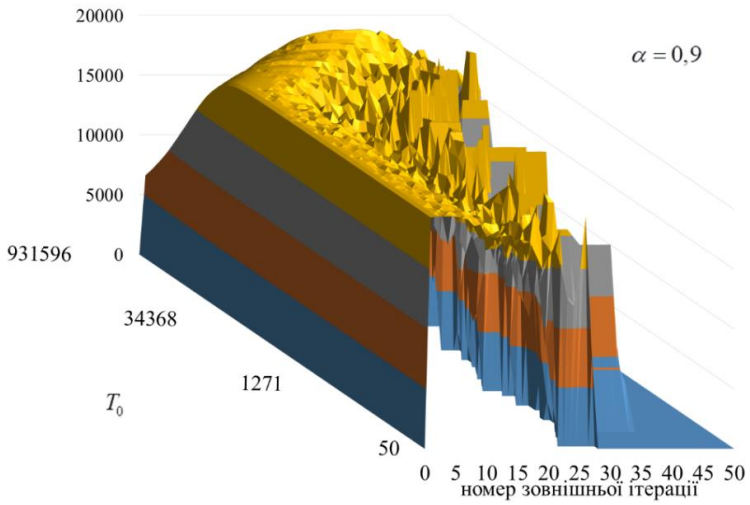


Рис. 14. Середньоарифметичне значення кількості неприйнятих погіршень функції вартості у ітераціях при $\alpha = 0,9$

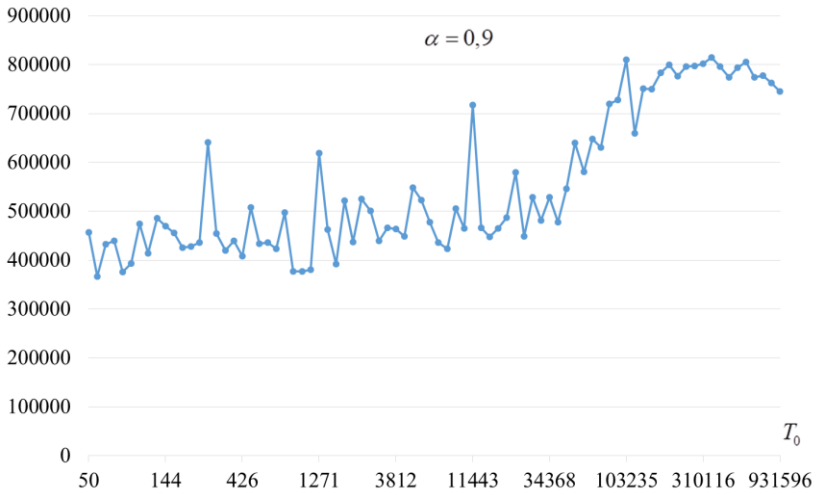


Рис. 15. Сумарне число середньоарифметичної кількості неприйнятих погіршень функції вартості у ітераціях при $\alpha = 0,9$

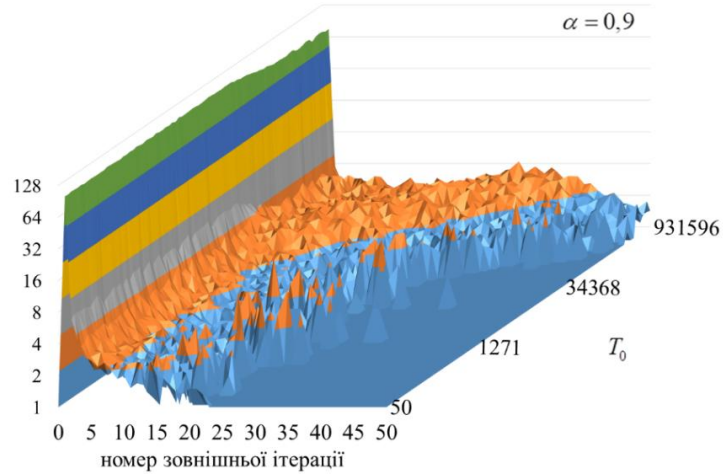


Рис. 16. Середньоарифметичне значення кількості прийнятих покращень функції вартості у ітераціях при $\alpha = 0,9$

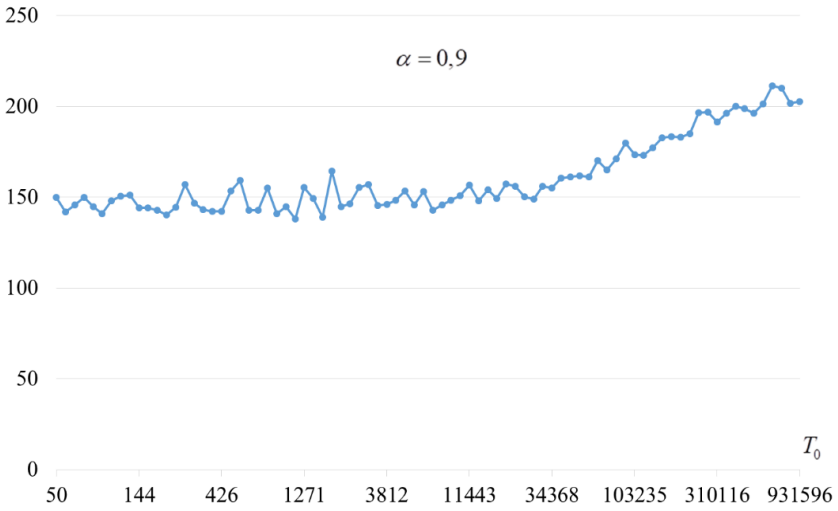


Рис. 17. Сумарне число середньоарифметичної кількості прийнятих покращень функції вартості у ітераціях при $\alpha = 0,9$

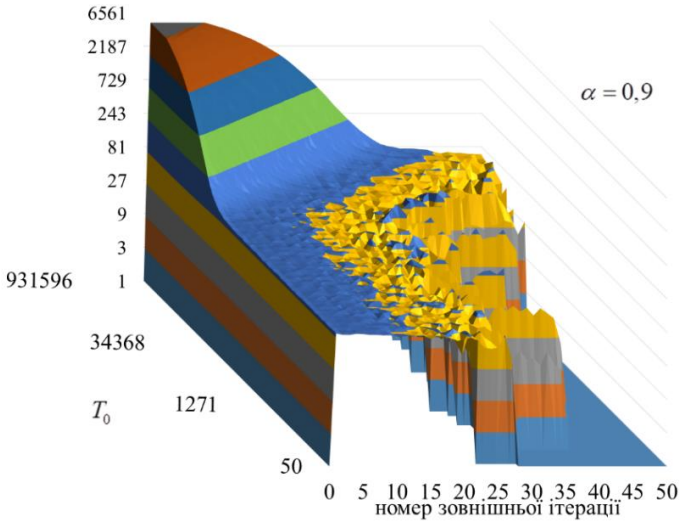


Рис. 18. Середньоарифметичне значення кількості неприйнятих покращень функції вартості у ітераціях при $\alpha = 0,9$

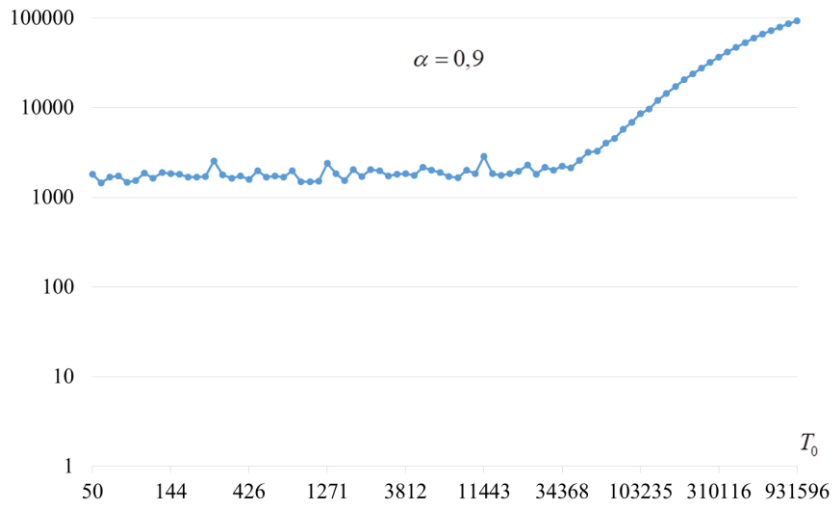


Рис. 19. Сумарне число середньоарифметичної кількості неприйнятих покращень функції вартості

Обговорення результатів

Як наведено у [16], при обраних вхідних параметрах, ймовірність формування цільового S-блоку за допомогою алгоритму локального пошуку складає 0,215, середній час пошуку одного блоку – 33,2 секунди.

При малих значеннях початкової температури ймовірність прийняття погіршуючого рішення дуже мала і тому алгоритм імітації відпалу веде себе яка звичайний алгоритм пошуку локального мінімуму та, відповідно, має такій ж самі значення ймовірності сформувати цільовий S-блок та середній час пошуку.

При збільшенні початкової температури збільшується ймовірність прийняття погіршуючих рішень, що приводить до виходу з поточного стану, яке, з одного боку, може бути непотрібним локальним мінімумом, а з іншого – одним з прийнятних рішень, яке може привести до формування цільового S-блоку. Аналіз отриманих результатів вказує на те, що середнє арифметичне значення нелінійності N_f досягається приблизно при ітерації зовнішнього циклу, що відповідає поточної температурі знайденого мінімуму ($T_0 = 20\,000 \ldots 40\,000$).

Більш висока температура приводить до появлення так званих *непродуктивних погіршень*, тобто погіршення, які приводять до постійного відкату найденого рішення до погіршеного стану. Тому більшу кількість ітерацій, яка здійснена при непродуктивних погіршеннях, можливо також віднести до *непродуктивних ітерацій*, тобто таких, які не приводять до покращення загального стану системи.

З аналізу результатів N_f видно, що у правій частині середні арифметичні значення N_f досягають значень, які відповідають лівій частині після першої ітерації зовнішнього циклу, лише приблизно після кількості ітерацій, які приводять поточну температуру до значень знайденого мінімуму ($T_0 = 20\,000 \ldots 40\,000$).

Також змінюється час пошуку цільового S-блоку. Починаючи з малих значень T_0, при поступовому збільшені, час пошуку скорочується та в кінці середнього етапу може складати у 1,5 – 2 рази менше значення. Потім, враховуючи значну кількість непродуктивних погіршень, час пошуку значно зростає. Чим вище значення T_0, тім більше така кількість непродуктивних погіршень, чим вище значення α, тим довше воно триває.

При високому значенні початкової температури або низькій швидкості її знижування, необхідна значна кількість зовнішніх циклів для стабілізації системи у деякому локальному мінімумі. При недостатній максимальній кількості зовнішніх циклів алгоритм може не знайти локальний мінімум, що приведе до значного зниження кількості знайдених рішень або їх повної відсутності.

Значення початкової температури, при якій ймовірність знайти цільовий S-блок є максимальною та ще не спостерігаються непродуктивні ітерації, будемо називати *оптимальною температурою* (позначимо як T_0^{opt}). Знайдений мінімум середнього часу формування цільового S-блоку відповідає інтервалу початкової температури $T_0^{\text{opt}} = 20\,000 - 40\,000$. Зі збільшенням параметру α мінімум зсувається в бік меншого значення T_0.

Для підвищення точності отриманих значень було підвищено кількість запусків для кожної температури до 1000. Для прийнятного часу тестування було зменшено діапазон значень $T_0 = 12500 - 37500$ та протестовано всього 11 значень T_0 при трьох значеннях $\alpha = 0{,}85; 0{,}9; 0{,}95$ (тестування проведено за 77 годин). Результати ймовірності формування цільового S-блоку та середній час формування наведено на рис. 20 та 21, пунктир – апроксимаційне значення.

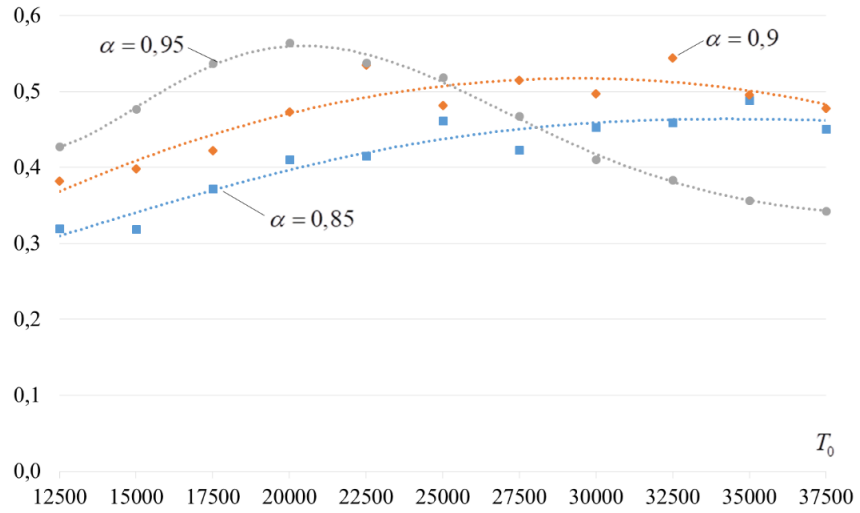


Рис. 20. Ймовірність формування цільового S-блоку при $\alpha = 0{,}85;\ 0{,}9;\ 0{,}95$ та max_inner_loops=650
(кожна точка – середнє значення за 1000 тестів)

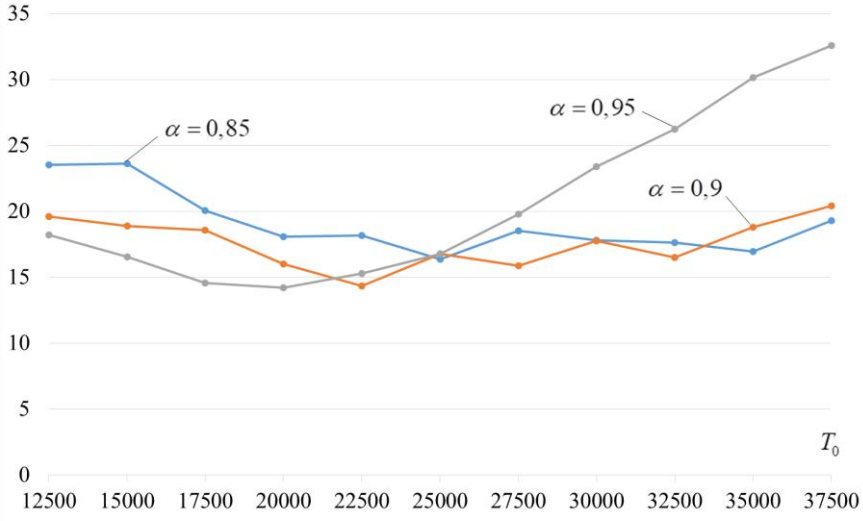


Рис. 21. Середній час (с) формування цільового S-блоку при $\alpha = 0{,}85;\ 0{,}9;\ 0{,}95$ та max_inner_loops=650
(кожна точка – середнє значення за 1000 тестів)

Згідно з наведеними даними при обраних параметрах (max_outer_loops=50, max_inner_loops=650, max_frozen_outer_loops=5, thread_count=30), найкращі результати отримано при $\alpha = 0{,}95$ та $T_0 = 20\,000$. Ймовірність знайти цільовий S-блок (з $N_f = 104$) дорівнює 56,4 %, а середній час пошуку складає 14,2 с.

Для порівняння отриманих результатів із іншими відомими реалізаціями SA алгоритму в табл. 2 наведено оцінки складності пошуку цільового S-блоку (із нелінійністю N_f).

Таблиця 2

Порівняння отриманих результатів з генерації бієктивних 8-бітних S-блоків
(для різних реалізацій SA алгоритму)

Параметр	[8, 22]	[20]	[19]	**Our work**
Найвище значення N_f, що було отримано у знайденому S-блоку	102	92	104	**104**
Ймовірність формування S-блоку	1/200 = 0,5%	–	–	**56,4 %**
Час генерації (пошуку) S-блоку	–	–	–	**14,2 с**
Складність генерації (кількість ітерацій пошуку)	–	–	30,000,000	**450,000**

Позначеннями «–» в табл. 2 наведено випадки з невизначеними показниками.

Висновки

За результатами досліджень робимо висновок, що метод імітації відпалу добре проводить пошук цільового (тобто з заданими властивостями) S-блоку. При вдало підібраних параметрах алгоритму ймовірність знайти S-блок з нелінійністю $N_f = 104$ буде дорівнювати майже одиниці. Однак 100 % ймовірність знайти цільовий S-блок не є оптимальним шляхом з точки зору затраченого на пошук часу. Введення додаткових обмежень зменшує час, що затрачується при кожній спробі, але й зменшує ймовірність знайти цільовий S-блок у кожній спробі. Тому результати пошуку за допомогою методу імітації відпалу дуже чутливі до майже всіх вхідних параметрів пошуку, а їх оптимізація є дуже трудомістким процесом.

Під час дослідження було вивчено вплив вхідних параметрів методу імітації відпалу на результат пошуку цільового S-блоку. За результатами досліджень наведено порівняльні характеристики часу пошуку та внутрішніх станів алгоритму, проведено оптимізацію за критерієм мінімізації часу пошуку.

При обраних параметрах алгоритму (max_outer_loops=50, max_inner_loops=650, max_frozen_outer_loops=5, thread_count=30) найкращі результати було отримано при $\alpha = 0,95$ та $T_0 = 20\,000$. При цьому ймовірність знайти цільовий S-блок (з $N_f = 104$) дорівнює 56,4 %, а середній час пошуку складає 14,2 с. При цьому алгоритм потребує в середньому близько 450,000 ітерацій пошуку. При підвищенні кількості внутрішніх ітерацій ймовірність знайти цільовий S-блок підвищується до 97 %. Це кращий із відомих результатів застосування SA алгоритму для генерації бієктивних 8-бітних S-блоків.

Список літератури:

1. Álvarez-Cubero J. Vector Boolean Functions: applications in symmetric cryptography, (2015). https://doi.org/10.13140/RG.2.2.12540.23685.
2. Cusick T., Stănică P. Cryptographic Boolean Functions and Applications: Second edition. (2017).
3. Freyre Echevarría A. Evolución híbrida de s-cajas no lineales resistentes a ataques de potencia, (2020). https://doi.org/10.13140/RG.2.2.17037.77284/1.
4. Schneier B. Applied cryptography: protocols, algorithms, and source code in C. New York : Wiley (1996).
5. Menezes A.J., Oorschot P.C. van, Vanstone S.A., Oorschot P.C. van, Vanstone S.A. Handbook of Applied Cryptography. CRC Press (2018). https://doi.org/10.1201/9780429466335.
6. Kuznetsov A.A., Potii O.V., Poluyanenko N.A., Gorbenko Y.I., Kryvinska N. Stream Ciphers in Modern Real-time IT Systems: Analysis, Design and Comparative Studies. Springer International Publishing (2022). https://doi.org/10.1007/978-3-030-79770-6.
7. Delahaye D., Chaimatanan S., Mongeau M. Simulated annealing: From basics to applications. In: Gendreau, M. and Potvin, J.-Y. (eds.) Handbook of Metaheuristics. pp. 1-35.ISBN 978-3-319-91085–7. Springer (2019). https://doi.org/10.1007/978-3-319-91086-4_1.
8. Clark J.A., Jacob J.L., Stepney S. The design of s-boxes by simulated annealing. In: Proceedings of the 2004 Congress on Evolutionary Computation (IEEE Cat. No.04TH8753). pp. 1533-1537 Vol.2 (2004). https://doi.org/10.1109/CEC.2004.1331078.
9. Tesar P. A New Method for Generating High Non-linearity S-Boxes. (2010).
10. Picek S., Cupic M., Rotim L. A New Cost Function for Evolution of S-Boxes. Evolutionary Computation. 24, 695–718 (2016). https://doi.org/10.1162/EVCO_a_00191.
11. Freyre-Echevarría A., Alanezi A., Martínez-Díaz I., Ahmad M., Abd El-Latif A.A., Kolivand, H., Razaq, A. An External Parameter Independent Novel Cost Function for Evolving Bijective Substitution-Boxes. Symmetry. 12, 1896 (2020). https://doi.org/10.3390/sym12111896.
12. Freyre Echevarría A., Martínez Díaz I. A new cost function to improve nonlinearity of bijective S-boxes. (2020).
13. Kuznetsov A., Poluyanenko N., Kandii S., Zaichenko Y., Prokopovich-Tkachenko D., Katkova T. WHS Cost Function for Generating S-boxes // 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S T). pp. 434–438 (2021). https://doi.org/10.1109/PICST54195.2021.9772133.
14. Ivanov G., Nikolov N., Nikova S. Reversed genetic algorithms for generation of bijective s-boxes with good cryptographic properties. Cryptogr. Commun. 8, 247–276 (2016). https://doi.org/10.1007/s12095-015-0170-5.
15. Rodinko M., Oliynykov R., Gorbenko Y. Optimization of the High Nonlinear S-Boxes Generation Method. Tatra Mountains Mathematical Publications. 70, 93–105 (2017). https://doi.org/10.1515/tmmp-2017-0020.
16. Kuznetsov A., Poluyanenko N., Kandii S., Zaichenko Y., Prokopovich-Tkachenko D., Katkova T. Optimizing the Local Search Algorithm for Generating S-Boxes // 2021 IEEE 8th International Conference on Problems of

Infocommunications, Science and Technology (PIC S T). pp. 458–464 (2021). https://doi.org/10.1109/PICST54195.2021.9772163.

17. Chen G. A novel heuristic method for obtaining S-boxes. Chaos, Solitons & Fractals. 36, 1028–1036 (2008). https://doi.org/10.1016/j.chaos.2006.08.003.

18. Souravlias D., Parsopoulos K.E., Meletiou G.C. Designing bijective S-boxes using Algorithm Portfolios with limited time budgets. Applied Soft Computing. 59, 475–486 (2017). https://doi.org/10.1016/j.asoc.2017.05.052.

19. McLaughlin J., Clark J.A. Using evolutionary computation to create vectorial Boolean functions with low differential uniformity and high nonlinearity. arXiv (2013). https://doi.org/10.48550/arXiv.1301.6972.

20. Wang J., Zhu Y., Zhou C., Qi Z. Construction Method and Performance Analysis of Chaotic S-Box Based on a Memorable Simulated Annealing Algorithm. Symmetry. 12, 2115 (2020). https://doi.org/10.3390/sym12122115.

21. McLaughlin J. Applications of search techniques to cryptanalysis and the construction of cipher components, https://etheses.whiterose.ac.uk/3674/, (2012).

22. Ivanov G., Nikolov N., Nikova S. Cryptographically Strong S-Boxes Generated by Modified Immune Algorithm // Pasalic, E. and Knudsen, L.R. (eds.) Cryptography and Information Security in the Balkans. pp. 31–42. Springer International Publishing, Cham (2016). https://doi.org/10.1007/978-3-319-29172-7_3.

Надійшла до редколегії 10.05.2022

Відомості про авторів:

Кузнецов Олександр Олександрович – 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: kuznetsov@karazin.ua; ORCID: https://orcid.org/0000-0003-2331-6326

Полуяненко Микола Олександрович – канд. техн. наук, Харківський національний університет імені В.Н. Каразіна, доцент кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук; Україна; e-mail: nlfsr01@gmail.com; ORCID: https://orcid.org/0000-0001-9386-2547

Кандій Сергій Олегович – технік-конструктор, АТ «Інститут інформаційних технологій», Україна; e-mail: sergey.kandy@gmail.com, ORCID: https://orcid.org/0000-0003-0552-8341

Логачова Єлизавета Олегівна – студентка кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук; Харківський національний університет імені В.Н. Каразіна, Україна; e-mail: lohachova2020kb11@student.karazin.ua, ORCID: https:// orcid.org/0000-0002-9815-466X

УДК 004.056.52 **DOI:10.30837/rt.2022.2.209.11**

В.О. ПОДДУБНИЙ, Р.Ю. ГВОЗДЬОВ, О.В. СЄВЄРІНОВ, канд. техн. наук,
В.М. ФЕДОРЧЕНКО, канд. техн. наук

ОБ'ЄКТНО-ОРІЄНТОВАНА МОДЕЛЬ ФОРМАЛЬНОГО ОПИСУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ СИСТЕМИ

Вступ

Під час проєктування (побудови) систем захисту інформації в інформаційно-комунікаційних системах розробники стикаються з великою кількістю проблем. Одна з таких проблем – це створення опису інформаційно-комунікаційної системи та механізмів захисту, який би повністю відображав систему, інформацію та зв'язки між об'єктами системи. Такий опис повинен бути формалізованим, тобто мати таке представлення, яке базується на чітко визначених математичних концепціях. В свою чергу, математичні концепції визначають синтаксис і семантику подання, що дозволяє унеможливити неоднозначність розуміння моделі.

Метою статті є розгляд алгоритму формального опису на основі взаємозв'язків об'єктів.

Процес побудови опису інформаційно-комунікаційної системи

Основним етапом при проєктуванні та побудові систем захисту інформації в інформаційно-комунікаційних системах (далі – ІКС) є документований опис роботи інформаційної системи. Існують багато підходів та методів для такого опису, але в основному детально розглядаються та аналізуються наступні компоненти інформаційно-комунікаційної системи:

– фізичне середовище;
– середовище обчислювальної системи;
– середовище користувачів;
– інформаційне середовище.

При розгляді фізичного середовища здійснюється аналіз апаратних засобів обробки інформації, комунікаційного обладнання, а також режим функціонування цих об'єктів.

При розгляді обчислювальної системи інформаційно-комунікаційної системи описується загальний склад технічних і програмних засобів, їхні зв'язки, особливості конфігурації, архітектури й топології.

При аналізі середовища користувачів фіксується функціональний та кількісний склад користувачів, їх функціональні обов'язки та рівень кваліфікації, повноваження щодо допуску до відомостей, які обробляються в ІКС, доступу до ІТС та її окремих компонентів, рівень можливостей різних категорій користувачів в системі.

При розгляді інформаційного середовища аналізу підлягає вся інформація, що обробляється, а також зберігається в ІКС. Також виділяється критична інформація в системі та властивості захищеності інформації, що повинні бути їм притаманні (конфіденційність, цілісність, доступність).

Типовий зміст документу (інструкції) опису системи містить неформальний опис наведених вище середовищ функціонування системи, може містити загальну структурну схему, схему інформаційних потоків та безліч інших таблиць і схем (правила розмежування доступу, перелік та представлення в системі інформаційних об'єктів тощо) [1, 2].

Як приклад, на рис. 1 наведена загальна структурна схема типової інформаційно-комунікаційної системи, яка представляє собою веб-сайт, що функціонує під керуванням веб-серверів, які, в свою чергу функціонують у віртуальному середовищі. Фізичний (апаратний) сервер у складі окремого сегменту мережі має доступ до мережі Інтернет через комунікаційне обладнання та міжмережевий екран. Адміністрування серверу здійснюється через робочу станцію адміністратора серверу, яка підключення до комутатора.

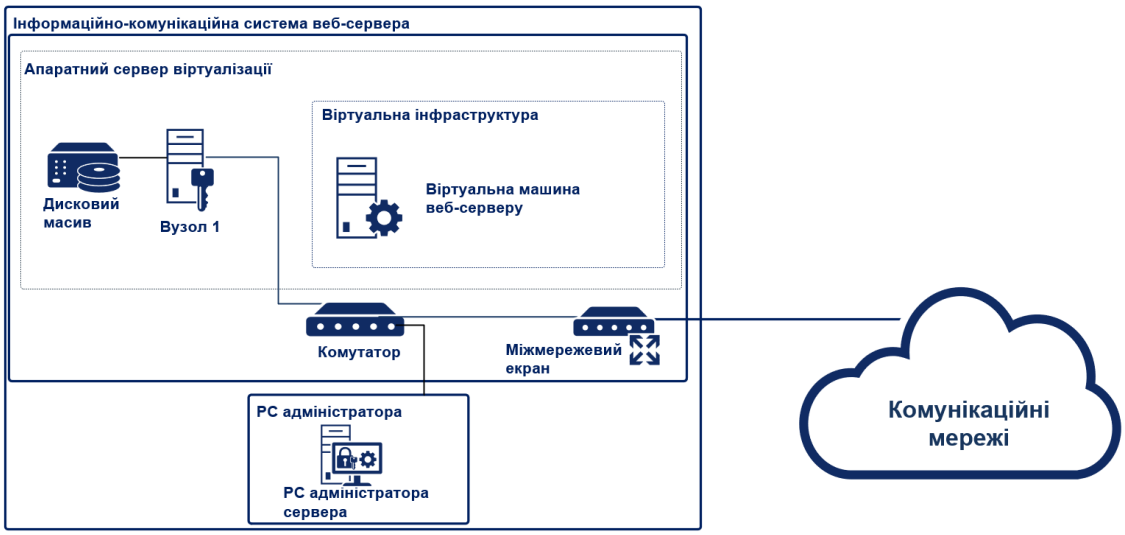


Рис. 1. Загальна структурна схема типової ІКС

Наведена на рис. 1 структурна схема є прикладом простої у розумінні системи. Зазвичай інформаційно-комунікаційні системи мають набагато більше технічних засобів, функцій, користувачів, в деяких випадках навіть мати у своєму складі спеціалізовані апаратні засоби захисту інформації.

Виникає необхідність у механізмі єдиного опису системи, що буде включати в себе всі середовища. Такий опис буде однозначно формалізований з чітко визначеними математичними поняттями. Механізм єдиного формального опису або методика формального опису ІКС буде однозначна в розумінні та слугуватиме керуючим описом при розробці політики безпеки інформації в ІКС.

Основні проблеми при побудові алгоритму формального опису ІКС є розробка уніфікованої системи опису, що дозволить врахувати усі варіанти зміни стану системи та складність розуміння такого опису.

Проблему складності розуміння опису можна вирішити шляхом залучення висококваліфікаційного персоналу та навчання нових користувачів, що відповідальні за дані задачі.

Проблема розробки єдиного формального опису може критично вплинути на менеджмент процесів управління системою, бо може виникнути ситуація, коли методика формального опису не має інструментів (математики) опису нових механізмів або функцій. Цю проблему можна вирішити шляхом тестового впровадження методики опису до різних ІКС та постійний аналіз і покращення алгоритму опису та математичної бази [3].

Формальні методики опису ІКС

Проблема створення методик формального опису не є новою, найбільш часто розглядалися такі мови формального опису, як UML, розширення UMLsec, Ponder 2.

В роботі [4] пропонується використання мови UML або розширення UMLsec для побудови моделі мережі. Проте, така модель складніша за рахунок переліку стереотипів та властивості даних, оскільки UML – це універсальна мова, яка створювалася для опису в області розробки ПЗ, системного програмування, бізнес процесів. Розширення UMLsec додає додаткові стереотипи та типи даних, ускладнюючи існуючу модель. Це не означає, що за допомогою UML неможливо здійснювати опис системи, даний процес буде більш складним і потре-

буватиме більше часу. Нотація мови UML не має змогу відобразити головні елементи ІКС та архітектуру механізмів захисту системи.

Загальна структура запропонованої методики

Пропонується створення нової моделі формального опису системи. В даній системі пропонується зосередитися на типах об'єктів та взаємодії об'єктів один з іншим. В такій схемі відбувається зосередження уваги на таких поняттях як:

1. Об'єкт;
2. Характеристики об'єкту;
3. Тип взаємодії з об'єктом.

Об'єкт – фізичний, операційна система, віртуальний пристрій, програма, інформація. Абстрактна модель, що має чітке відображення, має характеристики, цінність для ІКС, може взаємодіяти з іншими об'єктами.

Характеристики об'єкту являються його змінними, до даних характеристик відносяться як його явні характеристик та характеристики що надаються політикою безпеки ІКС (вимоги до КЦД, користувачі що можуть використовувати об'єкт)

Тип взаємодії (характеристика) – вплив одного об'єкта на інший, внаслідок якого відбувається взаємодія двох об'єктів,.

Об'єкт, що відображає інформацію, не містить деяких полів, що буде показано далі.

Дана модель схожа до UML, проте пропонується зменшення та переробка стереотипів. Дані стереотипи реалізовані в вигляді окремих полів. Перелік полів наведений в таблиці 1. Деякі поля можуть мати рівні (тобто являтися заголовками для інших).

Структурна форма об'єкту наведена нижче, кожний об'єкт починається з заголовку першого рівня (Element) та містить окремі характеристики. Внесення та обробку таких елементів планується виконати за допомогою програмного забезпечення. Знаком «#»зображені коментарі.

Element:
ID: # ID елемента для посилань
Type: Physical/OS/VM/ Program/Information/ #Тип елемента
Name: #назва елемента
CIA: x/y/z # К/Ц/Д в якісній шкалі
UserRead: #Перелік користувачів, що можуть читати об'єкт
UserWrite: #Перелік користувачів, що можуть змінювати об'єкт
UserCreate: #Перелік користувачів, що можуть створювати об'єкт
UserDel: #Перелік користувачів, що можуть видаляти об'єкт
Domen: #Елементи, що виконують даний елемент
  ElementD1: ID
  ElementD2: ID
    …….
Connected in: #Вхідні з'єднання
  Connection 1:
    Element: ID #Елемент, з яким відбувається з'єднання
    Transition element: ID #Елемент, що передається (посилання)
    Type connected: admin control/local use/ send data #Тип з'єднання
  Connection 2:
  …….
Connected out:
  Connection 1:
    Element: ID
    Transition element: ID
    Type connected: admin control/local use/ send data
  Connection 2:
  ……

Таблиця 1

Назва	Пояснення	Значення, що може набувати	Пояснення
Element	Заголовок окремого об'єкту	-	Рівень 1
ID	ID об'єкту слугує для технічних потреб при програмній реалізації моделі. Також може слугувати для відображення групи елементів	Беззнакове ціле число	
Type	Тип елементу	Physical	Фізичний пристрій
		OS	Операційна система
		VM	Гіпервізор
		Program	Програмний засіб
		Information	Дані/інформація
Name	Назва елементу (пояснення)	Рядок	
CIA	Вимоги до об'єкту відносно його цілісності/ конфіденційності/доступності	Беззнакове ціле число для цілісності/ конфіденційності/ доступності	Максимальне значення встановлюється згідно політики безпеки
UserRead	Перелік користувачів, що можуть читати об'єкт	Рядок	Згідно політики безпеки
UserWrit	Перелік користувачів, що можуть змінювати об'єкт	Рядок	Згідно політики безпеки
UserCreate	Перелік користувачів, що можуть створювати об'єкт	Рядок	Згідно політики безпеки
Domen	Заголовок доменів. Перелік об'єктів, для яких об'єкт являється доменом (обробляються) об'єктом	-	Рівень 2
ElementDx	Посилання на елемент за допомогою ID	Беззнакове ціле число (з ID, що були створені)	Кількість елементів необмежена
Connected in	Заголовок об'єктів, що взаємодіють на даний об'єкт		Рівень 2
Element: ID	Елемент, з яким відбувається з'єднання	Беззнакове ціле число (з ID, що були створені)	
Transition element	Елемент, що передається	Беззнакове ціле число (з ID, що були створені)	
Type connected	Тип взаємодії	admin control	адміністративний контроль
		local use	використання ресурсів
		send data	відправка даних
Connected out	Заголовок об'єктів, з якими взаємодіє даний об'єкт		Рівень 2
Element: ID	Елемент, з яким відбувається з'єднання	Беззнакове ціле число (з ID, що були створені)	
Transition element	Елемент, що передається	Беззнакове ціле число (з ID, що були створені)	
Type connected	Тип взаємодії	admin control	адміністративний контроль
		local use	використання ресурсів
		send data	відправка даних

Процес побудови формального опису з використанням запропонованої методики

Процес створення опису системи здійснюється по наступних етапах:

1. Визначається перелік інформації що функціонує в системі;
2. Створюються об'єкти інформації;
3. Визначаються об'єкти, що здійснюють обробку інформації;
4. Поетапно створюються об'єкти Physical (фізичний), OS (операційна система), VM (віртуальний), Program (програмний), Information (інформаційний), що здійснюють обробку інформації;

5. Формується логічний зв'язок об’єктів, що були створені;

6. Політикою безпеки визначається цінність кожного об’єкту та визначаються ролі користувачів;

7. Внесення політики безпеки до створеної структури;

8. Перегляд та взаємне доповнення політики та створеної структури.

Як приклад розглянемо взаємодію веб-браузера та веб-сервера. Створення моделі відбуватиметься поетапно.

1. На етапі №1 відбувається визначення об’єктів інформації (в даному прикладі це веб-сторінка та веб-запит).

2. На етапі №2 відбувається залучення даної моделі для створення об’єктів інформації:

Element: # Елемент веб-сторінки:
ID: 100
Type: Information
Name: Web-page
CIA:
UserRead:
UserWrite:
UserCreate:
UserDel:
Domen: -
Connected in: -
Connected out: -

Element: #Веб-запит :
ID: 101
Type: Information
Name: request
CIA:
UserRead:
UserWrite:
UserCreate:
UserDel: -
Domen: -
Connected in: -
Connected out: -

На даному етапі об’єкти не містять полів пов’язаних з політикою безпеки. Об’єкт інформації не містить полів Domen, Connected in, Connected out, за визначенням властивості інформації.

3. На етапі №3 відбувається визначення об’єктів, що здійснюють обробку інформації. В прикладі якості веб-сервера використовується Apache2, в якості веб-браузера Google Chrome. В даному прикладі ми не будемо опускатися до низьких рівнів опису об’єктів (Операційна система та фізичний пристрій) для спрощення прикладу. Глибину опису розробник вибирає сам на свій розсуд та згідно з висунутих вимог.

4. Далі, на етапі №4 здійснюється створення об’єктів обробки інформації:

Element: #Apache
ID: 103
Type: Program
Name: Apache2
CIA:
UserRead:
UserWrite: -
UserCreate:
UserDel:
Domen:
Connected in:
Connected out:

Element: # Google Chrome
ID: 104
Type: Program
Name: Chrome
CIA:
UserRead:
UserWrite: -
UserCreate:
UserDel:
Domen:
Connected in:
Connected out:

5. На етапі №5 формується зв’язок елементів, заповнюються поля взаємозв’язку (Connected in, Connected out) та вносяться елементи, для яких об’єкт являється доменом виконання (Domen):

Element: #Apache
ID: 103
Type: Program
Name: Apache2
CIA:

Element: # Google Chrome
ID: 104
Type: Program
Name: Chrome
CIA:

UserRead:
UserWrite: -
UserCreate:
UserDel:
Domen:
Element: 100 #домен для веб-сторінки
Connected in:
Connection 1:
Element: 104 #вхідне #з'єднання з веб-браузером
Transition element: 102 #веб-браузер
Type connected: send data #передача даних
Connected out:
Connection 1:
Element: 104 #вхідне #з'єднання з веб-браузером
Transition element: 100# передача сторінки до веб-браузеру
Type connected: send data

UserRead:
UserWrite:
UserCreate:
UserDel:
Domen:
Element: 102 #Домен відповіді
Connected in:
Connection 1:
Element: 103 #Apache
Transition element: 100 #передача сторінки до веб-браузеру
Type connected: send data
Connected out:
Connection 1:
Element: 103
Transition element: 102 #передача запиту веб-браузером
Type connected: send data

6. На етапі №6 відбувається призначення об'єктам цінності та визначення користувачів, в якості прикладу – це адміністратор веб-серверу «Admin» та користувач «User». Тег «ALL» значить, що вибрані всі користувачі. Кінцевий опис виглядає так:

Element: # Елемент веб-сторінки:
ID: 100
Type: Information
Name: Web-page
CIA: 0/2/5
UserRead: ALL
UserWrite: Admin
UserCreate: Admin
UserDel: Admin
Domen: -
Connected in: -
Connected out: -

Element: #Веб-запит :
ID: 101
Type: Information
Name: request
CIA: 0/2/2
UserRead: User
UserWrite: User
UserCreate: User
UserDel: -
Domen: -
Connected in: -
Connected out: -

Element: #Apache
ID: 103
Type: Program
Name: Apache2
CIA: 0/2/5
UserRead: Admin
UserWrite: -
UserCreate: Admin
UserDel: Admin
Domen:
Element: 100 #домен для веб-сторінки
Connected in:
Connection 1:

Element: # Google Chrome
ID: 104
Type: Program
Name: Chrome
CIA: 0/0/0
UserRead: ALL
UserWrite: -
UserCreate: ALL
UserDel: ALL
Domen:
Element: 102
Connected in:
Connection 1:

Element: 104 #Google Chrome
Transition element: 102 #передача відповіді
Type connected: send data #передача даних
Connected out:
Connection 1:
Element: 104//вхідне з'єднання з веб-браузером
Transition element: 100 #передача сторінки
Type connected: send data

Element: 103 #Apache
Transition element: 100 #передача сторінки до веб-браузеру
Type connected: send data
Connected out:
Connection 1:
Element: 103
Transition element: 102 #передача запиту веб-браузером
Type connected: send data

На рис. 2 показано графічне представлення розглянутого прикладу у вигляді блок-схеми. Кожен блок містить посилання на об'єкт що був створений раніше.

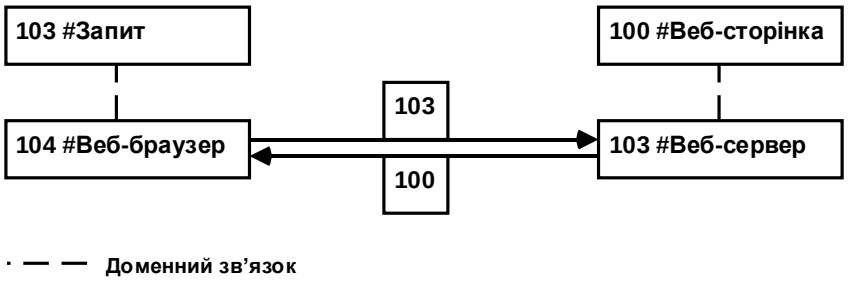


Рис. 2. Графічне представлення створеного прикладу

Можливості використання запропонованої моделі із залученням теорії графів

Пропонується подальший розгляд створених блок схем (графів) для дослідження можливостей використання даної моделі для симуляції кібератак. Оскільки кожний елемент містить поля, що зв'язують його з іншими елементами, а кожна атака має «точку входу» за допомогою теорії графів, можливо здійснювати обхід графу для визначення можливих шляхів горизонтального розповсюдження кібератаки.

Також в перспективі можливе додавання додаткових полів, що визначатимуть зрілість об'єкту (можливість об'єкту протистояти кібератакам). Після такого додавання стане можливим використання алгоритмів знаходження короткого шляху для визначення слабких місць мережі. До таких алгоритмів можна віднести алгоритм Дійкстри, Белмана – Форда, або знайти загальну зв'язність мережі за допомогою таких алгоритмів Клеймана, Прийм – Дійкстри та Крускаля. Такі алгоритми можуть бути залучені до процесу менеджменту вразливостями [5, 6].

Розробка програмних засобів для реалізації запропонованої моделі можлива будь-якою об'єктно-орієнтованою мовою програмування.

Висновки

Була запропонована модель формального опису інформаційно-комунікаційної системи з використанням об'єктного запису даних та графічного відображення. Основними перевагами такого опису є його цілеспрямованість під конкретні вимоги: опис ІКС, взаємозв'язок між об'єктами ІКС, взаємозв'язок опису ІКС та політики безпеки.

Наступними шляхами реалізації запропонованої моделі є:

– програмна реалізація засобу внесення та обробки даних;
– програмна реалізація представлення створюваних елементів у вигляді графів:

– дослідження можливості використання моделей графів для моделювання сценаріїв розповсюдження кібератаки;

– дослідження можливості додавання додаткових полів та можливості використання моделей графів для знаходження слабких місць мережі та визначення загальної зрілості мережі.

Така модель може пришвидшити розробку систем захисту інформації за рахунок автоматизації та стандартизації процесів, та покращити їх якість за рахунок формалізації та детального опису об'єктів, інтеграції з політикою безпеки. При наявності можливості використання теорії графів дана модель може здійснювати аналіз ІКС та будувати можливі шляхи розвитку атаки (з будь-якої точки мережі).

Список літератури:

1. НД ТЗІ 2.5-004.99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.

2. Закон України «Про захист інформації в інформаційно-комунікаційних системах».

3. НД ТЗІ 2.7-010-09. Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу.

4. Гвоздьов Р.Ю., Олійников Р.В. Метод та методика формального проєктування комплексної системи захисту інформації в інформаційно-телекомунікаційних системах // Радіотехніка. 2020. Вип. 203. С. 91-96.

5. Поддубний В.О., Сєвєрінов О., Пустомельник О. Менеджмент вразливостей як складова частина політики безпеки ІТС. Системи управління, навігації та зв'язку. Збірник наукових праць. Полтава : ПНТУ, 2020. Т. 4 (62). С. 55-58.

6. Poddubnyi V., Severinov O. Vulnerability management using a formalized description // Радіотехніка. 2020. Вип. 203. С. 121–125.

Надійшла до редколегії 07.06.2022

Відомості про авторів:

Поддубний Вадим Олександрович – аспірант кафедри безпеки інформаційних технологій, факультет комп'ютерної інженерії та управління, Харківський національний університет радіоелектроніки, Україна; e-mail: vadym.poddubnyi@nure.ua, ORCID: https://orcid.org/0000-0002-4380-491X

Гвоздьов Роман Юрійович – аспірант кафедри безпеки інформаційних технологій, факультет комп'ютерної інженерії та управління, Харківський національний університет радіоелектроніки, Україна; e-mail: roman.hvozdov@nure.ua, ORCID: https://orcid.org/0000-0002-5408-943X

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

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

УДК 681.3.06 **DOI:10.30837/rt.2022.2.209.12**

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

КОНЦЕПЦІЯ ОЦІНКИ РИЗИКІВ КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОБ'ЄКТА КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Вступ

Вважається, що основним підходом до забезпечення кібер- і інформаційної безпеки інформаційної системи є стратегія захисту на основі ризику [1]. Одним з головних завдань управління інформаційними ризиками є об'єктивно ідентифікувати і оцінити найбільш значущі для об'єкта критичної інфраструктури ризики. В [2] визначені критерії підходів до вибору методів оцінки і управління ризиками безпеки. Саме тому, на наш погляд, актуальним є пошук методів оцінки і управління ризиками безпеки, які в певній мірі відповідають визначеним критеріям. У цьому дослідженні використано один з відомих підходів до моделювання, – «дерево атак» [3]. Метод «дерева атак» є систематичним методом визначення характеристик безпеки системи на основі всіх атак, яким піддається інформаційна система. Виявлення всіх можливих атак полегшує аналіз можливих шляхів реалізації кібератак та вибір адекватних контрзаходів і їх оптимальне використання. Дерево атаки складається з вузлів, ребер та з'єднувальних елементів, де кожен вузол відповідає кроку атаки. Кореневий вузол є кінцевою метою зловмисника, а дочірні вузли даного вузла представляють підцілі. Ребра представляють зміну стану, спричинену діями зловмисника. З'єднувальний елемент – це шлях для просування до мети атаки: АБО (диз'юнктивне), чи І (кон'юнктивне) для вузлів із двома або більше дочірніми елементами.

Основні результати досліджень

Архітектура інформаційної системи

Інформаційна система компанії, відповідно до її компонентів, може бути розділена на дві частини: компоненти, які доступні користувачеві (наприклад, термінал), і компоненти, які доступні тільки постачальнику послуг, такі як сервер центрального офісу компанії. Можливі сценарії загроз безпеки, засновані на потоці інформації через зазначені компоненти, наведені нижче [4, 5] (рис. 1):

1) Поширення шкідливого коду у обладнанні, порушення бар'єру безпеки, доступ до конфіденційної інформації користувача та отримання доступу до основного сервера через сенсорний пристрій.

2) Виток інформації або підробка даних у процесі передачі даних.

3) Виявлення (вимірювання) ризиків витоку даних через вразливості у персональному комп'ютері (ПК), смарт-пристрої чи шлюзі, який використовується для передачі даних сховищем або персоналом.

4) Ризики кібератак через вразливість основного сервера та репозиторію в зоні дії провайдера.

Виявлення та ідентифікація загроз інформаційної системи компанії

Для того щоб виявити загрози, що можуть бути використані для побудови дерева атак інформаційної системи компанії, доцільно обрати типові та засновані на відповідних сценаріях загрози безпеки відповідно до ISO/IEC 27005 [6, 7]. Нарешті, щоб визначити вразливості інформаційної системи компанії, доцільно структурувати використані загрози, щоб зробити їх придатними для середовища інформаційної системи компанії відповідно до ISO/IEC 27005. Отримані дані використовувалися як компоненти дерева атак інформаційної системи компанії. Відповідно до архітектури системи, виявлених загроз безпеки та уразливостей, пропонується виділити сім областей загроз безпеці інформаційної системи компанії (рис. 2).



Рис. 1. Архітектура інформаційної системи компанії



Рис. 2. Області, що пов'язані із загрозами безпеки

Варіанти використання областей загроз безпеки інформаційної системи

З а г р о з а 1 : Користувач

При використанні користувачами терміналів часто виникають загрози безпеці, що пов'язані з помилками використання пристроїв, слабкими паролями, втратою пристроїв, фішингом тощо.

З а г р о з а 2 : Пристрої

Термінали засновані або на операційній системі загального призначення (GPOS) або на вбудованій операційній системі реального часу (RTOS). Пристрої на базі RTOS захищені від несанкціонованого доступу, оскільки вони оптимізовані для конкретних функцій на етапах проектування та виробництва. І навпаки, пристрої на основі GPOS, такі як смартфони, вразливі для загроз безпеки, оскільки вони використовують зовнішні програми. Використання терміналів у таких умовах робить їх вразливими для загроз безпеки через функції збереження та обміну даними цих пристроїв, а також ризик втрати/крадіжки пристрою, уразливості додатків та передачі відкритого тексту.

З а г р о з а 3 : Домашня мережа (мережа філіалу компанії)

Передача інформації між терміналом в особистому просторі користувача (вдома або в офісі) та до серверу центрального офісу компанії відбувається переважно бездротовою мережею. Як показано на рис. 3, типи мереж, що використовуються в домашніх умовах, включають LAN (локальна обчислювальна мережа), Wi-Fi, Bluetooth, NFC (комунікація ближнього радіусу дії) та мережі довгострокової еволюції. У той час як деякі пристрої вбудованого типу повинні бути підключені до локальних мереж, інтелектуальні пристрої на основі GPOS можуть зв'язуватися із сервером центрального офісу компанії. У таких умовах сервісні

системи на базі домашніх мереж піддаються загрозам безпеці, пов'язаним із наскрізною передачею відкритого тексту та атаками посередника (MITM-атаками) (рис. 3) [8].

З а г р о з а 4 : Шлюз, наприклад, VPN

Шлюз відіграє роль посередника між користувачем та сервером центрального офісу компанії, піддаючи систему загрозам безпеці, пов'язаними з шахрайськими шлюзами, а також втратою/крадіжкою шлюзів та MITM атаками [8].

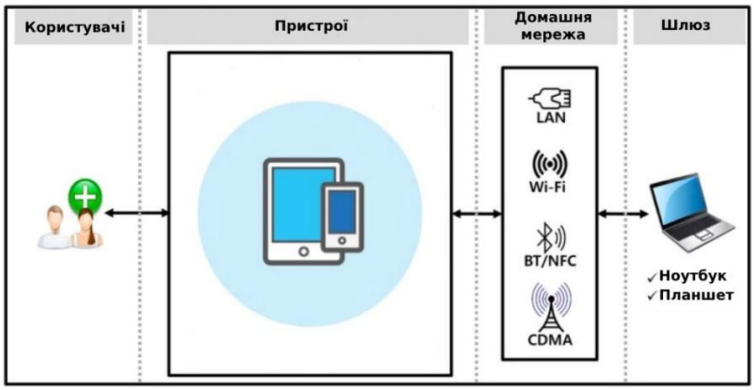


Рис. 3. Домашня мережа

З а г р о з а 5 : Інтернет (загальнодоступна мережа)

Зв'язок між користувачем та сервером центрального офісу компанії відбувається через мережу загального користування (Інтернет). Оскільки особиста інформація передається через загальнодоступний Інтернет, важливо встановити наскрізні правила безпеки. Крім того, потрібна зашифрована передача даних. У таких умовах інформаційна система компанії вразлива для загроз безпеки, пов'язаних з перехопленням даних, підробкою/зміною та підвищенням привілеїв [8].

З а г р о з а 6 : Сервер центрального офісу компанії

Сервер центрального офісу компанії знаходиться у місці розташування постачальника послуг. Він складається з ПК та програмного забезпечення, необхідного для віддалених консультацій, а його користувачами є персонал та системні адміністратори (співробітник служби безпеки та інший допоміжний персонал). Ця система дуже важлива, тому що вона опрацьовує всі дані користувачів. Крім того, якщо сервер центрального офісу компанії підключений до відповідних установ через урядовий мережевий концентратор, необхідні суворі правила безпеки для запобігання проникненню в державну систему. У таких умовах інформаційна система компанії може піддаватися загрозам безпеки, пов'язаним з MITM-атаками, шкідливим кодом, підробкою/зміною застосунків та незаконним доступом до мережі за допомогою обходу перевірок фізичної безпеки [8].

З а г р о з а 7 : Реалізація послуг, що надаються центральним офісом – постачальником послуг

У таких умовах інформаційна система компанії може приваблювати загрози безпеки, пов'язані з MITM-атаками, шкідливим кодом, підробкою/зміною застосунків та незаконним доступом до Korea-Net, оминаючи наявні перевірки фізичної безпеки [8]. Ця область також може бути вразливою для загроз безпеки, пов'язаних з помилками використання пристрою, витоком важливих даних та прослуховуванням телефонних розмов.

Метод дерева атак

Першим кроком в оцінці ризику безпеки є визначення задіяних активів та розрахунок їхньої вартості. Дерево атак використовується для оцінки всіх загроз безпеці, з якими може зіткнутися кожен актив, як визначено у кожній із семи областей загроз безпеці. Як показано на рис. 5, ймовірність виникнення атаки обчислюється з використанням з'єднувальних елементів АБО та І, які є входом для кожного вузла, що представляє просування атаки до мети.

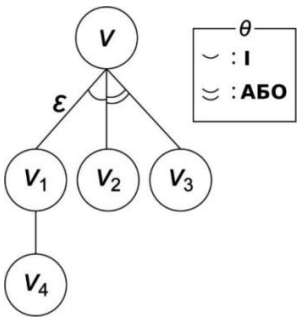


Рис. 5. Дерево атак

Теоретично, ймовірність успіху потенційної атаки збільшується прямо пропорційно до мотивації зловмисника і обернено пропорційно до зусиль, необхідних для організації атаки. У цьому дослідженні вартість активів, ймовірність виникнення атаки та ймовірність успіху атаки використовувалися як параметри оцінки ризиків безпеки, пов'язаних з інформаційною системою компанії.

На рис. 6 наведено приклад того, як проводиться оцінка ризиків. Методика оцінки ризику може бути стисло викладена наступним чином.

1. Оцінка вартості активів інформаційної системи компанії (див. табл. 1 – 3).

Таблиця 1

Критерії оцінки вартості активів

Розподіл	**Низький**	**Помірний**	**Високий**
Конфіденційність	1	2	3
Цілісність	1	2	3
Доступність	1	2	3
Внесок активів	1	2	3

Таблиця 2

Класифікація вартості активів

Мета безпеки	**Потенційна дія**	**Опис**
Конфіденційність	Високий	Повинний бути доступним усередині лише уповноваженим особам; несанкціоноване розкриття інформації може призвести до порушення конфіденційності особи та/або фатального пошкодження інформаційної системи компанії.
	Помірний	Може бути розкритий усередині, але у разі зовнішнього впливу може викликати серйозні проблеми щодо конфіденційності та інформаційної системи компанії.
	Низький	При впливі зовнішніх осіб матиме незначний вплив на приватне життя та інформаційну систему компанії.
Цілісність	Високий	Випадкові або навмисні зміни можуть завдати серйозної шкоди приватному життю або інформаційній системі компанії.
	Помірний	Випадкові або навмисні зміни можуть завдати значної шкоди особистому життю або інформаційній системі компанії.
	Низький	Випадкові або навмисні зміни матимуть незначний вплив на особисте життя або інформаційну систему компанії.
Доступність	Високий	Переривання обслуговування може призвести до фатального пошкодження інформаційної системи компанії.
	Помірний	Переривання обслуговування може призвести до значного пошкодження інформаційної системи компанії.
	Низький	Переривання обслуговування завдасть незначної шкоди інформаційній системі компанії.
Внесок активів	Високий	Актив необхідний для послуг інформаційної системи компанії.
	Помірний	Актив частково потрібний для обслуговування інформаційної системи компанії.
	Низький	Актив відіграє допоміжну роль у послугах інформаційної системи компанії.

Таблиця 3

Класифікація вартості активів

Шкала важливості	Сумарна оцінка	Опис
1	4-5	Може завдати шкоди активам, однак майже не впливає на інформаційну систему компанії.
2	6-7	Пошкоджений актив незначно впливає на пов'язаний домен або систему.
3	8-9	Пошкодження активів призводить до значних втрат для бізнесу.
4	10-11	Пошкодження активів призводить до дуже значних втрат для бізнесу.
5	12	Пошкодження активів призводять до великих втрат для бізнесу, який може перестати функціонувати.

2. Оцінка ймовірності виникнення внутрішніх та зовнішніх атак на інформаційну систему компанії (див. табл. 4).

Таблиця 4

Критерії оцінки ймовірності виникнення атаки

Розподіл	Низький	Помірний	Високий
	1	2	3
Ймовірність виникнення атаки	1-50%	51-80%	81-100%

3. Оцінка ймовірності успіху внутрішніх та зовнішніх атак на інформаційну систему компанії (див. табл. 5 – 7).

Таблиця 5

Оцінки різних аспектів потенціалу атаки

Фактор	Рівень	Значення
Витрачений час	≤ 1 день	0
	≤ 1 тиждень	1
	≤ 1 місяць	4
	≤ 3 місяці	10
	≤ 6 місяців	17
	>6 місяців	19
	недоцільно	∞
Експертиза	Непрофесіонал	0
	Досвідчений	3
	Експерт	6
	Численні експерти	8
Знання системи	Відкритий	0
	Обмежений	3
	Секретний	7
	Критичний	11
Можливість доступу	Непотрібний/необмежений	0
	Легкий	1
	Помірний	4
	Важкий	10
	Відсутній	∞
Обладнання	Стандартний	0
	Спеціалізований	4
	Індивідуальний	7
	Ряд індивідуальних	9

Таблиця 6

Оцінки ймовірності успіху атаки

Значення	**Потенціал атаки, необхідний для виявлення та використання сценарію атаки**	**Ймовірність успіху атаки**
0-9	Базовий	5
10-13	Розширений базовий	4
14-19	Помірний	3
20-24	Високий	2
≥ 25	За межами високого	1

Таблиця 7

Приклади оцінок ймовірності успіху атаки

Атака	**Витрачений час**	**Експертиза**	**Знання системи**	**Можливість доступу**	**Обладнання**	**Потрібний потенціал атаки**	
						Сума	Оцінка
Витік інформації про клієнта з пристрою	0	6	7	4	4	21	Високий
Підробка шляхом прослуховування телефонних розмов та спуфінг	0	3	0	4	4	11	Помірний
MITM-атаки з використанням шахрайської точки доступу	0	6	3	10	4	23	Високий
Підбір інформації	0	0	0	4	4	8	Базовий

4. Вибір пріоритетної мети для забезпечення безпеки інформаційної системи компанії (див. табл. 8 та 9).

Таблиця 8

Оцінки значення ризику

Значення	**Рівень**
1-12	Низький
13-32	Помірний
≥33	Високий

Таблиця 9

Оцінки значення ризику

Актив		**Вартість активу**	**Проблема**	**Ймовірність виникнення атаки AOP)**	**Ймовірність успіху атаки (ASP)**	**Значення ризику (RV)**	
Пристрій	RTOS	5	Витік інформації про користувачів	1	2	10	H
	GPOS	5	Ненадійний пароль	2	5	50	B
	Шлюз	5	Критична інформація, що передається через помилки в роботі пристрою	3	4	60	B
		5	Збитки через неправильне поводження з пристроєм	2	5	50	B

Продовження табл. 9

		5	Доступ до внутрішньої системи та розкриття важливої нформації через вразливість застосунків пристрою	2	4	40	В
		5	Пристрій: передача відкритого тексту між внутрішньою системою	3	5	75	В
		5	Пристрій: передача відкритого тексту між інформаційною системою компанії	3	5	75	В
		5	Пристрій: MITM-атаки між інформаційною системою компанії	3	1	15	П
		5	Шлюз: передача відкритого тексту між внутрішньою системою	3	3	27	П
		5	Витік інформації через зараження шкідливе ПЗ	1	2	10	Н
		5	Розкриття важливої інформації шляхом зламування шлюзу	2	1	10	Н
		5	MITM-атаки з використанням шахрайського шлюзу	2	1	10	Н
		5	Значний витік інформації з втраченого/викраденого шлюзового пристрою	2	3	30	П
ПК	ПК	4	Підробка шляхом прослуховування телефонних розмов та спуфінгу	3	5	60	В
		4	Несанкціонований доступ через MITM-атаки	2	3	24	П
		4	Шлюз: передача відкритого тексту між інформаційною системою компанії	3	5	60	В
		4	MITM-атаки з використанням шахрайської точки доступу	2	1	8	Н
		4	Витік інформації через зараження шкідливим ПЗ	1	2	8	Н
		4	Розкриття важливої інформації через злам шлюзу	1	1	4	Н
		5	Доступ до внутрішньої системи, що використовується незатвердженим пристроєм	1	1	5	Н
		5	Витік інформації з пристрою через зараження шкідливим ПЗ	1	1	5	Н
		5	Збереження важливої інформації у пристрої	2	4	40	В
		5	Витік важливої інформації з втраченого/викраденого пристрою	2	4	40	В

Закінчення табл. 9

		4	Внутрішній доступ до національних мереж зв'язку шляхом засобів фізичного захисту	1	1	4	Н
		4	Внутрішній доступ до національних мереж зв'язку шляхом використання вразливості бездротової мережі	1	1	4	Н
		4	Залишення робочого місця на тривалий час після входу в систему	2	5	40	В
		4	Збій безвідмовності через відсутність збереження записів, до яких здійснюється доступ	1	5	20	П
		4	Аварія через помилки в роботі інформаційної системи компанії	1	5	20	П
ПЗ	ПЗ для передачі даних	3	Доступ до внутрішньої системи та розкриття важливої інформації шляхом експлуатації вразливості програми, що використовується	1	1	3	Н
	ПЗ для моніторингу	2	Доступ до внутрішньої системи через файли оновлень для ПЗ	2	1	4	Н
Інформація	Особиста інформація	4	Підбір	3	3	36	В

Вартість активів

Національний інститут стандартів та технологій США (NIST) розробив концепцію управління ризиками: Risk Management Framework for Information Systems and Organizations для захисту комп'ютерних мереж від кібератак [2]. Керівні принципи NIST-RMF поділяють дії з управління ризиками на наступні етапи життєвого циклу: 1) підготовка організації до впровадження концепції RMF. 2) категоріювання інформації та інформаційних систем; 2) вибір (на основі таких факторів, як мінімальні вимоги безпеки та аналіз витрат) заходів захисту; 3) впровадження заходів безпеки); 4) оцінювання безпеки; 5) авторизація безпеки; 6) постійний моніторинг безпеки. Зазначені елементи концепції RMF запропоновані і гармонійно відповідають моделі побудови системи управління інформаційною безпекою організації: ПВПД (плануй, виконуй, перевіряй, дій), яка визначена у стандарті ISO/IEC 27005 [6], і яка, у свою чергу, є частино системи управління організацією. Публікація FIPS PUB 199 [9] визначає критерії категоризації інформації та безпеки інформаційних систем (на основі потенційного впливу системи). FIPS PUB 199 встановлює три цілі безпеки (конфіденційність, цілісність та доступність) та визначає рівні потенційного впливу порушень безпеки на окремих осіб та організації як низький, помірний та високий. При категоризації загальна вартість кожного активу (рис. 6), що підлягає захисту, розраховується наступним чином:

$$AV_a = \sum_{i=1}^{n} A_i\,, \tag{1}$$

де AV_a – сума значень активів (3–12) активу a, розрахована як сума коефіцієнтів, пов'язаних із значеннями активів (1–3: вклад конфіденційності, цілісності та доступності).

У табл. 1 наведено критерії оцінки вартості активів. Вартість активів кожного з чотирьох елементів (цілей безпеки) оцінюється за трибальною шкалою. Загальна оцінка вартості активів розраховується шляхом додавання всіх індивідуальних оцінок, а клас вартості активів

визначається на основі обчисленого результату. Вартість активів оцінюється по відношенню до кожної з цілей безпеки за допомогою трьох рівнів, що відповідають потенційним наслідкам кожної мети безпеки, як описано в табл. 2, і варіюються від 3 до 12. Підставляючи розраховане значення рівняння (1) можна отримати ступінь важливості активу, залежну від вартості активу, яка варіюється від 1 до 5.

У табл. 3 представлені визначення кожного зі ступенів важливості активів, класифікованих вище. Оцінені вартості активів аналізуються з використанням положень, визначених у ISO/IEC 27005 [6] та ISO 31000 RM [10] та перевіряються з використанням методу оцінки ризику, заснованого на урахуванні конфіденційності, цілісності та доступності, відповідно до NIST 800–37 RMF, FIPS PUB 199, виду відмови, наслідків загроз та аналізу критичності активу.

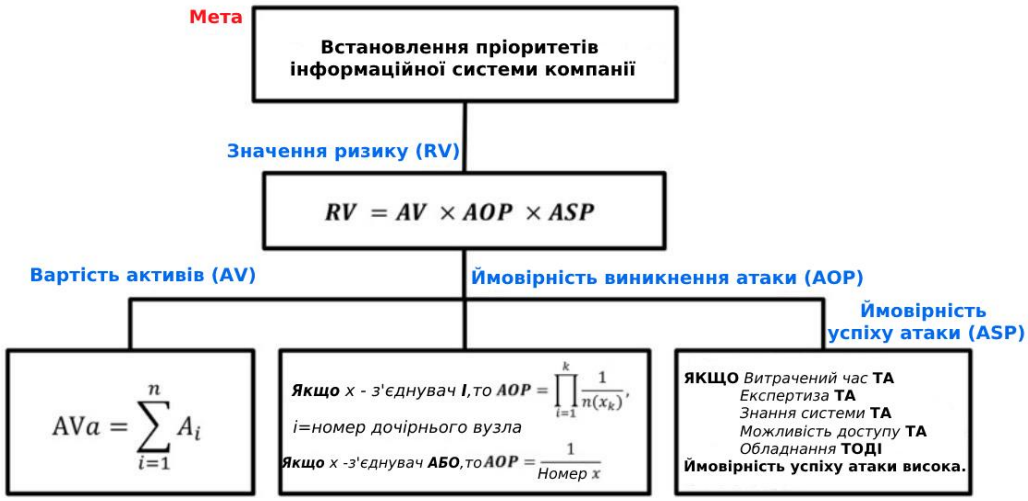


Рис. 6. Етапи оцінки ризиків інформаційної системи компанії

Ймовірність виникнення атаки

Ймовірність виникнення атаки (AOP – Attack occurrence probability) визначається як відношення кількості подій атаки всіх вузлів до кількості дочірніх вузлів атаки, пов'язаних із кореневим вузлом із ціллю досягнення мети атаки кореневого вузла. Нехай один з вузлів – X буде кінцевим вузлом, тоді AOP = 1 (див. рівняння (2), (3)).

$$\text{Якщо } x - \text{з}'\text{єднувальний елемент I, то } AOP = \prod_{i=1}^{k} \frac{1}{n(x_k)}, \quad i = \text{номер вузла}. \tag{2}$$

$$\text{Якщо } x - \text{з}'\text{єднувальний елемент АБО, то } AOP = \frac{1}{\text{Номер } x}. \tag{3}$$

Однак у цьому випадку дерево атак має два основних обмеження. По-перше, вузлам не привласнюється вага, хоча кожен вузол має різний рівень ризику та його потенційна загроза може призвести до різного ступеня збитків. По-друге, замість порівняння ймовірностей появи вузлів вказується лише ймовірність досягнення мети верхнього вузла без урахування частоти появи вузла та рівня ризику кожного вузла, що ускладнює кількісну оцінку вразливостей загроз для безпеки пристроїв. Ймовірність виникнення атаки розраховується шляхом розробки дерева атак для кожного сценарію загроз безпеки відповідно до сімох областей загроз безпеки, як показано на рис. 7. Ймовірність виникнення атаки для прикладу на рис. 7 можна розрахувати в такий спосіб. Оскільки для досягнення v_4 можна вибрати v_8 або v_9, v_2 має ймовірність виникнення атаки 1/2. Крім того, оскільки для досягнення v_4 необхідно вибрати один з методів, представлених v_4, v_5, v_6 і v_7, його ймовірність виникнення атаки становить 1/4. Оскільки для досягнення v_1 обрано єдиний вузол v_3, його ймовірність виникнення

атаки дорівнює 1. Отже, якщо метою атаки є користувач, ймовірність виникнення атаки для витоку інформації про користувача становить 6,25%, як показано нижче:

$$AOP = \frac{1}{2} \times \frac{1}{4} \times \frac{1}{2} = \frac{1}{16} \times 100. \quad (4)$$

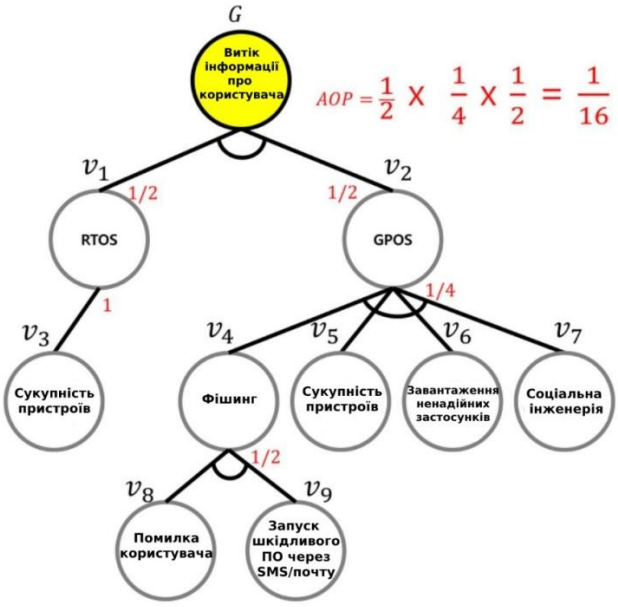


Рис. 7. Приклад дерева атак сценарію загроз безпеки для користувача

Після побудови дерева атак для кожної із семи областей загроз безпеки розраховується ймовірність виникнення атаки кожного дерева атак і, відповідно, кожній області надається оцінка. Оцінка надається кожній області на основі трибальної шкали відповідно до значення ймовірність виникнення атаки, розрахованого за рівнянням (4) та відповідно до критеріїв оцінки (табл. 4).

Ймовірність успіху атаки

Ймовірність успіху атаки (ASP–Attack success probability), визначена у ISO/IEC 15408 [11] та ISO/IEC 18045 [12], і оцінюється на основі наступних факторів [12]:

- Час, що витрачається зловмисником на виявлення вразливості, розробку методу атаки та проведення атаки;
- Необхідні спеціальні експертні знання;
- Знання досліджуваної системи;
- Можливість доступу до мети атаки;
- IT-апаратне/програмне забезпечення або інше обладнання, необхідне для виявлення та використання вразливості.

Ці фактори, що впливають на ймовірність успіху атаки, не є незалежними, а скоріше взаємозамінні з різних точок зору. Наприклад, необхідні знання та обладнання можуть бути замінені витраченим часом (див. табл. 5).

Ймовірність успіху атаки розраховується шляхом застосування значення коефіцієнта (табл. 5) відповідно до сценарію атаки для семи областей загроз безпеки. Потім надається оцінка на основі значення потенціалу атаки (див. таблицю 6), а категоризація виконується на основі рівня потенціалу атаки (див. табл. 7). Для розрахунку ймовірності успіху атаки кожної загрози безпеці рівні ймовірності успіху атаки порівнюються з кінцевими вузлами дерева атак. Наприклад, кожен вузол на рис. 7 відображається на призначеному йому рівні ймовірності успіху атаки відповідно до оцінок ймовірності успіху атаки (див. табл. 7).

Розрахунок значення ризиків

Значення ризику (RV – Risk value) є добутком вартості активів (AV – Asset value), ймовірності виникнення атаки (AOP – Attack occurrence probability) та ймовірності успіху атаки (ASP – Attack success probability):

$$RV = AV \times AOP \times ASP\ . \tag{5}$$

Розраховані значення ризиків оцінюються на трьох рівнях: низькому, помірному та високому (див. табл. 8). При інтерпретації результатів оцінки ризику чим вище вартість активів, ймовірність виникнення атаки і ймовірність успіху атаки, тим вище значення ризику.

Результати аналізу ризиків інформаційної системи компанії відображають рівні ризику загроз безпеці і можуть бути інтерпретовані з погляду відносного ефекту даної атаки. Необхідно встановити відповідні рекомендації щодо безпеки на основі вартості активів кожної загрози з урахуванням її ймовірності виникнення атаки та ймовірності успіху атаки (див. табл. 10).

Таблиця 10

Результати аналізу ризиків

RV = AV × AOP × ASP						
Вартість активів (AV)	Ймовірність виникнення атаки (AOP)	Ймовірність успіху атаки(ASP)				
		За межами високої	Помірна	Висока	Розширена базова	Базова
Оцінка 5	Низька	5	10	15	20	25
	Помірна	10	20	30	40	50
	Висока	15	30	45	60	75
Оцінка 4	Низька	4	8	12	16	20
	Помірна	8	16	24	32	40
	Висока	12	24	36	48	60
Оцінка 3	Низька	3	6	9	12	15
	Помірна	6	12	18	24	30
	Висока	9	18	27	36	45
Оцінка 2	Низька	2	4	6	8	10
	Помірна	4	8	12	16	20
	Висока	6	12	18	24	30
Оцінка 1	Низька	1	2	3	4	5
	Помірна	2	4	6	8	10
	Висока	3	6	9	12	15

Висновки

1. Метод «дерева атак» є систематичним методом визначення характеристик безпеки системи на основі всіх атак, яким піддається інформаційна система. Виявлення всіх можливих атак полегшує аналіз можливих шляхів реалізації кібератак та вибір адекватних контрзаходів і їх оптимальне використання.

2. Щоб виявити загрози, що можуть бути використані для побудови дерева атак інформаційної системи компанії, доцільно обрати типові та засновані на відповідних сценаріях загрози безпеки відповідно до ISO/IEC 27005, а щоб визначити вразливості інформаційної системи компанії, доцільно структурувати враховані загрози та зробити їх придатними для середовища інформаційної системи компанії також відповідно до ISO/IEC 27005.

3. Основними варіантами загроз безпеки інформаційної системи є: користувач; пристрої; домашня мережа (мережа філіалу компанії); шлюз, наприклад, VPN; інтернет (загальнодоступна мережа); сервер центрального офісу компанії; загрози безпеки, пов'язані з MITM-атаками, шкідливим кодом, підробкою/зміною застосунків та незаконним доступом до KoreaNet, оминаючи наявні перевірки фізичної безпеки.

4. Запропонована концепція припускає визначення: областей загроз безпеки інформаційної системи; задіяних інформаційних активів та розрахунок їхньої вартості; оцінку ймовірності виникнення атак на інформаційну систему; оцінку ймовірності успіху атак на інформаційну систему та інше.

5. Основна перевага метода «дерева атак» в тому, що він дозволяє спеціалістам з захисту ідентифікувати потенційні атаки та впроваджувати відповідні контрзаходи. Недоліки цього підходу полягають у тому, що при його впровадженні важко врахувати всі дії і, при цьому, відсутня можливість для моделювання атак, що включають одночасні дії зловмисників.

6. Обґрунтовані методи оцінки ризику, включаючи урахування ймовірності успіху атаки та ймовірності виникнення атаки, дозволяють усунути зазначені недоліки та забезпечити більш точну ідентифікацію методів атаки, пов'язаних із поведінкою зловмисника.

7. Концепція оцінки ризиків кібербезпеки і методика аналізу та оцінки загроз безпеки, які використані, відповідають підходам до побудови ризикоорієнтованих систем управління інформаційною безпекою і можуть стати основою для розробки системи безпеки інформації в інформаційній системі об’єкта критичної інфраструктури.

Список літератури:

1. Schneier B. Attack trees. Dr Dobbs J. 1999;24:21–29. doi: 10.1002/9781119183631.ch21. [CrossRef] [Google Scholar]
2. NIST SP800–37 Rev. 2. Risk Management Framework for Information Systems and Organizations, 2018.
3. Потій О.В., Горбенко І.Д., Замула О.А., Ісірова К.В. Аналіз методів оцінки і управління ризиками кібер і інформаційної безпеки // Радіотехніка. 2021. Вип. 206. С. 5-23.
4. Maji A, Mukhoty A, Majumdar A, Mukhopadhyay J, Sural S, Paul S, et al. Security analysis and implementation of web-based telemedicine services with a four-tier architecture // Proceedings of the Second International Conference on Pervasive Computing Technologies for Healthcare. Tampere; 2008. p. 46–54. 10.4108/icst.pervasivehealth2008.2518.
5. She H, Lu Z, Jantsch A, Zheng LR, Zhou D. A network-based system architecture for remote medical applications. Asia-Pac Adv Netw. 2007;1:27–31. [Google Scholar].
6. International Organization for Standardization. Information security risk management. (second edition). ISO/IEC 27005:2011. 2011. [Google Scholar].
7. International Organization for Standardization . Health informatics – Information security management in health using ISO/IEC 27002. ISO/DIS 27799:2014(E) 2015. [Google Scholar].
8. Camara C., Peris-Lopez P., Tapiador JE. Security and privacy issues in implantable medical devices: a comprehensive survey. J Biomed Inf. 2015;55:272–289. doi: 10.1016/j.jbi.2015.04.007. [PubMed] [CrossRef] [Google Scholar].
9. Stine KM, Kissel RL, Barker WC, Lee A, Fahlsing J, Gulick J. Guide for mapping types of information and information systems to security categories. NIST SP800–64 Rev. 4. 2008. [Google Scholar].
10. International Organization for Standardization. Risk management. ISO 31000:2018. 2018. [Google Scholar].
11. International Organization for Standardization. Information technology – Security techniques – Evaluation criteria for IT security Part 1: Introduction and general model. ISO/IEC 15408–1:2009. 2009. [Google Scholar].
12. International Organization for Standardization. Refining software vulnerability analysis under ISO/IEC 15408 and ISO/IEC 18045. ISO/IEC 18045. 2015. [Google Scholar].

Надійшла до редколегії 22.05.2022

Відомості про авторів:

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

Замула Олександр Андрійович – д-р техн. наук, професор, професор кафедри безпеки інформаційних систем і технологій, факультет комп’ютерних наук, Харківський національний університет імені В.Н. Каразіна, Україна; e-mail: zamylaaa@gmail.com, ORCID: http://orcid.org/0000-0002-8973-6190

Осипенко Юлія Сергіївна – магістрант кафедри безпеки інформаційних систем і технологій, факультет комп’ютерних наук, Харківський національний університет імені В.Н. Каразіна, Україна; e-mail: julie.osipenko17@gmail.com

УДК 004.056 **DOI:10.30837/rt.2022.2.209.13**

В.І. ЮХИМЕНКО, О.І. ФЕДЮШИН, канд. техн. наук

АНАЛІЗ МАСШТАБУВАННЯ БЛОКЧЕЙН ПРОЄКТУ TELEGRAM OPEN NETWORK

Актуальність теми та постановка завдання

Блокчейн, також відомий як технологія розподіленої книги (DLT), було визнано проривною технологією в різних галузях, не тільки в криптовалютах, а ще і в фінансах, Internet of Things, охороні здоров'я, енергетиці та логістиці. У порівнянні з традиційними централізованими рішеннями блокчейн має ряд значних переваг, таких як незмінність, підвищена безпека, відмовостійкість та прозорість.

Однак децентралізована природа блокчейну різко обмежує його продуктивність (наприклад, пропускну здатність і затримку). Так, Bitcoin [1] може досягти лише низької пропускної здатності сім транзакцій в секунду (TPS), а для створення нового блоку з транзакціями потрібно близько 10 хвилин. На відміну від нього, поточні централізовані платіжні системи, такі як VisaNet і MasterCard, можуть охоплювати тисячі TPS і здійснювати платежі майже в реальному часі.

Використовуючи подібний алгоритм консенсусу, Proof-of-Work (PoW), інші блокчейн платформи, такі як Ethereum [2] і Litecoin, також успадковують недоліки продуктивності Bitcoin.

Без сумніву, проблема продуктивності стала основною перешкодою для застосування рішень на базі блокчейну у системах з великою кількістю активних користувачів. Це особливо актуально для систем, які потребують високої продуктивності, таких як онлайн-обробка транзакцій і платіжні системи в режимі реального часу.

Щоб подолати цю проблему, розробники блокчейн систем докладають зусиль, щоб покращити свою продуктивність, наприклад, змінюючи структуру системи та розробляючи нові алгоритми консенсусу. Для вирішення цієї проблеми запропоновано багато методів, таких як використання side-chain, off-chain та орієнтованих ациклічних графів [3 – 6]. Однак вони мають притаманні накладні витрати, такі як, наприклад, утворення "паразитних" ланцюжків. Шардинг став хорошим кандидатом на рішення, оскільки є стандартним рішенням для горизонтального масштабування у традиційних базах даних, то ж може бути застосованим для розподілення консенсусного навантаження та транзакцій для прискорення часу обробки транзакції та створення нового блоку[7 – 12].

Цікавим та інноваційним блокчейн проєктом є Telegram Open Network (TON) [13]. Розпочавши розробку системи у 2017 р., команда Павла Дурова та його брата, швидко привернула увагу інвесторів та криптоспільноти, заявивши, що їхня система вирішує проблеми масштабування блокчейну за допомогою шардингу, і при цьому система масштабується динамічно залежно від поточного навантаження на систему.

Мета роботи – зробити огляд блокчейн проєкту Telegram Open Network, а саме TON Blockchain, та проаналізувати безпеку, надійність та масштабування цієї системи.

TON Blockchain

У цій частині наведено опис основного компоненту екосистеми Telegram Open Network – TON Blockchain, а також стислий опис механізму динамічного шардування та консенсусної мережі.

Telegram Open Network (скор. TON) – базована на блокчейні децентралізована комп'ютерна мережа, а також проєкт захищеної вбудованим проксі та анонімайзером даркнет-платформи, побудованої на принципі оверлейної P2P-мережі, що має послуги обміну повідомленнями, платіжних операцій у криптовалюті Gram, зберігання даних, а також операційна система для розподілених програм.

Концепція TON розроблена братами Дуровими [1], які залучили під цей проєкт інвестиції у кілька мільярдів доларів та запланували переведення на TON свого популярного месенджера Telegram.

На думку рецензентів, TON, з одного боку, приваблює інвесторів ідеєю популярної криптовалюти, а з іншого – дозволяє користувачам у країнах із сильною Інтернет-цензурою вільно використовувати інформаційні ресурси, оминаючи державні системи блокування та відстеження.

30 травня 2019 р. Telegram представив спрощену версію платформи.

7 травня 2020 р., у зв'язку з відмовою команди TON від запуску проєкту після тривалих судових розглядів з комісією з цінних паперів та бірж США, на базі протоколу TON був запущений блокчейн-проєкт Everscale [14] (також відомий як Free TON).

12 травня 2020 р. Павло Дуров у своєму Telegram-каналі оголосив, що закрив блокчейн-проєкт TON.

29 червня 2021 р. Павло Дуров передав домен ton.org та GitHub-репозиторій незалежному співтовариству розробників The Open Network (TON).

TON Blockchain – це умовна назва децентралізованої мережі (сукупності ланцюжків блоків) або 2D-блокчейн, що складається з трьох основних типів блокчейнів:

- Master blockchain або Masterchain – єдиний у своєму роді ланцюжок блоків, що містить загальну інформацію про протокол і поточні значення його параметрів, набір валідаторів та їх часток, набір активних на даний момент workchains та їх «шардів» – shardchains, а також набір хешів останніх блоків workchains та shardchains .
- Working blockchains або Workchains – безліч (до 2^{32}) блокчейнів, які є «робочими волами», що містять транзакції з інформацією про переміщення активів та смарт-контракти. При цьому окремі workchains можуть мати власні «правила», формати адрес акаунтів, формати транзакцій, різні віртуальні машини для смарт контрактів, різні базові токени або криптовалюти і т.д. Але всі вони повинні відповідати деяким основним критеріям функціональної сумісності для забезпечення простої взаємодії між собою. Таким чином, TON Blockchain по суті є гетерогенним, також як блокчейни EOS та Polkadot.
- Shard blockchains або Shardchains – підмножина блокчейнів (до 2^{60}) всередині безлічі workchains, що забезпечує роботу системи шардингу і має ті самі правила та формат блоків, що й у workchains. Shardchains містять лише підмножину облікових записів, в залежності від декількох перших (найбільш значущих) бітів адреси кожного конкретного облікового запису. Оскільки всі shardchains мають загальний формат і правила побудови блоків, TON Blockchain у цьому відношенні є гомогенним і відповідає вимогам, описаним в одній з пропозицій з масштабування блокчейн системи Ethereum.

Кожен блок shardchain (так само як і masterchain) насправді не просто блок, а невеликий блокчейн. Як правило, цей «вертикальний блокчейн» складається рівно з одного блоку; таким чином, його можна вважати просто блоком відповідного йому «традиційного» блокчейна (або «горизонтального блокчейна»). Однак, якщо виникає необхідність у виправленні некоректних блоків, то в «вертикальний блокчейн» додається новий блок, який містить або заміну діючого «горизонтального» блоку, або «різницю блоків», що містить тільки опис тих частин попередньої версії блоку, які потребують заміни. Цей специфічний для TON механізм заміни виявлених некоректних блоків без необхідності hardfork отримав назву 2D-блокчейн, або просто 2-блокчейн (рис. 1). Ідея шардингу полягає в тому, щоб розділити базу даних (або розподілену базу даних, тобто блокчейн) на кілька незалежних дійсних частин – шарди (англ. “shards” – сегмент). Таким чином, база даних в першу чергу розбивається на рядки, а не на стовпці.

У результаті кожен шард складається з усіх необхідних даних. Шардинг може здійснюватися відповідно до попередньо визначеної структури або динамічно, коли транзакції можуть ініціювати роздвоєння або злиття шардів. Розробники TON пропонують динамічний шардинг на основі Infinite Sharding Paradigm (парадигма нескінченного шардингу).

Згідно з цією парадигмою кожен workchain складається з множини (розміром $2^{(0..M)}$, де M=60) shardchains, і підтримує динамічне шардування.

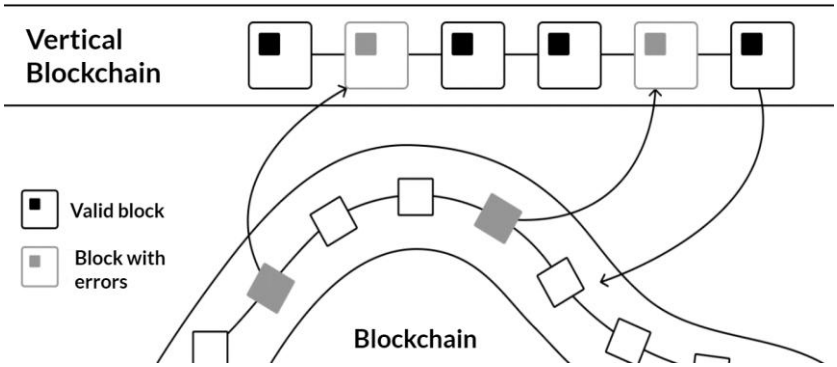


Рис. 1. Умовна схема роботи 2D-блокчейну

Кожен shardchain відповідає за підмножину облікових записів, що визначається за бітовим префіксом accound_id. Всі shardchains мають однаковий формат блоку та правила. Кожен shardchain ідентифікується shard_prefix – бітова послідовність довжиною від 0 до M. Цей префікс буде використовуватись для визначення підмножини облікових записів, що належать до даного шардчейну. Простими словами, будь-який обліковий запис, у якого бітове уявлення account_id починається з shard_prefix, вважається, що належить до даного шардчейну.

Спочатку, workchain складається тільки з одного shardchain, який відповідає за всю множину акаунтів. При цьому сценарії наш блокчейн мало відрізняється від “звичайного” одновимірного.

Але, як тільки кількість транзакцій в одному блоці помітно зростає, то наш шард розділяється (split) на два окремі shardchain, що розділяють між собою всю безліч акаунтів навпіл. При цьому перші блоки "нових" гілок ланцюжка будуть вказувати на останній блок початкового chardchain.

Аналогічно, якщо сумарне навантаження (кількість транзакцій у нових блоках) на два сусідні shardchains суттєво впало, то система може їх об'єднати (merge) в один. При цьому перший блок об'єднаного shardchain зберігатиме хеші останніх блоків з двох початкових шардів.

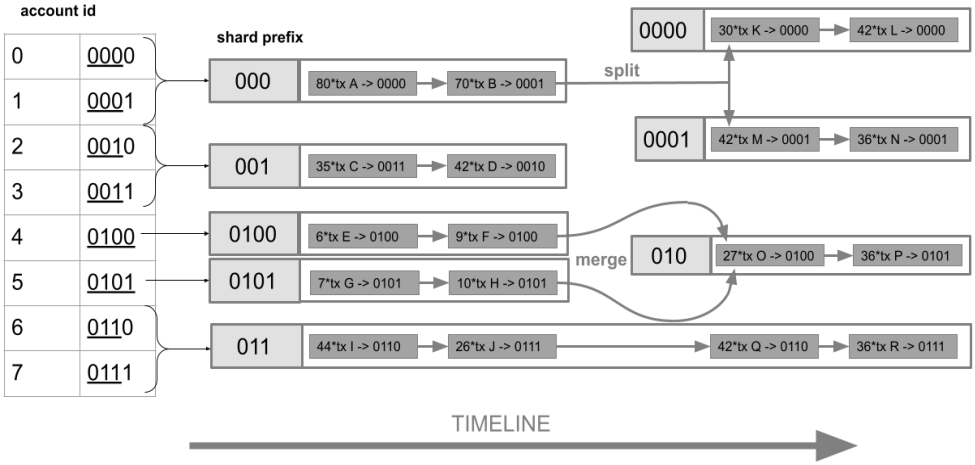


Рис. 2. Приклад split/merge операцій залежно від кількості транзакцій у блоках

Теоретично, workchain може прийти в такий стан, що на кожен обліковий запис виділено один shardchain, що містить історію змін тільки для одного облікового запису. Тож можемо вважати, що один workchain підтримує 2^M унікальних облікових записів (рис. 3).

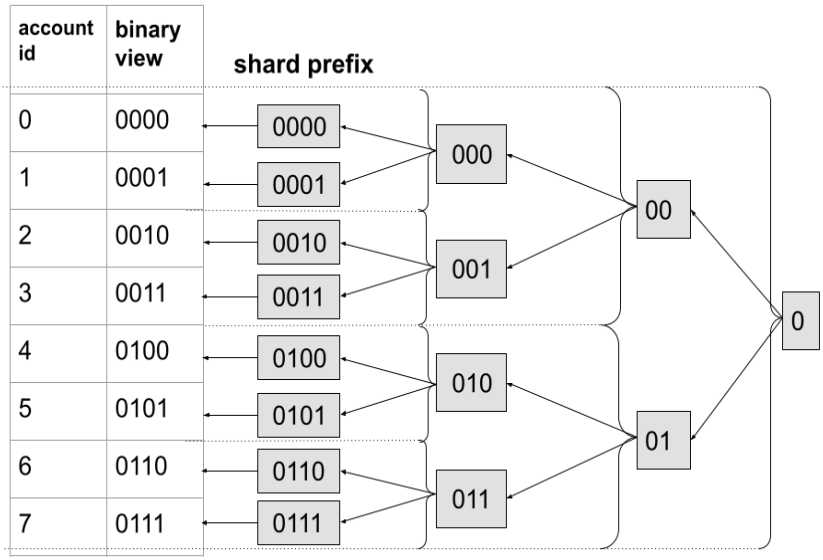


Рис. 3. Схематичний приклад максимального розшардування для M=3

Коли shardchain відповідає тільки за один аккаунт, то його називають account shard. Базуючись на інформації вище, можна скласти "ієрархію" блокчейнів у TON Blockchain (рис. 4).

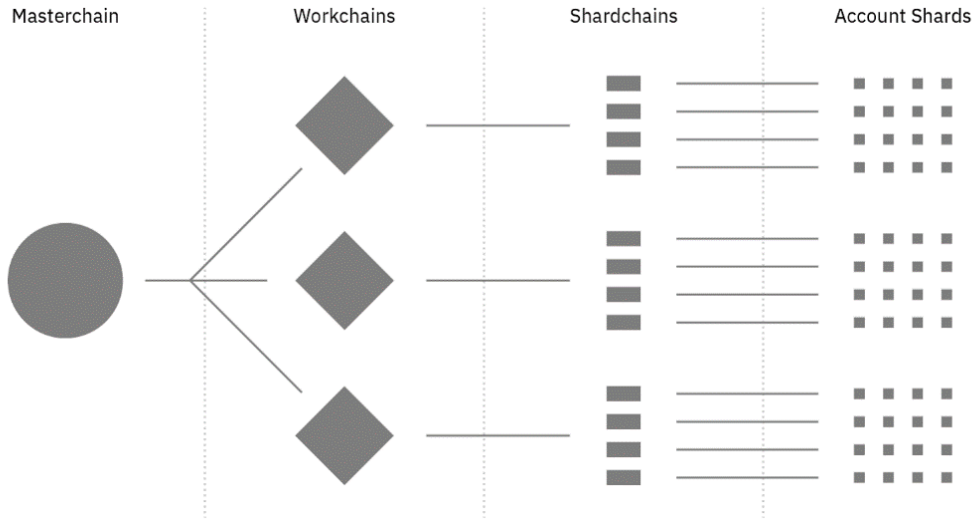


Рис. 4. Зв'язок між блокчейнами TON

Усі згадані елементи доповнюються та вкорінюються в механізм консенсусу. Механізм, який має підтримувати масштабування та, оскільки механізми синхронного консенсусу вимагають тимчасових запасів надійності, уповільнення угоди стану системи, повинен бути асинхронним. З цієї причини має бути розгорнутий асинхронний варіант Proof of Stake (PoS). У технічній документації TON [13] викладено процес прийняття рішення, що стоїть за вибором, і порівнюється делегований PoS з обраною Візантійською версією PoS з відмовос-

тійкістю (BFT). На жаль, у технічних документах бракує детального опису фактичної реалізації цього алгоритму.

Консенсусна мережа TON Blockchain складається з різних типів вузлів: валідатори, номінатори, фішери та коллатори (рис. 5).

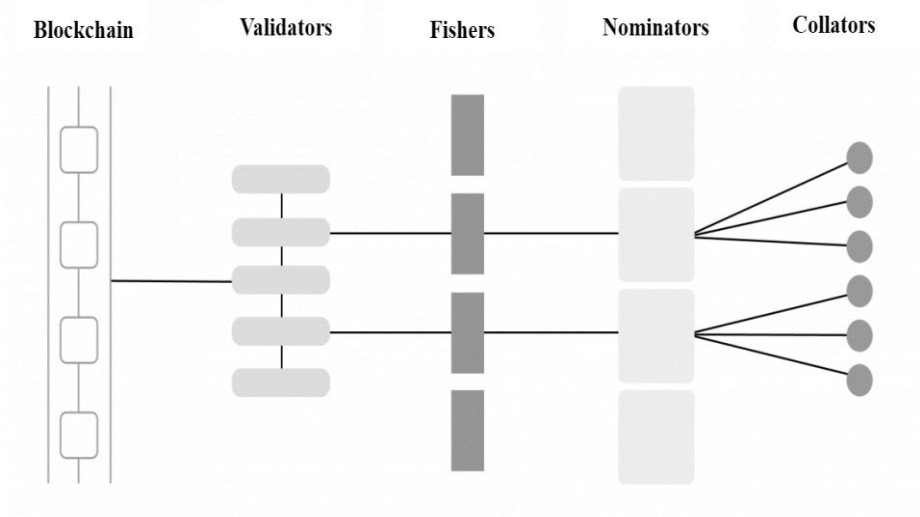


Рис. 5. Консенсусна мережа TON Blockchain

Валідаторами є вузли PoS та виробники блоків. Фішери стежать за консенсус-мережею з метою знайти помилку або виявити ймовірно зловмисний вузол консенсусу і у випадку, якщо фішер однозначно підтвердить, що вузол є таким, він отримує винагороду у вигляді конфіскації частини частки (stake) цього валідатора.

Завдання колаторів – підготовка блоків шардчейна та надання їх на валідацію PoS-вузлам, за що вони отримують свою частину винагороди за створення блоку. При цьому колатори є, по суті, додатковими учасниками консенсусу, оскільки валідатори майже завжди генерують блоки самостійно.

Номінатори надають свої активи (токени workchain) валідаторам у позику з метою отримання прибутку. Фактично, номінатори не входять до інфраструктури валідаторів, а лише поділяють свою велику початкову частку активу між ними в обмін на пропорційний відсоток від загальної винагороди. Таким чином, схема та розмір винагороди, яку отримують номінатори, повністю залежить від результатів роботи валідаторів, при цьому номінатори «голосують» за валідаторів, надаючи їм у позику свої токени. У ролі номінаторів можуть виступати як індивідуальні власники токенів, так і пули (pools), що управляють засобами окремих користувачів TON і одночасно виступають у ролі валідаторів, діючи як делегати за допомогою смарт-контракту TON. При цьому сумарна винагорода такого пулу розподіляється між його учасниками пропорційно до їхніх вкладів.

Сам процес генерації нових блоків відбувається наступним чином: деяка певна кількість валідаторів за спеціальним алгоритмом вибирають придатні для валідації блоки masterchain (шарди), потім для кожного такого шарда відбирається менше підмножини валідаторів в порядку, визначеному псевдовипадковим способом з інтервалом приблизно кожні 1024 блоки.

Таким чином, для кожного блоку існує псевдовипадково обраний набір валідаторів для визначення того, чий кандидат у блок має найвищий пріоритет. Валідатори та інші вузли перевіряють достовірність запропонованих кандидатів у блоки. У випадку, якщо валідатор автоматично (не навмисно) підписує недійсного кандидата в блоки, він карається втратою частини або всієї своєї винагороди, або зовсім відстороненням від участі у відборі валідаторів на деякий час.

Далі валідаторам необхідно досягти консенсусу на основі алгоритму BFT. Потім після досягнення консенсусу створюється новий блок, при цьому комісії за транзакції розподіляються між валідаторами.

Необхідно зазначити, що кожен валідатор може бути обраний для участі в кількох підмножинах валідаторів, тому передбачається, що всі алгоритми валідації та консенсусу запущені паралельно.

Після того, як всі нові блоки шардів ланцюга згенеровані або тайм-аут закінчено, з'являється повідомлення про те, що створено новий блок у masterchain, що включає хеші останніх блоків всіх шардів на основі BFT-консенсусу всіх валідаторів.

Аналіз масштабування Telegram Open Network

Як зазначено на початку роботи, основні критерії, за якими оцінюється ефективність масштабування, – це пропускна здатність системи (transactions per second, скорочено TPS) та середній час появи нового блоку в мережі (average block time).

Для аналізу масштабування за критерієм average block time було вирішено порівняти показники найпопулярніших блокчейн платформ (Bitcoin, Ethereum) з реалізаціями TON Blockchain (The Open Network та Everscale).

Як джерело даних було обрано сервіси для аналітики блокчейн систем, такі як: Blockchair, Ever.live, Everscan, Tonscan та Blockchain.com. Основною причиною вибору є те, що ці сервіси надають змогу досліджувати метрики блокчейн систем у реальному часі.

На основі інформації, зібраної за допомогою цих сервісів, була зроблена порівняльна таблиця (табл. 1).

Таблиця 1

Середній час появи нового блоку в мережі

Блокчейн система	Average Block Time, *c*
Bitcoin	600
Ethereum	12-14
The Open Network	3-5 (невідома кількість шардів)
Everscale	0,3 (16 шардів)

За цими даними можна сказати, що застосування динамічного шардування значно прискорює середній час створення блоку. Особливо це видно на прикладі проєкту Everscale – у порівнянні з Bitcoin у 2000 разів швидше створюється новий блок. Однак слід зазначити, що показники для The Open Network є неточними, оскільки вони базувалися на замірах розробників, а інструментів для самостійного аналізу мережі у реальному часі знайти не вдалося. Тож реальний час створення блоку може бути навіть швидшим.

Що стосується показнику transactions per second, то потрібно оцінити два показники: прогнозована пропускна здатність та TPS системи у реальному часі.

За даними Binance Research [15], загальна архітектура TON унікальна і дуже орієнтована на підтримку масштабування. З поставленим завданням підтримки «мільйони транзакцій в секунду» TON не тільки ставить надзвичайно амбітну мету, але, здається, перевершує попит галузі на 1000 порядків. Для порівняння, одна з найбільш завантажених платіжних мереж у світі, Visa, складає в середньому 1700 TPS. Результати їх прогнозу можна побачити на рис. 6.

Однак варто зазначити, що система типу TON має намір масштабувати за запитом і не намагатиметься почати з мільйонів транзакцій. Базуючись на цьому, можна припустити, що при невеликій кількості активних користувачів показники TPS будуть достатньо помірними.

Це припущення було підтверджено у ході порівняння TPS тих самих систем за допомогою сервісів для моніторингу стану блокчейн систем, використаних раніше (табл. 2).

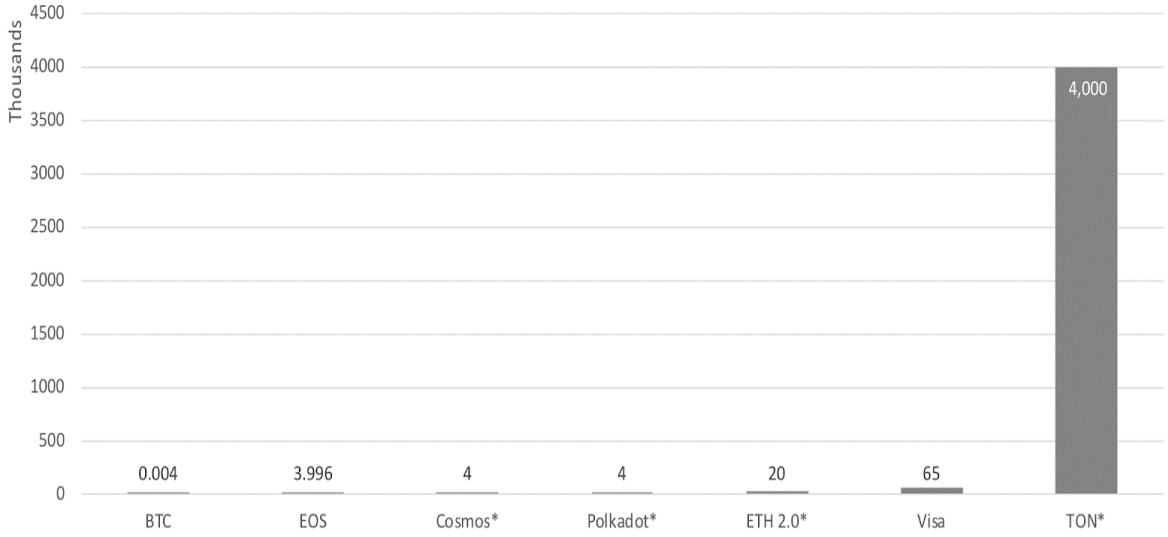


Рис. 6. Прогнозована пропускна здастність у TPS різних баз даних (у тисячах)

Таблиця 2

Реальні метрики систем станом на травень 2022

Блокчейн система	Transactions per second	Total number of transactions in last 24 hours	Total number of transactions
Bitcoin	1,98	247 680	742 642 891
Ethereum	10,21	1 056 240	1 611 997 470
The Open Network	2,02	180 738	218 035 610
Everscale	1,9	189 956	108 965 377

Як ми бачимо, за реальними показниками TPS системи-реалізації протоколу TON поки що поступаються навіть системі Bitcoin. Але варто зазначити загальне навантаження на системи TON та Everscale: кількість транзакцій за останній день та в цілому значно менші ніж у популярних систем. А базуючись на тому, що ці системи масштабуються динамічно, можна припустити, що ці показники TPS є оптимальними для користування при реальному навантаженні, оскільки ці системи ще не набули бажаної популярності у криптоспільноті.

Висновки

1. Зроблений порівняльний аналіз найпопулярніших блокчейн платформ (Bitcoin, Ethereum) з реалізаціями TON Blockchain (The Open Network та Everscale) за трьома показниками: пропускна здатність системи (transactions per second, скорочено TPS), середній час появи нового блоку в мережі (average block time) та прогнозована пропускна здатність у TPS. Для порівняння було використано сервіси аналізу блокчейн систем у реальному часі (так звані blockchain explorers) та відкрите дослідження Binance Research Group [14].

2. У ході порівняння average block time було виявлено, що застосування шардингу значно прискорює середній час появи нового блоку в мережі. Як приклад, система Everscale створює 3-4 блоки за секунду, коли Bitcoin створює один блок у середньому за 10 хвилин.

3. У ході порівняння показників TPS було виявлено, що показники TON та Everscale не є вражаючими. Однак слід зазначити, що ці системи є дуже молодими та не набули бажаної популярності серед користувачів щоб реалізувати свій потенціал у масштабуванні.

4. Базуючись на дослідженні прогнозованої пропускної здатності, можна зробити висновок, що TON та Everscale, здається, перевершують попит галузі на 1000 порядків. Тож, щоб реалізувати їхній потенціал, потрібна багатомільйонна аудиторія активних користувачів. Гарними напрямками для цього є сфера Вільного Інтернету та конкуренція з міжнародними платіжними системами типу MasterCard та Visa.

Список літератури:

1. S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. Working Paper, 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf.
2. V. Buterin. Ethereum Sharding FAQ. Accessed: Jan. 28, 2020. [Online]. Available: https://github.com/ethereum/wiki/wiki/Sharding-FAQ.
3. F. Gai, J. Niu, S. Ali Tabatabaee, C. Feng and M. Jalalzai. Cumulus: A Secure BFT-based Sidechain for Off-chain Scaling // 2021 IEEE/ACM 29th International Symposium on Quality of Service (IWQOS), 2021, pp. 1-6, doi: 10.1109/IWQOS52092.2021.9521363.
4. J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll and E. W. Felten. SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies // 2015 IEEE Symposium on Security and Privacy, 2015, pp. 104-121, doi: 10.1109/SP.2015.14.
5. H. Moudoud, S. Cherkaoui, and L. Khoukhi. An IoT Blockchain Architecture Using Oracles and Smart Contracts: the Use-Case of a Food Supply Chain // IEEE Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), 2019.
6. C. Profentzas, M. Almgren and O. Landsiedel. TinyEVM: Off-Chain Smart Contracts on Low-Power IoT Devices // 2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS), 2020, pp. 507-518, doi: 10.1109/ICDCS47774.2020.00025.
7. Singh, Amritraj & Click, Kelly & Parizi, Reza & Zhang, Qi & Dehghantanha, Ali & Choo, Kim-Kwang Raymond. Sidechain technologies in blockchain networks: An examination and state-of-the-art review // Journal of Network and Computer Applications. 149. 102471. 10.1016/j.jnca.2019.102471.
8. A. Hafid, A. S. Hafid, and M. Samih. A methodology for a probabilistic security analysis of sharding-based blockchain protocols // Proc. Int. Congr. Blockchain Appl. Cham, Switzerland: Springer, 2019, pp. 101–109.
9. L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert, and P. Saxena. A secure sharding protocol for open blockchains // Proc. ACM SIGSAC Conf. Comput. Commun. Secur., Oct. 2016, pp. 17–30.
10. G. Yu, X. Wang, K. Yu, W. Ni, J. A. Zhang, and R. P. Liu. Survey: Sharding in blockchains // IEEE Access, vol. 8, 2020, pp. 14155–14181.
11. C. Huang, Z. Wang, H. Chen, Q. Hu, Q. Zhang, W. Wang, and X. Guan, RepChain: A reputation-based secure, fast and high incentive blockchain system via sharding, 2019, arXiv:1901.05741. [Online]. Available: http://arxiv.org/abs/1901.05741.
12. Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou. A survey of distributed consensus protocols for blockchain networks // IEEE Commun. Surveys Tuts., vol. 22, no. 2, pp. 1432–1465, 2nd Quart., 2020, doi: 10.1109/COMST.2020.2969706.
13. The Open Network / N. Durov. Режим доступу: https://ton.org/ton.pdf. Дата звернення: 24.05.2022.
14. Everscale Whitepaper / Mitja Goroshevsky. Режим доступу: https://everscale.network/docs/everscale-whitepaper.pdf. Дата звернення: 24.05.2022.
15. Exploring Telegram Open Network / Binance Research Group. Режим доступу: https://research.binance.com/en/analysis/telegram-open-network. Дата звернення: 24.05.2022.

Надійшла до редколегії 07.06.2022

Відомості про авторів:

Юхименко Валентин Ігорович – студент 4-го курсу спеціальності 125 Кібербезпека кафедри безпеки інформаційних технологій, Харківський національний університет радіоелектроніки, Україна; e-mail: valentin.yukhymenko@gmail.com; ORCID: http://orcid.org/0000-0002-7191-2969

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

УДК 004.056: 004.056.5 **DOI:10.30837/rt.2022.2.209.14**

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

ДОСЛІДЖЕННЯ ОСНОВНИХ МЕТОДІВ І СХЕМ ШИФРУВАННЯ З МОЖЛИВІСТЮ ПОШУКУ

Вступ

За останнє десятиріччя системи баз даних, що пропонуються у вигляді хмарних сервісів, широко використовуються та демонструють вибухове зростання [1]. Модель бази даних як послуга забезпечує користувачів можливістю створювати, зберігати, модифікувати та отримувати дані з віддаленого джерела, маючи доступ до інтернету. Однак, у міру того, як ми продовжуємо агрегувати дані, ключовою проблемою стає балансування дотримання безпеки та приватності (privacy) даних з їх аналітичним використанням для підтримки прийняття рішень. При переміщенні своїх даних у загальнодоступну хмару користувачі турбуються про їхню безпеку та приватність. А оскільки все більша кількість даних переноситься в хмарні сервіси зберігання, потрібні гарантії безпеки цих даних, у тому числі такі, що передбачаються міжнародними законами та стандартами, такими як: Загальний регламент захисту персональних даних Європейського Союзу (General Data Protection Regulation – GDPR) [2], Стандарт безпеки даних індустрії платіжних карт (PCI DSS) [3], Закон про переносимість і підзвітність медичного страхування (Health Insurance Portability and Accountability Act – HIPAA) [4, 5] та деякими іншими. Це стимулювало дослідження в галузі безпечного управління даними та підвищило їх актуальність [6].

Для безпечного зберігання конфіденційних даних на ненадійному віддаленому сервері останні мають бути зашифровані. Шифрування унеможливлює доступ до даних без ключів як для внутрішніх, так і для сторонніх осіб, але в той же час позбавляє власника даних всіх можливостей пошуку за цією інформацією.

Одним з простих рішень цієї проблеми є завантаження всієї бази даних, з подальшим її локальним розшифруванням і пошуком бажаних результатів отриманих розшифрованих даних. Проте для більшості застосунків такий підхід буде недоцільним.

Інший метод дозволяє серверу розшифровувати дані, виконувати запит на стороні сервера і надсилати користувачеві лише результати. Але в цьому випадку знижується рівень безпеки, оскільки дані, що захищені шифруванням, розкриваються серверу. Тому бажано підтримувати максимально повну функціональність пошуку на стороні з найменшою можливою втратою конфіденційності даних. Зокрема, захищена система пошуку повинна бути спрямована на те, щоб сервер нічого не дізнався про дані, що зберігаються в захищеній базі даних, або про запити, а той, хто запитує (querier) відповідні дані, нічого не дізнався, крім результатів запиту [7].

Одним із таких підходів, відомим із досить великої кількості робіт у світі, є підхід, що спирається на шифрування з можливістю пошуку (searchable encryption – SE). Ця технологія ґрунтується на можливостях сучасних криптографічних методів в умовах поділу ролей надання, адміністрування та доступу до даних. Її завдання – забезпечити необхідну функціональність із прийнятною втратою продуктивності.

Однак, незважаючи на досягнутий прогрес у цій галузі, комплексний підхід до підтримки конфіденційних хмарних обчислень поки що відсутній, і, таким чином, цей напрямок залишається плідною областю досліджень [1].

Основні методи шифрування з можливістю пошуку

Шифрування з можливістю пошуку (SE) – це технологія, яка дозволяє виконувати операції пошуку зашифрованих даних без розкриття будь-якої інформації про те, що шукається. Шифрування з можливістю пошуку діє як метод керування даними, який дозволяє власникам

даних зберігати свої дані та керувати ними на сторонньому, ненадійному віддаленому (у тому числі хмарному) сервері, а також дозволяє користувачеві даних делегувати функції пошуку хмарному серверу для отримання цих даних. Таким чином, шифрування з можливістю пошуку забезпечує безпечне зберігання та отримання даних при оптимізованих витратах. Шифрування з можливістю пошуку застосовується у сценаріях, де потрібна як конфіденційність, так і доступність відповідних даних [8].

Схема SE дозволяє серверу виконувати пошук у зашифрованих даних від імені клієнта без отримання інформації про відкриті дані. Схеми шифрування з можливістю пошуку зазвичай поділяються на два класи. Деякі схеми безпосередньо шифрують дані відкритого тексту спеціальним чином так, що шифртекст може бути запитаний (наприклад, за ключовими словами). Це призводить до того, що час пошуку лінійно залежить від довжини даних, що зберігаються на сервері. Наприклад, використання n документів із w ключовими словами дає складність, лінійну за кількістю ключових слів у документі $O(nw)$, оскільки кожне ключове слово має бути перевірено на відповідність.

В інших схемах для прискорення процесу пошуку в базах даних використовується індекс, що створюється на основі відкритих текстових даних. Введення індексу дозволяє значно знизити складність пошуку та, таким чином, збільшити продуктивність схеми пошуку. Підвищення продуктивності пошуку досягається з допомогою етапу попередньої обробки. Але при цьому слід пам'ятати, що оскільки індекс будується на даних відкритого тексту, створення індексу не завжди можливе і залежить від даних, які необхідно зашифрувати [6].

Основними методами доказово безпечного шифрування з можливістю пошуку є симетричне шифрування з можливістю пошуку (Symmetric Searchable Encryption – SSE) та шифрування з відкритим ключем із пошуком за ключовими словами (Public Key Encryption with Keyword Search – PEKS). Хоча існують і деякі інші, такі як предикативне шифрування (Predicate Encryption – PE), шифрування скалярного/внутрішнього добутку (Inner Product Encryption – IPE), анонімне шифрування на основі ідентичності (Anonymous Identity-Based Encryption – AIBE), приховане векторне шифрування (Hidden Vector Encryption – HVE), шифрування з ранговим пошуком за множиною ключових слів (Multi-keyword Rank Searchable Encryption – MRSE) [9], гомоморфне шифрування (Homomorphic Encryption – HE).

Дамо коротку характеристику деяких із цих методів.

Шифрування з відкритим ключем із пошуком за ключовими словами (PEKS)

Цей метод вперше був представлений авторами роботи [10] у 2004 р. Ідея їхньої схеми PEKS полягає у використанні шифрування на основі ідентичності (Identity-Based Encryption – IBE), в якому ключове слово діє як посвідчення ідентичності (identity). Завдяки використанню PKE кожний користувач дозволяє створювати доступний для пошуку контент за допомогою відкритого ключа одержувача. Тільки власник закритого ключа може створити лазівку (Trapdoor) для пошуку всередині зашифрованих даних.

Щоб створити зашифрований текст із можливістю пошуку, відправник шифрує своє повідомлення M (загалом, під повідомленнями можна мати на увазі дані у відкритому вигляді, такі як файли, документи або записи в реляційній базі даних) за допомогою стандартної системи відкритого ключа і додає PEKS кожного ключового слова (тобто загальновідомий рядок, зашифрований за допомогою відкритого ключа (K_{pub}), пов'язаного з ключовим словом (w_j) як посвідчення справжності):

$$E_{K_{pub}}(M) \| C_1 = \text{PECS}(K_{pub}, w_1) \| ... \| C_m = \text{PECS}(K_{pub}, w_m) \quad (1)$$

Схематично цей процес можна подати так (рис. 1).

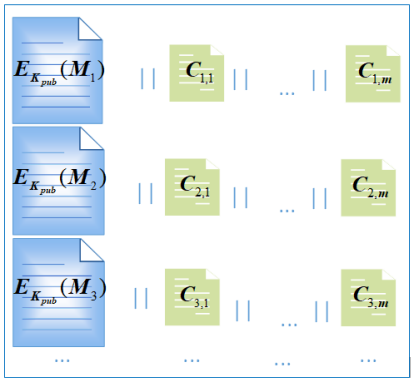


Рис. 1. Процес шифрування повідомлення з можливістю пошуку відповідно до схеми PEKS

Схема PEKS складається з наступних імовірнісних алгоритмів із поліноміальним часом реалізації:

– KeyGen(s). При параметрі безпеки s, що задається, генерується пара відкритий/закритий ключ K_{pub}, K_{priv};

– $c_j \leftarrow \text{PEKS}(K_{pub}, w_j)$. Для відкритого ключа K_{pub} та ключового слова w_j виконується шифрування w_j з можливістю пошуку;

– $T_j \leftarrow \text{Trapdoor}(K_{priv}, w_j)$. При заданому ключовому слові w_j та закритому ключі K_{priv} створюється лазівка T_j;

– $\text{Search}(K_{pub}, C, T_j) \rightarrow \{0,1\}$. Даний алгоритм пошуку/перевірки (Test), враховуючи відкритий ключ K_{pub}, виконане шифрування з можливістю пошуку $c_j \leftarrow \text{PEKS}(K_{pub}, w_j)$ та лазівку T_j, видає значення 1 (істинно), якщо $w_j = w'_j$, (тобто вкладене зашифроване повідомлення містить задане ключове слово), або 0 (хибно) в іншому випадку.

Основні особливості даної схеми [6, 8]:

– Основними сценаріями подібних схем є отримання електронних листів або документів з сервера та дозвіл серверу перенаправляти/маршрутизувати електронні листи. Відсутність взаємодії між відправником та одержувачем.

– Підтримується декілька власників даних (відправників) та один користувач даних (одержувач). Така схема широко відома як архітектура M/S (кілька письменників та один читач).

– Підходить для простору ключових слів поліноміального розміру.

– PEKS захищений від адаптивної атаки за вибраним ключовим словом (PK-CKA2) відповідно до білінійного припущення Діффі – Хеллмана (Bilinear Diffie-Hellman – BDH) у моделі Random Oracle.

– Поштовий сервер вважається чесним та допитливим, тобто правильно виконує всі алгоритми, але може спробувати дізнатися про якусь корисну інформацію.

Обмеження PEKS [6, 8]:

– Потрібен безпечний канал для запобігання прослуховування. Потрібний захищений канал для передачі лазівок, щоб зловмисник не зміг заволодіти лазівкою.

– Для підтримки кількох користувачів даних надсилається те саме повідомлення, зашифроване відкритим ключем кожного передбачуваного користувача, що призводить до надмірності.

– Оскільки простір ключових слів невеликий, PEKS та всі схеми шифрування з можливістю пошуку з відкритим ключем страждають від атак із підбором ключових слів.

– PEKS було розроблено для одноразового використання. Сервер може запам'ятати лазівку та використовувати її для отримання інформації про майбутні електронні листи.

– Не підтримує пошук за кількома ключовими словами.

Предикативне шифрування (PE)

Поняття предикатного шифрування (Predicate Encryption – PE) було вперше представлено у роботі [11]. PE забезпечує детальне керування доступом до зашифрованих даних. Предикатне шифрування – це нова парадигма шифрування з відкритим ключем, яке узагальнює шифрування, що охоплює різні криптографічні примітиви, такі як шифрування на основі ідентичності (IBE) [12 – 15], шифрування з прихованим вектором (HVE) [16, 17] і шифрування на основі атрибутів (ABE) [18]. PE націлений на більш потужні запити, але складність запиту призводить до вищих обчислювальних витрат. У PE секретні/закриті ключі пов'язані з предикатами, а зашифровані тексти пов'язані з атрибутами (I). Користувач може розшифрувати зашифрований текст, якщо предикат закритого (private) ключа набуває значення 1 при застосуванні до атрибуту зашифрованого тексту. PE поставляється у двох версіях: 1) із загальнодоступним індексом; 2) із прихованими атрибутами. Схеми (1) непридатні для шифрування з можливістю пошуку, тому що їм не вистачає властивості анонімності через виток набору атрибутів, за допомогою яких дані зашифровані. Схеми (2) можна використовувати для SE, але вони часто засновані на білінійних парах і тому менш ефективні ніж схеми, засновані на більш простих примітивах.

Схема предикативного шифрування для класу предикатів над множиною атрибутів складається з чотирьох алгоритмів Setup, GenKey, Enc, Dec:

$\mathrm{Setup}(1^n)$ приймає як вхідні дані параметр безпеки 1^n і виводить (головний – master) відкритий ключ *PK* і (головний) секретний ключ *SK*.

$SK_f \leftarrow \mathrm{GenKey}_{SK}(f)$ приймає на вхід головний секретний ключ *SK* та опис предикату $f \in F$; виводить ключ SK_f.

$C \leftarrow \mathrm{Enc}_{PK}(I, M)$ приймає як вхідні дані відкритий ключ *PK*, атрибут $I \in \Sigma$ і повідомлення M в деякому асоційованому просторі повідомлень; повертає зашифрований текст C.

$\begin{cases} M, f(I)=1 \\ \perp, f(I)=1 \end{cases} \leftarrow \mathrm{Dec}_{SK_f}(C)$ приймає як вхідні дані секретний ключ SK_f і зашифрований текст C; повертає або повідомлення M (тільки у тому випадку, коли предикат $f \in F$ і атрибут I пов'язані між собою), або виділений символ $\perp$ (з дуже малою ймовірністю).

Шифрування внутрішнього добутку (IPE)

Криптографічне IPE (Inner Product Encryption) або відоме як обчислення внутрішнього/скалярного добутку найчастіше використовуються в PE, IBE, AIBE та HVE [19]. IPE, представлене в роботах [11, 20], відомо, як криптографічний механізм, що дозволяє більш детально контролювати доступ до даних, що шифруються (механізм, що дозволяє полегшити користувачеві доступ до даних, які задовольняють потреби і вимоги поставленого завдання). В IPE предикати та атрибути представлені у вигляді векторів. Якщо внутрішній/скалярний добуток цих двох векторів дорівнює 0, то предикат дорівнює 1 (наприклад, атрибути відповідають вектору – $\vec{x}$, кожен предикат $f_{\vec{v}}$ відповідає вектору – $\vec{y}$, де $f_{\vec{v}}(\vec{x}) = 1$ тоді і тільки тоді, коли – $\vec{x} \cdot \vec{y} = 0$). Скалярний добуток дозволяє більш складні обчислення диз'юнкцій, багаточленів та формул КНФ (кон'юнктивна нормальна форма)/ДНФ (диз'юнктивна нормальна форма).

У роботах [11, 20] автори запропонували систему над $\square_N$ (для деякого великого цілого числа *N*). Автори робіт [19, 21] надали функції над F_p. Потім у роботах [22 – 25] було

запропоновано досконаліші схеми. Авторам роботи [11] вдалося побудувати схеми приховування атрибутів, які обробляють диз'юнкції предикатів з поліноміальним часом, відмінні від приховування корисного навантаження. Приховування корисного навантаження (payload-hiding) – це поняття безпеки для досягнення високих гарантій рівня безпеки, де зашифрований текст пов'язаний з атрибутом, який приховує всю інформацію, доки не буде отримано секретного ключа для розшифрування. Корисне навантаження та приховування атрибутів трохи відрізняються способом приховування зашифрованого тексту від відкритого тексту. Для приховування атрибута пов'язаний параметр повинен бути прихований разом із зашифрованим текстом, тоді як приховування корисного навантаження потрібно лише приховування відкритого тексту разом із зашифрованим текстом [24].

Анонімне шифрування на основі ідентичності (AIBE)

Анонімне шифрування на основі ідентичності (Anonymous Identity-Based Encryption – AIBE) у своїй стандартній формі може підтримувати лише перевірки на рівність та працює у сценарії/архітектурі M/S. Автори [10] були першими, хто розглянув шифрування з можливістю пошуку в налаштуваннях асиметричного ключа. Вони відзначають, що схема PEKS має тісний зв'язок із AIBE. Згодом їхня схема PEKS була вдосконалена авторами робіт [26, 27]. Автори [28] формалізували AIBE і представили загальну конструкцію SE, перетворивши схему шифрування на основі анонімної ідентифікації на схему шифрування з можливістю пошуку. Більш досконалі схеми IBE, що використовуються для шифрування з можливістю пошуку, було запропоновано авторами робіт [16, 29 – 31]. Щоб дозволити делегування, було введено ієрархічне шифрування на основі ідентичності (HIBE) [32 – 34], у якому закриті ключі та зашифровані тексти пов'язані з упорядкованими списками посвідчень (identities). Пізніше було запропоновано анонімні схеми HIBE (AHIBE) [16, 17, 35, 36]. Автори [28] також запропонували перетворення AHIBE-to-IBE з пошуком за ключовими словами (IBEKS) (hibe-2-ibeks).

Приховане векторне шифрування (HVE)

Приховане векторне шифрування (Hidden Vector Encryption – HVE) – це схема шифрування з відкритим ключем, яка підтримує знаки підстановки всередині ключа. Це дозволяє використовувати різні сценарії застосування. У роботі [37] автори у 2007 р. запропонували першу схему HVE для пошуку у зашифрованих даних. Їх схема допускає кон'юнктивні запити, запити підмножин та діапазонів. У роботі [11] автори розширили список диз'юнкцій, поліноміальних рівнянь та скалярних добутків. HVE можна як узагальнення AIBE [37]. Якщо HVE приховує ключове слово, перетворений PEKS не пропускає жодної інформації про ключове слово, що використовується в алгоритмі шифрування.

Гомоморфне шифрування (HE)

Гомоморфне шифрування (Homomorphic encryption – HE) – це особливий тип шифрування, який дозволяє виконувати операції алгебри над зашифрованими текстами, не розшифровуючи їх. Це робить HE цікавим інструментом пошуку за зашифрованими даними, оскільки над зашифрованими даними можна виконувати осмислені обчислення. Розрізняють криптосистеми частково гомоморфні та повністю гомоморфні. Частково гомоморфна криптосистема дозволяє робити тільки одну з операцій – або додавання, або множення. Повністю гомоморфна криптосистема підтримує виконання обох операцій, тобто, у ній виконуються властивості гомоморфізму як щодо множення, і щодо додавання. Тобто криптосистема є повністю гомоморфною (має і мультиплікативні, і адитивні гомоморфні властивості), якщо:

$$D(E(m_1)\otimes E(m_2)) = m_1 \square m_2;\ D(E(m_1)\oplus E(m_2)) = m_1 + m_2 \qquad (2)$$

де $E()$ – функція шифрування; $D()$ – функція розшифрування; m_1 та m_2 – відкриті тексти;

символи $\otimes$ та $\oplus$ позначають операції множення та додавання над шифртекстами, що відповідають операціям множення та додавання над відкритими текстами.

Більшість схем HE підтримують або додавання [38], або множення [39] за шифротекстом. Схема HE на основі пар, запропонована авторами [40], може виконувати довільну кількість додавань та одне множення. Повністю гомоморфне шифрування (Fully Homomorphic Encryption – FHE), яке може обчислювати довільні функції над зашифрованими даними, запропоновано авторами робіт [41 – 43]. Зазвичай вважається, що FHE може вирішити проблему запиту зашифрованих даних, оскільки будь-які значущі обчислення можуть бути виконані із зашифрованими даними. Однак однією з проблем із FHE є продуктивність, оскільки поточні схеми вимагають великих обчислювальних ресурсів та великих накладних витрат на зберігання. Починаючи з першої схеми FHE, дослідники намагалися зробити схеми ефективнішими, але досі не було запропоновано жодної практичної конструкції [44]. Для застосування можуть використовуватися так звані дещо (певною мірою) гомоморфні схеми шифрування (somewhat homomorphic encryption schemes). Ці схеми більш ефективні, ніж FHE, але допускають лише певну кількість додавань та множень [42, 45]. Основна проблема при частковому або повному використанні HE у тому, що підсумкові схеми пошуку вимагають часу пошуку лінійного за довжиною набору даних. Це занадто повільно для практичного застосування.

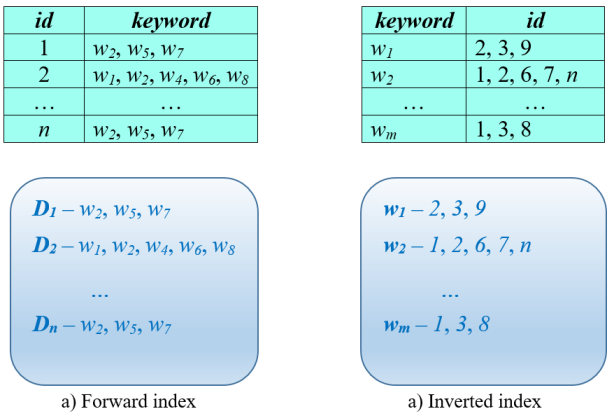
Симетричне шифрування із можливістю пошуку (SSE)

На методі симетричного шифрування з можливістю пошуку (Symmetric Searchable Encryption – SSE) зупинимося докладніше.

Припустимо, що $DB=(D_1,...,D_n)$ – це набір даних деякої БД. Під даними в даному випадку маємо на увазі деякий тип/категорію даних у відкритому вигляді, наприклад, такий як файли, документи, записи/значення атрибутів в реляційній базі даних і т. д. Є деякі похідні елементи даних: $W=(w_1,...,w_m)$, званими ключовими словами w_j. Між усіма ключовими словами W з DB і відповідними ідентифікаторами відповідного документа/запису D_i з DB існує певна відповідність (тобто є відповідності між усіма записами/документами що містять ключове слово w_j, де $j=1,...,m$).

Щоб створити доступний для пошуку зашифрований індекс I для даних, що розглядаються, вилучені з D_i ключові слова w_j зашифровуються (можливо таким способом, який не допускає розшифрування, – наприклад, за допомогою геш-функції) за допомогою секретного ключа K. Застосовується так званий алгоритм індексу збірки BuildIndex. У різних застосовуваних схемах SSE цей алгоритм має особливості реалізації.

Для побудови індексу, як правило, існує два підходи: створення прямого індексу (forward index) та створення зворотного/інвертованого індексу (inverted index) – рис. 2.



a) Forward index a) Inverted index

Рис. 2. Приклади незашифрованого прямого та інвертованого індексу

При першому підході індекс (прямий) будується на основі набору даних $(D_1,...,D_n)$, з кожним з яких пов'язані деякі ключові слова. При другому підході індекс (інвертований) будується за ключовими словами $(w_1,...,w_m)$. Він індексує кожне ключове слово, пов'язане з відповідним(и) D_i.

Прямий індекс є індексом для кожного D_i (рис. 2, *а*) і, природно, скорочує час пошуку до кількості таких D_i, тобто $O(n)$. Це пов'язано з тим, що під час запиту має оброблятися один індекс для кожного D_i.

В даний час переважним методом досягнення сублінійного часу пошуку є використання інвертованого/зворотного індексу, який є індексом за ключовим словом у базі даних (рис. 2, *б*). Інвертований індекс є індексом для кожного окремого слова в базі даних, а не для кожного D_i. Залежно від того, скільки інформації ми готові видати, складність пошуку можна скоротити до $O(\log w')$ (наприклад, за допомогою геш-дерева) або $O(|D(w)|)$ в оптимальному випадку, де $D(w)$ кількість D_i, що містить ключове слово w_j. Ідея використання інвертованого індексу скорочує час пошуку до кількості D_i, що містить ключове слово. Це не тільки сублінійно, а й оптимально [6].

Самі дані (у згаданому вище контексті) зашифровуються алгоритмом Enc за допомогою ключа K' (досить часто $K \neq K'$). Як Enc може використовуватися один із симетричних шифрів.

Зашифрований індекс (I) та зашифровані дані (C) зберігаються на сервері:

$$I = \text{BuildIndex}_K(DB = (D_1,...,D_n), W = (w_1,...,w_m)); \; C = \text{Enc}_{K'}(D_1,...,D_n). \qquad (3)$$

Сервер зазвичай вважається чесним, але допитливим (honest-but-curious), тобто йому можна довіряти у дотриманні протоколів зберігання та запитів, але слід враховувати, що він намагається отримати якнайбільше інформації. «Чесність» сервера виявляється в тому, що він не видаляє і не псує збережені дані, чесно діє за наперед визначеним протоколом, тобто виконує операцію пошуку зашифрованих даних за заданим ключовим словом/індексом і відправляє відповідні дані, пов'язані з запитами. Його «допитливість» полягає в тому, що решту інформації сервер намагається дізнатися з пошукових запитів та індексу.

Для пошуку необхідних зашифрованих даних створюється так звана лазівка/люк (Trapdoor), яку іноді називають токеном [8, 46] пошуку для ключового слова $T = \text{Trapdoor}_K(f)$, де f є предикатом на множині W ($f(w_1,...,w_m)$), що дозволяє серверу перевірити, чи є зашифроване ключове слово в результаті пошуку. За допомогою T сервер може шукати індекс, використовуючи алгоритм пошуку (Search), і дивитися, чи задовольняють зашифровані ключові слова предикату f, і якщо задовольняють, то алгоритм повертає відповідні зашифровані дані (див. рис. 3). Наприклад, f може визначити, чи міститься конкретне ключове слово в індексі, а більш складний може визначити, чи дорівнює 0 внутрішній добуток ключових слів в індексі і цільовому наборі ключових слів [47].

Загальна модель схеми шифрування з можливістю пошуку з урахуванням індексу представлено рис. 3.

Слід зазначити, що можуть бути невеликі відхилення. Наприклад, деякі схеми не вимагають повного списку ключових слів для побудови індексу [6].

Загалом можна виділити такі основні елементи (алгоритми з поліноміальним часом виконання), описаної вище схеми SSE:

$K \leftarrow \text{Keygen}\left(1^k\right)$: алгоритм генерації ключів, що запускається власником даних (користувачем). Він приймає параметр безпеки (security parameter) k як вхідні дані і видає секрет-

ний ключ K. Якщо для шифрування використовується ще другий ключ K', такий що $K \neq K'$, то для нього аналогічно, але з використанням параметра k' генерується ключ K';

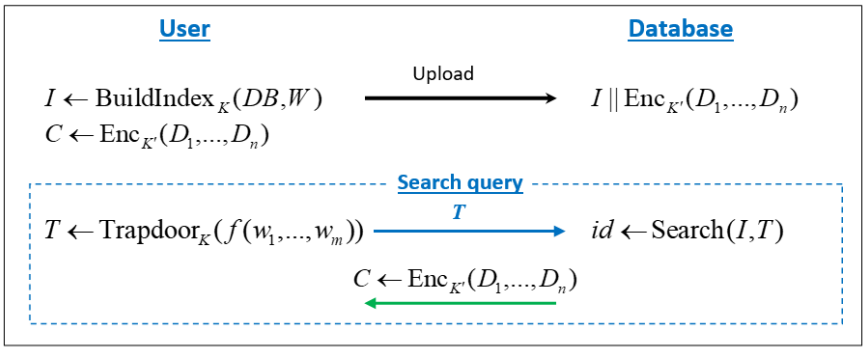


Рис. 3. Загальна модель схеми шифрування з можливістю пошуку на основі індексу

$I \leftarrow \text{BuildIndex}_K(DB,W)$: алгоритм, який запускає власник даних (користувач). Він приймає як вхідні дані секретний ключ K і набір даних $DB = (D_1,...,D_n)$, $W = (w_1,...,w_m)$, а видає безпечний індекс I;

$C \leftarrow \text{Enc}_{K'}(D_1,...,D_n)$: алгоритм, який запускає власник даних (користувач). Він приймає як вхідні дані секретний ключ K' і набір даних $DB = (D_1,...,D_n)$, а видає послідовність зашифрованих даних $C = (c_1,...,c_n) = Enc_{K'}(D_1,...,D_n)$;

$T \leftarrow \text{Trapdoor}_K(f(w_1,...,w_m))$: алгоритм, що запускається користувачем для створення лазівки для заданого ключового слова (внутрішнього добутку ключових слів). Він приймає як вхідні дані секретний ключ K і ключове(і) слово(а) w_j і видає лазівку T;

$id \leftarrow \text{Search}(I,T)$: алгоритм, який запускається сервером для пошуку D_i в DB, що містять ключове слово w_j. Він приймає як вхідні дані зашифрований індекс I для набору даних DB і лазівку T і виводить набір ідентифікаторів id відповідного D_i;

$D_i \leftarrow \text{Dec}_K(c_i)$: алгоритм, який запускається клієнтом для відновлення D_i. Він приймає як вхідні дані секретний ключ K і зашифрований текст c_i, а видає розшифрований D_i.

Моделі схем SE

Для розгляду принципів існуючих захищених пошукових систем слід враховувати деякі особливості сценаріїв їхнього функціонування. Так, наприклад, у роботі [7] виділяють два такі сценарії. А саме двосторонній сценарій, в якому один користувач діє як постачальник/власник даних та запитувач (клієнт). Такий сценарій моделює програму аутсорсингу хмарного сховища, в якому клієнт завантажує файли у хмару, які він може пізніше запросити. На рис. 4 зображено такий сценарій.

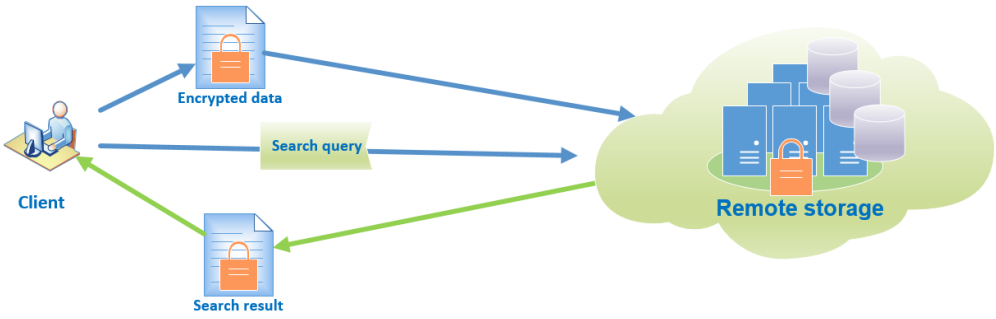


Рис. 4. Модель схеми SE із двома учасниками

У моделі схеми SE із двома учасниками клієнт має право знати всю інформацію у базі даних, тому необхідно враховувати лише захист від допитливого сервера.

Тристоронній сценарій (модель), передбачає наявність трьох учасників: постачальника (довіреного власника даних – trusted data owner), групу користувачів, яким дозволено пошук (які запитують), та напівдовірений (semi-trusted)/чесний, але допитливий сервер. Роль кожного з них така:

– Власник даних (Data owner). Власник даних хотів би передати на аутсорсинг набір даних $DB = (D_1, ..., D_n)$ разом із деякими ключовими словами $W = (w_1, ..., w_m)$. При цьому він має особливим чином зашифрувати ці дані та ключові слова, щоб згодом легко їх шукати, а потім надіслати зашифровані дані на сервер;

– Користувач даних (Data user). Авторизований користувач виконує пошук у наборі даних $DB = (D_1, ..., D_n)$, що містять певне ключове слово, для чого він відправляє лазівку T цього ключового слова на сервер. Після пошуку сервер повертає користувачеві відповідні дані ($id \leftarrow \text{Search}(I, T)$), що містять вказане ключове слово;

– Сервер (Server) Сервер здійснює пошук. Коли сервер отримує лазівку ключового слова запиту від користувача, він шукає зашифровані тексти, а потім повертає відповідні дані користувачеві. Передбачається, що сервер є чесним, але допитливим.

Слід пам'ятати, що безпечна система пошуку для одного сценарію не поширюється автоматично на інший сценарій.

На рис. 5 показано модель схеми SSE із трьома учасниками.

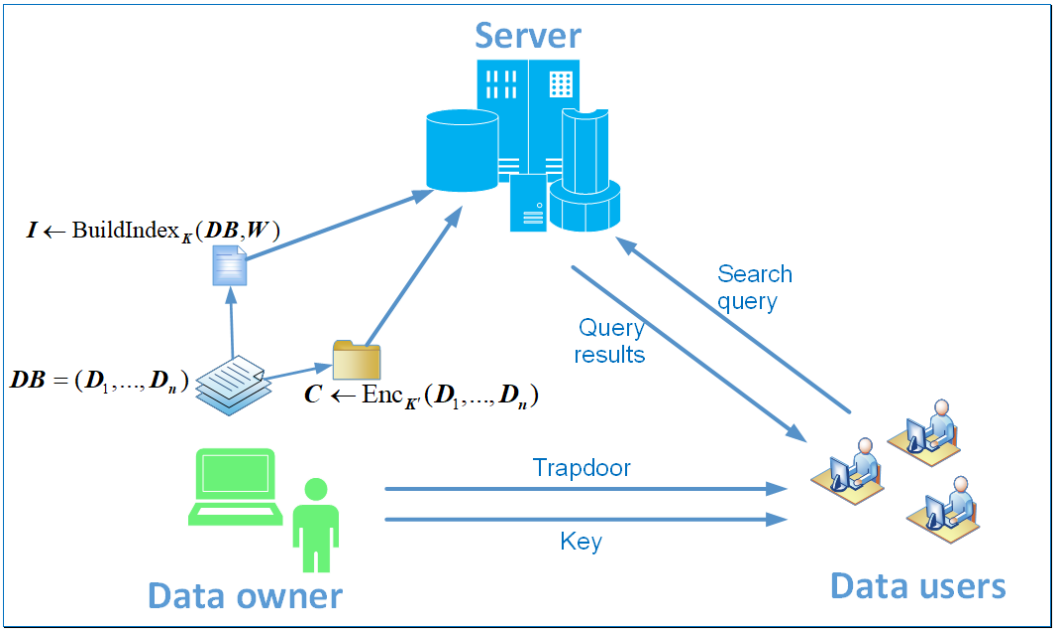


Рис. 5. Модель схеми SSE із трьома учасниками

Архітектури схем SE

Як зазначалося раніше, схеми SE будуються на основі клієнт-серверної моделі. Сервер зберігає зашифровані дані одного чи кількох клієнтів (так званих письменників). Щоб запросити контент із сервера, один або кілька клієнтів (читачів) можуть створювати лазівки для сервера, який потім шукає від імені відповідного клієнта. Як результат можуть мати місце наступні чотири архітектури SE [6]:

– один письменник / один читач (S/S);
– багато письменників / один читач(M/S);
– один письменник / багато читачів (S/M);
– багато письменників / багато читачів (M/M).

В залежності від архітектури схема SE підходить або для аутсорсингу даних (S/S), або для спільного використання даних (M/S, S/M, M/M).

Схеми симетричного шифрування з можливістю пошуку дозволяють одному користувачеві читати та записувати дані (S/S), тобто дозволяють власнику секретного ключа створювати доступні для пошуку зашифровані тексти та лазівки [8]. Перша схема S/S була запропонована у роботі [48].

У схемі шифрування з відкритим ключем (PKE) секретний ключ розшифровує всі повідомлення, які зашифровані відповідним відкритим ключем. Таким чином, PKE допускає розрахований на багато користувачів запис, але тільки власник секретного ключа може виконувати пошук. Для цього потрібна архітектура M/S. Перша схема M/S належить авторам роботи [10], які запропонували схему шифрування з відкритим ключем та пошуком за ключовими словами (PEKS). Серед доступних криптографічних примітивів з відкритим ключем вони використовували шифрування на основі ідентичності (IBE) як базову схему. Вони використовували відкритий ключ, відповідний особі користувача, для шифрування файлу даних та ключових слів, що містяться у файлі даних. Схема була розроблена для ефективного отримання зашифрованих листів з поштового сервера. Власник даних або, точніше, відправник хоче надіслати електронний лист, зашифрований за допомогою відкритого ключа одержувача, разом із ключовими словами, зашифрованими за допомогою того ж ключа. Надіслана електронна пошта зберігається на поштовому сервері одержувача, і одержувачу потрібен механізм для ефективного вилучення з них лише потрібних електронних листів. Цей ефективний механізм є методом шифрування з можливістю пошуку, без якого одержувач спочатку повинен завантажити всі електронні листи, а потім розшифрувати їх локально, використовуючи свій закритий ключ. Але за допомогою методу шифрування з можливістю пошуку одержувач може витягувати електронні листи відповідно до своїх поточних вимог, і йому необхідно розшифрувати лише вибрані електронні листи. Весь цей механізм підходить для тих сценаріїв, де мається один передбачуваний одержувач, однак обмежень на кількість відправників немає. PEKS використовується як назва класу схем M/S [6].

Деякі схеми SE розширюють налаштування */S шляхом дозволу розрахованого на багато користувачів читання (*/M). Це розширення призводить до необхідності розповсюдження (розподілу) секретного ключа, щоб дозволити кільком користувачам здійснювати пошук в зашифрованих даних. Деякі схеми SE використовують спільне використання ключів. Інші схеми використовують розподіл ключів, повторне шифрування проксі (proxy re-encryption) або інші методи вирішення проблеми.

При цьому важливою вимогою, що пред'являється до схем з безліччю читачів, є відкликання (анулювання) користувача. У роботі [49] автори, наприклад, розширюють свою однокористувацьку схему з широкомовним шифруванням (broadcast encryption – BE [50]) до розрахованої на багато користувачів схеми з безліччю читачів (S/M). Але оскільки тільки один ключ є спільним для всіх користувачів, кожне відкликання вимагає розповсюдження нового ключа серед користувачів, що викликає великі накладні витрати на відкликання. В інших схемах у кожного користувача може бути свій ключ, що спрощує відкликання користувача і робить його ефективнішим.

В цілому ж, проєктування захищеної системи пошуку – це баланс/компроміс між безпекою, функціональністю, ефективністю/продуктивністю та зручністю використання [6, 7].

Оскільки безпека ніколи не буває безкоштовною, завжди існує компроміс між безпекою (security) з одного боку та ефективністю (efficiency) та виразністю запитів (query expressiveness) з іншого. Схеми шифрування з можливістю пошуку, в яких використовується модель безпеки з сильнішим противником (зловмисником, порушником), ймовірно, матимуть більш високу складність. Коли у схемі покращується один із аспектів, зазвичай це призводить до погіршення одного або відразу кількох інших аспектів.

Безпека зазвичай визначається інформацією про дані користувача, яка стає відома атакуючому в процесі роботи схеми. Існує два типи сутностей, які можуть становити загрозу

безпеці бази даних: дійсний/законний користувач (valid user), відомий як інсайдер (insider), що виконує одну або кілька ролей, та сторонній (outsider), який може відслідковувати та потенційно змінювати мережеву взаємодію між дійсними користувачами. При цьому є зловмисники (порушники), які є напівчесними (або чесними, але допитливими), тобто вони наслідують запропоновані протоколи, але можуть пасивно намагатися дізнатися додаткову інформацію з повідомлень, які вони спостерігають. І є зловмисні порушники, тобто ті, хто активно бажає виконувати будь-які дії, необхідні для отримання додаткової інформації або впливу на роботу системи. Слід зазначити, більшість активних досліджень у сфері технології захищеного пошуку розглядає напівчесний захист від постійного внутрішнього противника [7].

Виразність схеми запитів визначає, які пошукові запити підтримуються, якого типу, як вони виражаються (зазвичай за допомогою стандартних мов, наприклад, SQL). У сучасних підходах часто буває так, що більш виразні запити призводять до меншої ефективності, або до меншої безпеки.

Ефективність вимірюється обчислювальною та комунікаційною складністю схеми. Вона поряд з обчислювальними та комунікаційними витратами залежить від структури даних та механізмів індексування у базі даних.

Розглянемо ці аспекти.

Проблеми конфіденційності у схемах SE

Для схем шифрування з можливістю пошуку характерне власне поняття безпеки, оскільки всі найпотужніші криптографічні атаки на такі системи будуються на основі експлуатації витоків логічного виводу (inference), до яких схильна більшою чи меншою мірою майже будь-яка практична SE-схема. У процесі роботи SE-схеми відбувається постійна взаємодія між клієнтом та сервером. При спостереженні та статистичному аналізі запитів і відповідей сервера, що надходять від клієнта, зловмисник може отримувати істотну кількість непрямих даних (іноді званих метаданими) про зашифровану інформацію користувачів. Припустимо, що зловмисник має доступ до зашифрованих даних на сервері та може спостерігати запити користувачів. Також він знає, скільки записів повертається у відповідь на кожен запит. Якщо ця кількість унікальна, то запит також унікальний і його можна розрізнити серед безлічі всіляких запитів.

Безпека зазвичай пов'язується з інформацією, яка в процесі роботи схеми розкривається або просочується зловмиснику, який має доступ до сервера бази даних. У схемі шифрування з можливістю пошуку має бути гарантована безпека набору даних та ключових слів, що зберігаються на сервері, а також має бути забезпечена безпека ключових слів запиту.

У схемах SE може мати місце витік інформації, яку можна розділити на три групи [6]:

– Інформація індексу (Index information) відноситься до інформації про ключові слова, що містяться в індексі. Інформація про індекс просочується із збереженого шифртексту (ciphertext)/індексу. Ця інформація може включати кількість ключових слів на документ/базу даних, кількість документів, довжину документів, ідентифікатори документів і/або подібність документів;

– Шаблон пошуку (Search pattern) відноситься до інформації, яка може бути отримана в наступному сенсі: за умови, що два пошуки повертають одні й ті самі результати, потрібно визначити, чи використовують ці два пошуки одне й те саме ключове слово/предикат. Або іншими словами шаблон пошуку визначається як будь-яка інформація, яку можна отримати, знаючи, чи відносяться два результати пошуку до одного й того самого ключового слова. Використання детермінованих лазівок безпосередньо призводить до витоку шаблону пошуку. Доступ до шаблону пошуку дозволяє серверу використовувати статистичний аналіз та (можливо) визначати інформацію про ключові слова запиту або самі ключові слова;

– Шаблон доступу (Access pattern) відноситься до інформації, яка передбачається результатами запиту. Наприклад, один запит може повернути D_i, а інший запит може повернути D_i і ще 5, 10 і т. д. інших $D_l \in DB$. Це означає, що предикат, який використовується

у першому запиті, є суворішим, ніж предикат в інших запитах. Шаблон доступу: визначається як послідовність результатів пошуку $(DB(w_1),...,DB(w_m))$, де $DB(w_j)$ – результати пошуку w_j. Інакше кажучи, $DB(w_j)$ – це набір даних у DB, що містить ключове слово w_j.

Слід зазначити, що у багатьох схемах [6] є витік як мінімум шаблону пошуку та шаблону доступу. Хоча більшість схем дотримуються визначення безпеки, що використовується у традиційному шифруванні з можливістю пошуку. А саме, в них виконується вимога того, щоб з віддалених даних і індексів нічого не просочувалося, крім результату і шаблону пошукових запитів. Схеми SE не повинні пропускати ключові слова відкритого тексту ні в лазівку, ні в індекс.

Щоб формально визначити безпеку схеми, було запропоновано багато різних моделей безпеки.

Коли автори роботи [48] запропоновували першу схему SE, не було формальних визначень безпеки для конкретних SE. Проте вони довели, що їхня схема є безпечною з погляду нерозрізненості для атак на основі підібраного відкритого тексту (indistinguishability under chosen plaintext attack – IND-CPA), інакше кажучи, є IND-CPA надійною [46]. Неформально схема шифрування є IND-CPA надійною, якщо зловмисник A не може розрізнити шифрування двох довільних повідомлень (вибраних самим A), навіть якщо може адаптивно посилати запити провісника (oracle) шифрування. Інтуїтивно це означає, що схема безпечна з погляду IND-CPA, якщо результуючі зашифровані тексти не містять навіть часткової інформації про відкриті тексти. Це визначення IND-CPA гарантує, що зашифровані тексти не допускають витоку інформації. Однак у SE основний витік інформації походить з лазівки/запиту, що не враховується у безпеці IND-CPA. Таким чином, безпека IND-CPA не співвідноситься з поняттям безпеки SE.

Перше поняття безпеки в контексті SE було введено автором роботи [51], який визначив безпеку індексів як семантичну безпеку (нерізницю) від адаптивних атак за вибраним ключовим словом (semantic security (indistinguishability) against adaptive chosen keyword attacks – IND1-CKA). IND1-CKA гарантує, що A не може відтворити вміст документа з його індексу. Схема безпеки IND1-CKA створює індекси, що містять однакову кількість слів для документів однакового розміру (на відміну документів різного розміру). Це означає, що за наявності двох зашифрованих документів рівного розміру та індексу, A не може вирішити, який із документів закодований в індексі. IND1-CKA був запропонований для «захищених індексів», захищеної структури даних з безліччю застосувань поряд із SSE. При цьому в роботі [51] зазначається, що IND1-CKA не вимагає, щоб лазівки були безпечними, оскільки це необхідно не для всіх застосувань безпечних індексів.

Автори роботи [52] представили нове визначення IND-CKA, засноване на моделюванні, яке є суворішою версією IND1-CKA у тому сенсі, що зловмисник не може відрізнити навіть індекси двох документів з різним розміром. Для цього потрібно, щоб документи різного розміру мали індекси, що містять однакову кількість слів. Пізніше було представлено визначення безпеки IND2-CKA, яке захищає розмір документа, як і визначення, дане в роботі [52], але все ж таки не забезпечує безпеку для лазівок. Обидва визначення безпеки IND1/2-CKA вважаються слабкими в контексті SE, оскільки вони не гарантують безпеку лазівок, тобто вони не гарантують, що сервер не зможе відновити інформацію про запитані слова з лазівки або самі слова. У роботі [49] переглянуто існуючі визначення безпеки. Її автори вказали, що попередні визначення не підходять для SSE і що безпека індексів та безпека лазівок нерозривно пов'язані. Вони представили дві нові змагальні моделі для шифрування з можливістю пошуку: неадаптивну (IND1-CKA) та адаптивну (IND2-CKA), які на сьогодні широко використовуються як стандартні визначення для симетричного шифрування з можливістю пошуку. Інтуїтивно зрозуміло, що визначення вимагають, щоб з файлів та індексів, що віддалено зберігаються, нічого не просочувалося, крім результату і шаблону пошукових запитів. Визначення безпеки IND-CKA1/2 включають безпеку для лазівок і гарантують, що лазівки не пропуска-

ють інформацію про ключові слова (за винятком тієї, яку можна вивести з шаблонів пошуку та доступу). Неадаптивні визначення гарантують безпеку схеми лише у тому випадку, якщо клієнт генерує всі запити одночасно. Це може бути нездійсненним для певних (практичних) сценаріїв. Адаптивне визначення дозволяє зловмиснику A вибирати свої запити залежно від раніше отриманих лазівок та результатів пошуку. Таким чином, IND-CKA2 вважається надійним визначенням безпеки SSE.

В асиметричному варіанті (з відкритим ключем) автори схеми [10] не гарантують безпеку лазівок, оскільки зазвичай лазівки генеруються з використанням відкритого ключа. Визначення в цьому контексті гарантує, що жодна інформація про ключове слово не буде отримана тільки в тому випадку, якщо для цього слова не буде доступна лазівка. Зловмисник не повинен мати можливості розрізняти шифрування двох вибраних ним ключових слів виклику (challenge keywords), навіть якщо дозволено отримувати лазівки для будь-яких ключових слів (крім ключових слів виклику). Дотримуючись попереднього поняття, для позначення невідмінності від адаптивних атак за вибраним ключовим словом схем з відкритим ключем, використовується позначення PK-CKA2 (public key CKA2).

Інші визначення безпеки були введені та/або адаптовані для SE наступним чином:

– Універсальна компоновність (universal composability – UC) – це модель загального призначення, в якій йдеться про те, що протоколи залишаються безпечними, навіть якщо вони довільно складені з інших екземплярів того ж чи інших протоколів.

– Вибірково безпечна (selectively secure – SEL-CKA) – ця модель схожа на PK-CKA2, але зловмисник A повинен зафіксувати ключові слова пошуку на початку забезпечення безпеки, а не після першої фази запиту.

– Цілком безпечна (fully secure – FS) – це визначення безпеки в контексті SSE, введене в роботі [47], яке не дозволяє витекти нічому, крім шаблону доступу.

Ефективність схем SE

Ефективність вимірюється обчислювальною та комунікаційною складністю схеми, а саме, даний аспект фокусується на обчислювальній складності алгоритмів шифрування/генерації індексу (фаза завантаження) та алгоритмів пошуку/тестування (фаза запиту). Для об'єктивного порівняння схем використовуються такі метрики, як кількість необхідних операцій, складність оновлення або інтерактивності (кількість раундів) та деякі інші. На продуктивність та зручність використання впливають структури даних бази даних та механізми індексування, а також необхідні обчислювальні та мережеві витрати.

З точки зору SSE, складність пошуку в деяких схемах лінійна за кількістю документів, що зберігаються на сервері. Хоча в деяких схемах досягається сублінійний час пошуку, при якому складність пошуку знаходиться в логарифмічній залежності кількості ключових слів у всіх документах. При цьому необхідно пам'ятати та враховувати, що документи/набір даних слід акуратно динамічно оновлювати, оскільки індекс пошуку прив'язаний до ключових слів. Отже, питання, як побудувати ефективну динамічну схему SSE, є відкритим.

З точки зору PKES велика кількість схем заснована на спарюванні (pairing)/білінійних відображеннях (bilinear maps). У результаті ці схеми є неефективними, тому що неефективними є алгоритми білінійних відображень.

Схеми симетричного шифрування з можливістю пошуку (SSE) швидше, ніж схеми шифрування з відкритим ключем та пошуком за ключовими словами (PEKS) [8]. Тому деякі автори [7] рекомендують по-можливості уникати повільніших операцій з відкритим ключем або мінімізувати їх на користь швидших примітивів із симетричним ключем. Однак, слід пам'ятати, що розподіл секретних ключів між усіма користувачами, враховуючи необхідність періодичного відкликання користувача і розповсюдження нового ключа серед користувачів, є досить складною процедурою, що викликає великі накладні витрати.

Захищений пошук швидко розвивається з 2000 р., переходячи від лінійних запитів на рівність за статичними даними до складного пошуку за динамічними даними. Сьогодні накладні витрати становлять від 30 до 500 % порівняно із стандартним SQL [7].

Порівняння кількох класичних схем SSE з погляду найгіршого часу паралельного пошуку за ключовим словом [53, 54] наведено у табл. 1.

Таблиця 1

Схема	Часова складність алгоритму пошуку	Часова складність алгоритму побудови індексу	Безпека
Song, et al.[48]	$O(n/p)$	N/A	IND-CPA
Goh[51]	$O(n/p)$	$O(n)$	IND-CKA1
Chang, et al. [52]	$O(n/p)$	$O(mn)$	IND-CKA1
Curtmola, et al.[49](SSE-1)	$O(r)$	$O(m+n)$	IND-CKA1
Curtmola, et al.[49](SSE-2)	$O(r)$	$O(mn)$	IND-CKA2
Liesdonk, et al. [55]	$O(n)$	$O(mn)$	IND-CKA2
Kurosawa, et al. [56]	$O(n)$	$O(mn)$	UC
Kamara, et al. [46]	$O(r)$	$O(m+n)$	IND-CKA2
Kamara, et al. [54]	$O((r/p)\log n)$	$O(mn)$	IND-CKA2

Де IND-CPA – невиразність для атак на основі підібраного відкритого тексту; IND1-CKA – семантична безпека (невідмінність) від адаптивних атак за вибраним ключовим словом; IND-CKA1 – неадаптивна модель, у якій зловмисник не враховує лазівки та результати попередніх пошуків, коли вибирає складні пошукові запити; IND-CKA2 – це адаптивна модель, в якій зловмисник вибирає свої пошукові запити, знаючи раніше отримані лазівки та результати пошуку; n – потужність множини DB, r – кількість D_i (документів), що містять ключове слово запиту w_j, m – розмір простору ключових слів, p – кількість ядер, N/A (not available) – немає відомостей (дані відсутні).

У той же час, наприклад, ефективність схеми PEKS [10] характеризується такими значеннями: шифрування вимагає від сервера виконання одного обчислення симетричної пари простого порядку p, двох зведень у ступінь e та застосування двох геш функцій h для кожного ключового слова; складність пошуку – лінійна (одне білінійне відображення, одна геш функція) за кількістю ключових слів у документі.

Виразність запитів у схемах SE

Проведено дослідження щодо розширення виразності запитів. Щоб зробити схеми більш практичними, підтримуються не тільки точний пошук за одним ключовим словом, але також нечіткий пошук за ключовими словами, пошук за діапазоном та пошук за підмножиною. При цьому результати запиту можуть також оптимізуватися.

Наприклад, ранжований пошук за ключовими словами знаходить найближчі результати, а пошук, що перевіряється за ключовими словами, перевіряє правильність і повноту результатів. Однак багато схем покращують виразність запитів за рахунок ефективності чи безпеки. Тому в майбутніх дослідженнях доцільно звернути увагу на компроміс між виразністю запитів та ефективністю чи безпекою. У схемі SE є такі варіанти компромісів [6]: безпека та виразність запитів, ефективність та виразність запитів.

Вирішення проблеми захищеного пошуку вимагає тісної взаємодії між фахівцями в галузі криптографії, розробниками захищеного пошуку та експертами з баз даних [7].

Висновки

Широке поширення конфіденційних даних у відкритих інформаційних та комунікаційних інфраструктурах стимулювало дослідження в галузі безпечного управління даними та підвищило їх актуальність. На підставі проведеного аналізу було виявлено, що методи SSE та PEKS є найбільш популярними методами SE, які використовуються серед інших методів шифрування з можливістю пошуку.

З моменту запропонування перших схем SSE та PEKS область досліджень шифрування з можливістю пошуку привернула значну увагу. Прогресу було досягнуто в наступних трьох основних напрямках:

1. *Виразність запитів*. Було проведено багато досліджень щодо розширення виразності запитів. Щоб зробити схеми більш практичними, підтримується не тільки точний пошук за одним ключовим словом, але також нечіткий пошук за ключовими словами, пошук за діапазоном та пошук за підмножиною. Однак багато схем покращують виразність запитів за рахунок ефективності чи безпеки. Тому майбутні дослідження повинні звернути увагу на компроміс між виразністю запитів та ефективністю чи безпекою.

2. *Ефективність.* З точки зору SSE, складність пошуку в деяких схемах лінійна за кількістю документів, що зберігаються на сервері. Однак у деяких схемах досягається сублінійний час пошуку, в якому складність пошуку логарифмічна за кількістю ключових слів у всіх документах. З настанням ери великих даних великі обсяги даних тепер потрібно зберігати на серверах. В результаті виникає закономірне питання про те, як ефективно працювати з великомасштабними даними, а отже, цей напрямок також вважається перспективним для подальшої роботи. Більше того, документи не можна гнучко оновлювати, оскільки пошуковий індекс прив'язаний до ключових слів. Отже, питання про те, як побудувати ефективну динамічну схему SSE, є ще одним напрямком майбутньої роботи.

З погляду PKES, велика кількість схем ґрунтується на парних відображеннях. У результаті ці схеми є неефективними, тому що парні (білінійні) відображення є неефективними алгоритмами. Таким чином, побудова практичних схем PKES є напрямом майбутніх робіт.

3. *Безпека.* Хоча практично всі схеми SE забезпечують безпеку, вони не використовують загальну модель безпеки. Тобто різні схеми використовують різні моделі безпеки при різних припущеннях. Тому завжди складно порівнювати їхню захищеність. Тому розробка деякої стандартної моделі безпеки для схем SE є перспективним напрямом майбутніх досліджень. Крім того, більшість схем компрометують шаблон пошуку та шаблон доступу. Таким чином, побудова ефективної схеми, що не допускає витоку шаблону пошуку та шаблону доступу, є ще одним перспективним напрямом досліджень.

Список літератури:

1. Abadi D., Ailamaki A., Andersen D., Bailis P., Balazinska M., Bernstein P., Boncz P., Chaudhuri S., et al. The Seattle Report on Database Research. ACM SIGMOD Record. 2019. 48. P. 44–53.
2. General Data Protection Regulation GDPR. URL: https://gdpr-info.eu/ (дата звернення: 12.06.2022).
3. Payment Card Industry (PCI) Data Security Standard. Requirements and Testing Procedures Version 4.0. 2022. URL: https://www.pcisecuritystandards.org/documents/PCI-DSS-v4_0.pdf (дата звернення: 12.06.2022).
4. Atchinson B. K., Fox D. M. From the field: the politics of the health insurance portability and accountability act // Health affairs. 1997. 16(3). P. 146-150.
5. Scholl M., Stine K., Hash J., Bowen P., Johnson A., et al. NIST Special Publication 800-66 Revision 1. An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. 2008. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-66r1.pdf (дата звернення: 12.06.2022).
6. Bösch, C., Hartel, P., Jonker, W., Peter, A. A survey of provably secure searchable encryption // ACM Computing Surveys (CSUR). 2014. 47(2). P. 1–51.
7. Fuller B., Varia M., Yerukhimovich A., Shen E., Hamlin A., Gadepally V., Shay R., Mitchell J. D., Cunningham R. K. Sok: Cryptographically protected database search // 2017 IEEE Symposium on Security and Privacy (SP), 2017. P. 172–191. https://doi.org/10.1109/SP.2017.10.
8. Gupta B., Mamta Secure Searchable Encryption and Data Management (1st ed.). CRC Press. 2021. 116 p. https://doi.org/10.1201/9781003107316.
9. Li R., Xu Z., Kang W., Yow K. C., Xu C. Z. Efficient multi-keyword ranked query over encrypted data in cloud computing // Future Generation Computer Systems. 2014. 30. P. 179–190.
10. Boneh D., Crescenzo G. D., Ostrovsky R., Persiano G. Public Key Encryption with Keyword Search // Cachin, C., Camenisch, J.L. (eds) Advances in Cryptology – EUROCRYPT 2004. EUROCRYPT 2004. Lecture Notes in Computer Science, 2004. Vol 3027. P. 506–522. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-24676-3_30/

11. Katz J., Sahai A., Waters B. Predicate encryption supporting disjunctions, polynomial equations, and inner products // Smart, N. (eds) Advances in Cryptology – EUROCRYPT 2008. EUROCRYPT 2008. Lecture Notes in Computer Science. Springer, Berlin, Heidelberg, 2008. Vol. 4965. P. 146–162. https://doi.org/10.1007/978-3-540-78967-3_9.

12. Shamir A. Identity-Based Cryptosystems and Signature Schemes // Blakley, G.R., Chaum, D. (eds) Advances in Cryptology. CRYPTO 1984. Lecture Notes in Computer Science. Springer, Berlin, Heidelberg. 1985. Vol. 196. P. 47–53. https://doi.org/10.1007/3-540-39568-7_5.

13. Boneh D., Franklin M. Identity-Based Encryption from the Weil Pairing // Kilian, J. (eds) Advances in Cryptology – CRYPTO 2001. CRYPTO 2001. Lecture Notes in Computer Science. Springer, Berlin, Heidelberg. 2001. Vol 2139. P. 213–229. https://doi.org/10.1007/3-540-44647-8_13.

14. Boneh D., Franklin M. Identity-based encryption from the Weil pairing // SIAM journal on computing. 2003. 32(3). P. 586–615.

15. Cocks C. An Identity Based Encryption Scheme Based on Quadratic Residues // Honary, B. (eds) Cryptography and Coding. Cryptography and Coding 2001. Lecture Notes in Computer Science. Springer, Berlin, Heidelberg. 2001. Vol 2260. P. 360–363. https://doi.org/10.1007/3-540-45325-3_32.

16. Boyen X., Waters B. Anonymous Hierarchical Identity-Based Encryption (Without Random Oracles) // Dwork, C. (eds) Advances in Cryptology – CRYPTO 2006. CRYPTO 2006. Lecture Notes in Computer Science. Springer, Berlin, Heidelberg. 2006. Vol 4117. P. 290–307. https://doi.org/10.1007/11818175_17.

17. Shi E., Bethencourt J., Chan T. H., Song D., Perrig A. Multi-dimensional range query over encrypted data. // 2007 IEEE Symposium on Security and Privacy (SP'07). IEEE, 2007. P. 350–364. https://doi.org/10.1109/SP.2007.29.

18. Sahai A., Waters B. Fuzzy Identity-Based Encryption // Cramer, R. (eds) Advances in Cryptology – EUROCRYPT 2005. EUROCRYPT 2005. Lecture Notes in Computer Science. Springer, Berlin, Heidelberg. 2005. Vol 3494. P. 457–473. https://doi.org/10.1007/11426639_27.

19. Lewko A., Okamoto T., Sahai A., Takashima K., Waters, B. Fully Secure Functional Encryption: Attribute-Based Encryption and (Hierarchical) Inner Product Encryption // Gilbert, H. (eds) Advances in Cryptology – EUROCRYPT 2010. Lecture Notes in Computer Science, 2010. Vol 6110. P. 62-91. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-13190-5_4.

20. Katz J., Sahai A., Waters B. Predicate encryption supporting disjunctions, polynomial equations, and inner products // Journal of cryptology. 2013. 26(2). P. 191-224. https://doi.org/10.1007/s00145-012-9119-4.

21. Okamoto T., Takashima K. Hierarchical Predicate Encryption for Inner-Products // Matsui, M. (eds) Advances in Cryptology. ASIACRYPT 2009. Lecture Notes in Computer Science, 2009, Vol 5912. P. 214-231. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-10366-7_13.

22. Okamoto T., Takashima K. Fully Secure Functional Encryption with General Relations from the Decisional Linear Assumption // Rabin, T. (eds) Advances in Cryptology – CRYPTO 2010. CRYPTO 2010. Lecture Notes in Computer Science, 2010. Vol 6223. P. 191–208. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-14623-7_11.

23. Okamoto, T., Takashima, K. Adaptively Attribute-Hiding (Hierarchical) Inner Product Encryption // Pointcheval, D., Johansson, T. (eds) Advances in Cryptology – EUROCRYPT 2012. EUROCRYPT 2012. Lecture Notes in Computer Science, 2012. Vol 7237. P. 591–608. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-29011-4_35.

24. Okamoto T., Takashima K. Adaptively attribute-hiding (hierarchical) inner product encryption // IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences. 2016. 99(1). P. 92-117.

25. Park J. H. Inner-product encryption under standard assumptions // Designs, Codes and Cryptography, 2011. 58(3), 235–257. https://doi.org/10.1007/s10623-010-9405-9.

26. Baek J., Safavi-Naini, R., Susilo W. Public Key Encryption with Keyword Search Revisited // Gervasi, O., Murgante, B., Laganà, A., Taniar, D., Mun, Y., Gavrilova, M.L. (eds) Computational Science and Its Applications – ICCSA 2008. ICCSA 2008. Lecture Notes in Computer Science, 2008. Vol 5072. P. 1249-1259. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-69839-5_96.

27. Rhee H. S. et al. Improved searchable public key encryption with designated tester // Proceedings of the 4th International Symposium on Information, Computer, and Communications Security. ASIACCS '09. ACM. 2009. P. 376-379. https://doi.org/10.1145/1533057.1533108.

28. Abdalla M., Bellare M., Catalano D., Kiltz E., Kohno T., Lange T., Shi H. Searchable Encryption Revisited: Consistency Properties, Relation to Anonymous IBE, and Extensions // Journal of cryptology, 2008. 21(3). P. 350–391. https://doi.org/10.1007/s00145-007-9006-6.

29. Gentry C. Practical Identity-Based Encryption Without Random Oracles // Vaudenay, S. (eds) Advances in Cryptology – EUROCRYPT 2006. EUROCRYPT 2006. Lecture Notes in Computer Science, 2006. Vol 4004. P. 445–464. Springer, Berlin, Heidelberg. https://doi.org/10.1007/11761679_27.

30. Kiltz E. From selective-ID to full security: The case of the inversion-based Boneh-Boyen IBE scheme. Cryptology ePrint Archive. 2007. URL: https://eprint.iacr.org/2007/033.pdf.

31. Nishide T., Yoneyama K., Ohta K. Attribute-Based Encryption with Partially Hidden Encryptor-Specified Access Structures // Bellovin, S.M., Gennaro, R., Keromytis, A., Yung, M. (eds) Applied Cryptography and Network Security. ACNS 2008. Lecture Notes in Computer Science, 2008. Vol 5037. P. 111-129. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-68914-0_7.

32. Horwitz J., Lynn B. Toward Hierarchical Identity-Based Encryption // Knudsen, L.R. (eds) Advances in Cryptology – EUROCRYPT 2002. EUROCRYPT 2002. Lecture Notes in Computer Science, 2002. Vol 2332. P. 466–481 Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-46035-7_31.

33. Gentry C., Silverberg A. Hierarchical ID-Based Cryptography // Zheng, Y. (eds) Advances in Cryptology — ASIACRYPT 2002. ASIACRYPT 2002. Lecture Notes in Computer Science, 2002, Vol 2501. P. 548–566. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-36178-2_34.

34. Boneh D., Boyen X., Goh EJ. Hierarchical Identity Based Encryption with Constant Size Ciphertext // Cramer R. (eds) Advances in Cryptology – EUROCRYPT 2005. EUROCRYPT 2005. Lecture Notes in Computer Science, 2005. Vol 3494. P. 440–456. Springer, Berlin, Heidelberg. https://doi.org/10.1007/11426639_26.

35. Shi E., Waters B. Delegating Capabilities in Predicate Encryption Systems // Aceto, L., Damgård, I., Goldberg, L.A., Halldórsson, M.M., Ingólfsdóttir, A., Walukiewicz, I. (eds) Automata, Languages and Programming. ICALP 2008. Lecture Notes in Computer Science, 2008. Vol 5126. P. 560–578. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-70583-3_46.

36. Lee K. S., Lee D. H. New techniques for anonymous hibe with short ciphertexts in prime order groups // KSII Transactions on Internet and Information Systems (TIIS). 2010. 4(5). P. 968–988.

37. Boneh D., Waters B. Conjunctive, Subset, and Range Queries on Encrypted Data // Vadhan, S.P. (eds) Theory of Cryptography. TCC 2007. Lecture Notes in Computer Science, 2007. Vol 4392. P. 535–554. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-70936-7_29.

38. Paillier P. Public-Key Cryptosystems Based on Composite Degree Residuosity Classes // Stern J. (eds) Advances in Cryptology – EUROCRYPT '99. EUROCRYPT 1999. Lecture Notes in Computer Science, 1999. Vol 1592. P. 223–238. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-48910-X_16.

39. ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms // IEEE transactions on information theory. 1985. 31(4). P. 469-472. https://doi.org/10.1109/TIT.1985.1057074.

40. Boneh D., Goh EJ., Nissim K. Evaluating 2-DNF Formulas on Ciphertexts // Kilian J. (eds) Theory of Cryptography. TCC 2005. Lecture Notes in Computer Science, 2005. Vol 3378. P. 325–341. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-30576-7_18.

41. Gentry C. Fully homomorphic encryption using ideal lattices // Proceedings of the forty-first annual ACM symposium on Theory of computing. 2009. P. 169-178. https://doi.org/10.1145/1536414.1536440.

42. Gentry C. Computing arbitrary functions of encrypted data //Communications of the ACM. 2010. 53(3). P. 97-105. https://doi.org/10.1145/1666420.1666444.

43. van Dijk M., Gentry C., Halevi S., Vaikuntanatha, V. Fully Homomorphic Encryption over the Integers // Gilbert, H. (eds) Advances in Cryptology – EUROCRYPT 2010. EUROCRYPT 2010. Lecture Notes in Computer Science, 2010. Vol 6110. P. 24–43. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-13190-5_2.

44. Naehrig M., Lauter K., Vaikuntanathan V. Can homomorphic encryption be practical? // Proceedings of the 3rd ACM workshop on Cloud computing security workshop. 2011. P. 113-124. https://doi.org/10.1145/2046660.2046682.

45. Brakerski Z., Vaikuntanathan V. Fully Homomorphic Encryption from Ring-LWE and Security for Key Dependent Messages // Rogaway P. (eds) Advances in Cryptology – CRYPTO 2011. CRYPTO 2011. Lecture Notes in Computer Science, 2011. Vol 6841. P. 505–524. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-22792-9_29.

46. Kamara S., Papamanthou C., Roeder T. Dynamic searchable symmetric encryption // Proceedings of the 2012 ACM conference on Computer and communications security. 2012. P. 965–976.

47. Shen E., Shi E., Waters B. Predicate Privacy in Encryption Systems // Reingold O. (eds) Theory of Cryptography. TCC 2009. Lecture Notes in Computer Science, 2009. Vol 5444. P. 457–473. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-00457-5_27.

48. Song D. X., Wagner D., Perrig A. Practical techniques for searches on encrypted data // Proceeding 2000 IEEE symposium on security and privacy. S&P 2000. IEEE, 2000. P. 44–55. https://doi.org/10.1109/SECPRI.2000.848445.

49. Curtmola R., Garay J., Kamara S., Ostrovsky R. Searchable symmetric encryption: improved definitions and efficient constructions // Journal of Computer Security, 2011. 19(5). P. 895–934.

50. Fiat A., Naor M. Broadcast encryption // Annual International Cryptology Conference. Springer, Berlin, Heidelberg, 1993. P. 480–491.

51. Goh E. J. Secure Indexes. Cryptology ePrint Archive, Report 2003/216. 2003. URL: http://eprint.iacr.org/2003/216/

52. Chang Y. C., Mitzenmacher M. Privacy preserving keyword searches on remote encrypted data // International conference on applied cryptography and network security. Springer, Berlin, Heidelberg, 2005. P. 442–455.

53. Wang Y., Wang J., Chen X. Secure searchable encryption: a survey // Journal of communications and information networks. 2016. 1(4). P. 52–65. https://doi.org/10.11959/j.issn.2096-1081.2016.043.

54. Kamara S., Papamanthou C. Parallel and dynamic searchable symmetric encryption // International conference on financial cryptography and data security. LNCS 7859. Springer, Berlin, Heidelberg, 2013. P. 258–274. https://doi.org/10.1007/978-3-642-39884-1_22.

55. van Liesdonk P., Sedghi S., Doumen J., Hartel P., Jonker W. Computationally Efficient Searchable Symmetric Encryption // Jonker, W., Petković, M. (eds) Secure Data Management. SDM 2010. Lecture Notes in Computer Science. Springer, Berlin, Heidelberg. 2010. Vol 6358. P. 87–100. https://doi.org/10.1007/978-3-642-15546-8_7.

56. Kurosawa K., Ohtaki Y. UC-secure searchable symmetric encryption // International conference on financial cryptography and data security. LNCS. Springer, Berlin, Heidelberg. 2012. Vol. 7397. P. 285–298. https://doi.org/10.1007/978-3-642-32946-3_21..

Надійшла до редколегії 11.05.2022

Відомості про авторів:

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

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

УДК 621.396:004.056 **DOI:10.30837/rt.2022.2.209.15**

А.М. ОЛЕЙНІКОВ, канд. техн. наук, В.А. ПУЛАВСЬКИЙ, канд. техн. наук, І.М. ЧИГІРЬОВ

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ МЕТОДІВ І ЗАСОБІВ ПОДАВЛЕННЯ НЕСАНКЦІОНОВАНОГО ЗАПИСУ МОВИ

Вступ

Актуальність захисту мовної інформації обумовлена в основному двома факторами: перший – мовна інформація має дуже високу інформативність і другий – широке поширення засобів запису мови, починаючи від сучасних смартфонів (на сьогодні у світі їх налічується понад 4 млрд. штук), що мають функцію запису мови, різноманітних диктофонів і закінчуючи спеціальними засобами запису мови, що мають властивості протидії засобам подавлення несанкціонованого запису. На жаль, жоден з відомих сьогодні методів запобігання та подавлення несанкціонованого запису мови не може, без знання типу записуючого пристрою, гарантувати повне недопущення несанкціонованого запису мовної інформації. У статті пропонується метод та на його основі засіб, що істотно підвищує ефективність протидії несанкціонованому запису мовної інформації, незалежно від типу записуючого пристрою.

Технічні вразливості засобів запису мови та методи захисту мовної інформації від несанкціонованого запису

Можливості запобігання несанкціонованому запису мови на звукозаписні засоби базуються на їх технічних вразливостях, які реалізуються за рахунок їх виявлення, а також за рахунок протидії їх штатному функціонуванню.

Класифікація методів захисту від несанкціонованого запису мови представлена на рис. 1 і включає в себе методи виявлення наявності диктофона за його демаскуючими ознаками та методи акустичного, електромагнітного та ультразвукового подавлення несанкціонованого запису.

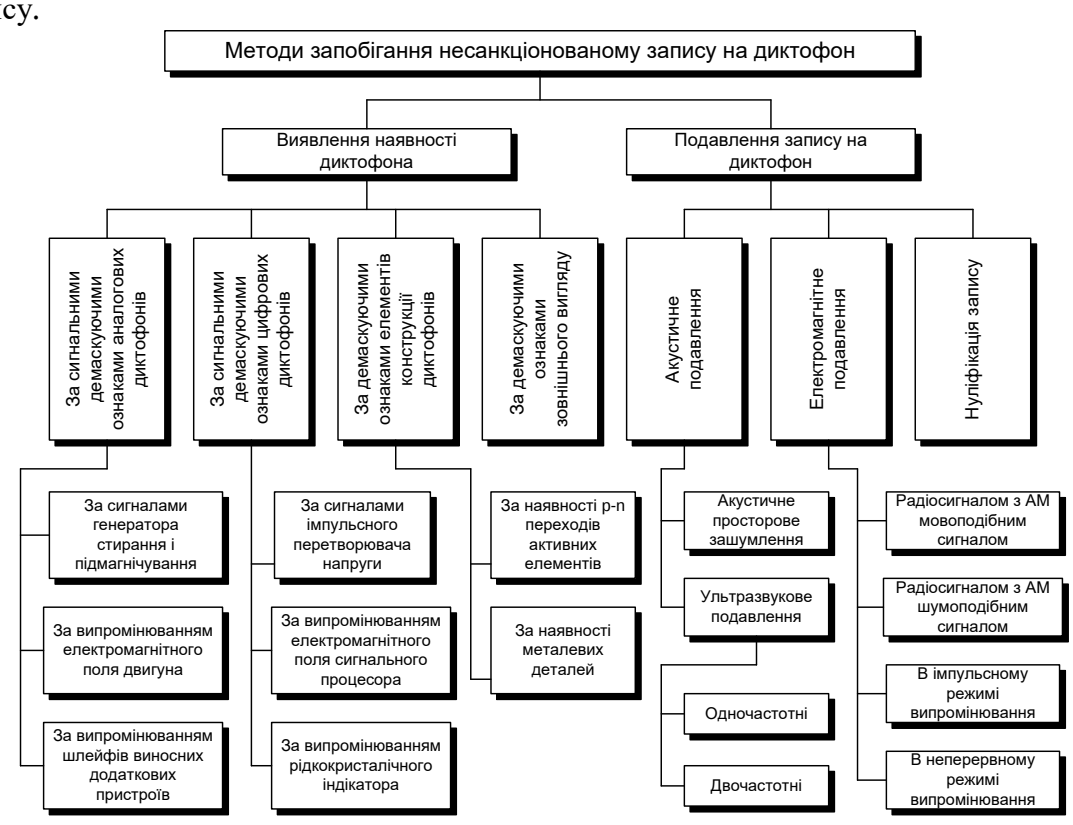


Рис. 1. Методи захисту мовної інформації від несанкціонованого запису

Подавлення несанкціонованого запису мови на диктофон може здійснюватися акустичним, електромагнітним та ультразвуковим методами [1 – 3] .

Акустичний метод подавлення несанкціонованого запису мови в його традиційній інтерпретації заснований на постановці просторової акустичної перешкоди у напрямку можливого розташування пристрою для запису. Збільшення амплітуди акустичної перешкоди не підвищує ефективність захисту, оскільки призводить до мимовільного підвищення гучності розмови обох співрозмовників. З цієї причини до недавнього часу акустичний метод протидії несанкціонованого запису на диктофон вважався *малоефективним*.

Електромагнітний метод полягає у наведенні високочастотного амплітудно-імпульсно-модульованого перешкодного сигналу на провідниках та елементах схеми диктофона як на випадкових антенах. Модулюючим сигналом найчастіше служить мовна або імпульсна перешкода, що збігається по смузі з низькочастотним трактом диктофона. Найбільш схильна до впливу зовнішніх електромагнітних перешкод є підсистема диктофона, відповідальна за перетворення акустичного сигналу. Протидія запису корисного мовного сигналу може проявляється у таких видах:

– наведений високочастотний сигнал детектується на нелінійності мікрофонного підсилювача диктофона. Далі у вигляді низькочастотної речеподібної перешкоди надходить у низькочастотний тракт диктофона і негативно впливає на корисний мовний сигнал;

- перевантаження вхідних каскадів мікрофонного підсилювача перешкодою з великою амплітудою спричинить реакцію схеми автоматичного регулювання підсилення диктофона, внаслідок якої через зменшення посилення корисний сигнал виявиться нижчим за поріг реальної чутливості підсилювача;

- при співвідношенні сигнал/шум близькому до одиниці аналого-цифровий перетворювач диктофона виходить із регламентованого режиму роботи, через що значно погіршується якість сигналу на виході;

- сигнал, наведений на генератор тактової частоти аналого-цифрового перетворювача диктофона, виводить схему з режиму синхронізації, і диктофон перестає нормально функціонувати.

Ефективність електромагнітного подавлення залежить від типу диктофона та її просторового становища стосовно пристрою подавлення. Є залежність уразливості диктофона від несучої частоти перешкодного сигналу до різних типів диктофонів. Пристрої електромагнітного подавлення запису ефективно виконують своє завдання стосовно деяких типів побутових диктофонів. Однак сучасна елементна база і хороше екранування дозволяють багаторазово послабити вплив зовнішньої електромагнітної перешкоди на корисний сигнал у диктофонах, розроблених як спецзасіб знімання акустичної інформації. Це стосується і більшості сучасних смарт-фонів, в яких електромагнітне екранування виконане дуже якісно.

Ультразвуковий метод подавлення використовує засоби, що випромінюють потужні ультразвукові коливання (УЗК). Сучасні звукозаписні пристрої оснащуються, як правило, мікрофонами, верхня межа смуги пропускання яких становить 25 – 27 кГц і потрапляє в ультразвуковий діапазон частот. Застосовують одночастотні та двочастотні ультразвукові подавлювачі.

Одночастотні подавлювачі призначені для протидії несанкціонованому запису для диктофонів, оснащених системою автоматичного регулювання підсилення (АРУ). При реагуванні на потужні ультразвукові сигнали АРУ знижує чутливість диктофона до вхідного мовного сигналу і цим різко знижується якість запису або повністю зривається запис мови.

Двочастотне ультразвукове подавлення базується на формуванні перешкоджаючого сигналу у вигляді двох ультразвукових коливань з рознесенням несучих частот, що співпадає з основною частиною частотного діапазону мовного сигналу (0,3 – 3,4 кГц). При впливі цих двох УЗК на нелінійні елементи мікрофонного підсилювача диктофона утворюються сигнали з комбінаційними (зокрема і різницевими) частотами, що у смугу пропускання звукового

тракту диктофона. Ці комбінаційні сигнали здійснюють енергетичне приховування корисного мовного сигналу в звукозаписному тракті диктофона і цим протидіють несанкціонованому запису мови.

Системи ультразвукового подавлення виявляються неефективними або взагалі марними, якщо мікрофон записуючого пристрою:

- має частотну характеристику лише звукового діапазону (без заходу в ультразвукову область, наприклад, у диктофонах старих років випуску);

-захищений спеціальним тканинним матеріалом (або просто знаходиться у кишені одягу);

- має спеціальний фільтр, що обмежує смугу вхідного сигналу межами мовного діапазону.

Враховуючи сказане можна зробити висновок про те, що акустична, електромагнітна та ультразвукова протидія без апріорного знання типу диктофона не забезпечує гарантованого подавлення несанкціонованого запису мови.

Адаптація акустичного методу для підвищення ефективності подавлення несанкціонованого запису мовлення

Для суттєвого підвищення ефективності подавлення запропоновано адаптувати акустичний метод з урахуванням особливостей поширення акустичних коливань у повітрі, психофізичного сприйняття звуків вухом людини та поліпшенням технічних характеристик акустичної системи пристрою подавлення, а саме:

- відстань між джерелом акустичної перешкоди та місцем ймовірного розташування диктофона необхідно звести до мінімуму і зробити його меншим, ніж відстань між джерелом мови та диктофоном;

- формувати акустичну перешкоду з промови співрозмовників. Така речеподібна перешкода не може бути відфільтрована, оскільки займає ту ж саму смугу частот, що і мовний сигнал;

- суттєво покращити технічні параметри акустичної системи для випромінювання мовної перешкоди, застосувавши електростатичну акустичну систему випромінювання перешкоди, відмовившись від використання традиційних електродинамічних випромінювачів, що призведе:

- до підвищення лінійності частотної характеристики акустичної системи;

- зменшення величини її нелінійних спотворень;

- звуження діаграму спрямованості акустичної системи.

Ці зміни технічних параметрів акустичної системи дозволять максимально наблизити спектральні характеристики перешкод до голосів співрозмовників. А звуження діаграми спрямованості електростатичної акустичної системи при однаковій випромінюючої потужності призведе до:

- збільшення щільності потоку потужності перешкодного сигналу, що підвищує ефективність подавлення запису мови;

- деякого зниження інтенсивності впливу перешкодного сигналу на органи слуху співрозмовників через просторову орієнтацію акустичного випромінювача на можливе місце розташування записуючого пристрою в одязі відвідувача.

Результати експериментального дослідження ефективності адаптованого акустичного методу подавлення несанкціонованого запису мови

Для оцінки ефективності адаптованого акустичного методу подавлення несанкціонованого запису мови з використанням перешкоди, сформованої електростатичним випромінювачем, було проведено два експерименти:

- перший – порівняння зони подавлення пристроїв з електростатичним та динамічним випромінюванням;

- другий – порівняння технічних параметрів засобів захисту від несанкціонованого запису мови побудованих з використанням адаптованого акустичного (EST-ST, EST-P), електромагнітного (Шумотрон – 3, PD – 2) та ультразвукового (USPD-C, UltraSonic-50) методів подавлення для п'яти сучасних типів звукозаписних пристроїв – цифрових диктофонів та смартфонів (Olimpus VP-20, Edic-mini B76, Galaxy S8+, Iphone Xs Max, Iphone 12 Pro Max).

Для першого експерименту використовувався електростатичний випромінювач з розмірами сторін 25 на 34 см за умов відкритого простору.

Окрема колонка відтворювала записану людську мову. Електростатичний випромінювач (а потім окремо динамічний випромінювач) відтворював подібну перешкоду, зформовану з мови людини з рівнем 65 дБ на відстані 1 метр. Акустичні вимірювання проводилися сертифікованим мікрофоном Behringer ECM8000 із нормованою частотною характеристикою та круговою діаграмою спрямованості. Зона подавлення визначалася за розбірливістю мови на тлі перешкоди при різних кутах і дальності ℓ з використанням методу експертної оцінки.

На рис. 2 представлені зони подавлення пристрою протидії з використанням електростатичного та динамічного випромінювача, які являють собою усічені еліпси з півосями 1,6 та 0,3 метра та 0,5 та 0,4 метра відповідно. Перевагу використання електростатичного випромінювача наочно видно.

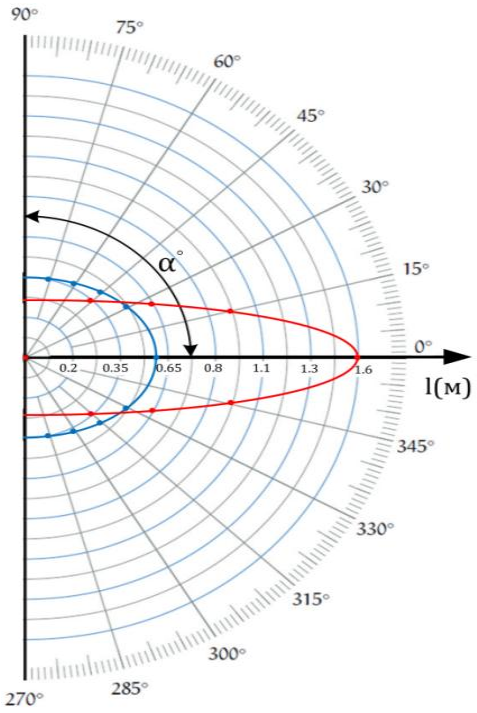


Рис. 2. Зони подавлення пристрою протидії несанкціонованого запису мови з використанням електростатичного та динамічного випромінювача

Результати другого експерименту представлені в табл. 1 – 4.

У табл. 1 наведено дальності повного подавлення диктофонів при використанні *електромагнітних* подавлювачів «ШУМОТРОН-3» та «PD-2».

Таблиця 1

Модель	**Шумотрон – 3** Потужність випромінювання 15Вт	**PD – 2** Потужність випромінювання 8Вт
Olimpus VP-20	2,2 м	1,6м
Edic-mini B76	0,6м	0,2м
Galaxy S8+	0,3м	0,1м
Iphone Xs Max	0м	0м
Iphone 12 Pro Max	0м	0м

У табл. 2 наведено дальність повного подавлення диктофонів при використанні *ультразвукових* подавлювачів.

Таблиця 2

Модель	**USPD-C** 26 випромінювачів з акустичним тиском 115дБ	**UltraSonic-50** 50 випромінювачів з акустичним тиском 115дБ
Olimpus VP-20	0,9 м	1,2м
Edic-mini B76	1,1м	1,3м
Galaxy S8+	6м	8м
Iphone Xs Max	1,8м	2,4м
Iphone 12 Pro Max	2,2м	3м

У табл. 3 наведено дальності повного подавлення диктофонів ультразвуковими пригнічувачами за умови закриття їх мікрофона кишеньковою матерією (диктофон знаходиться в кишені).

Таблиця 3

Модель	**USPD-C** 26 випромінювачів з акустичним тиском 15дБ	**UltraSonic-50** 50 випромінювачів з акустичним тиском 115дБ
Olimpus VP-20	0,1 м	1,1м
Edic-mini B76	0,2м	0,3м
Galaxy S8+	0,4м	0,5м
Iphone Xs Max	0,15м	0,2м
Iphone 12 Pro Max	0,2м	0.25м

У табл. 4 наведено дальності повного подавлення диктофонів при використанні електростатичних подавлювачів "EST-ST" та "EST-P".

Таблиця 4

Модель	**EST-ST** Акустична чутливість 88дБ	**EST-P** Акустична чутливість 86дБ
Olimpus VP-20	3,5 м	3,2м
Edic-mini B76	2,8м	2,6м
Galaxy S8+	2,4м	2,4м
Iphone Xs Max	2,2м	2м
Iphone 12 Pro Max	1,8м	2м

При закритті мікрофонів кишеньковою матерією дальність подавлення перерахованих диктофонів не змінюється.

Висновки

Запропонований адаптований акустичний метод протидії несанкціонованого запису мови однаково ефективний для будь-яких типів записуючих пристроїв, оскільки перешкода формується по функціональному каналу – акустичному з урахуванням особливостей поширення та сприйняття акустичних коливань людиною у повітрі.

Список літератури:

1. Гудков С.А. Проблемы и решения задачи обнаружения современных диктофонов // Специальная техника. 2001. №3. С. 37-43
2. Антіпов І.Є., Олейніков А.М., Ликов Ю.В., Кукуш В.Д., Милютченко І.О. Засоби та системи технічного захисту інформації: Навчальний посібник для студентів ЗВО. Харків : ХНУРЕ, 2019. 216 с.
3. Олейников А.Н., Пулавский В.А., Цыбулевский П.В. Оценка эффективности акустического противодействия несанкционированной записи на диктофон // Современная защита информации. Киев, 2010, №1. С. 8-16.
4. Олейников А.Н., Пулавский В.А., Кривенко М.А. Ультразвуковые методы защиты речевой информации // Радиотехника. 2012. Вып. 169. С. 176-181.

Надійшла до редколегії 02.03.2022

Відомості про авторів:

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

Пулавський Володимир Антонович – канд. техн. наук, директор, фирма «Пулавський», м. Харків, Україна; e-mail: pulavskiy.v@gmail.com; ORCID: https://orcid.org/0000-0002-9976-9439

Чигірьов Іван Миколайович – студент факультета інформаційних радіотехнологій та технічного захисту інформації; Харківський національний університет радіоелектроніки, Україна; e-mail: ivan.chyhirov@nure.ua

УДК 621.396.967.2 **DOI:10.30837/rt.2022.2.209.16**

І.В. СВИД, канд. техн. наук, В.В. СЕМЕНЕЦЬ, д-р техн. наук,
О.С. МАЛЬЦЕВ, М.Г. ТКАЧ, С.В. СТАРОКОЖЕВ, О.О. ДАЦЕНКО, І.О. ШЕВЦОВ

ПОРІВНЯЛЬНИЙ АНАЛІЗ МЕТОДІВ ВИЗНАЧЕННЯ КООРДИНАТ ПОВІТРЯНИХ ОБ'ЄКТІВ СИСТЕМАМИ ШИРОКОЗОНОВОЇ МУЛЬТИЛАТЕРАЦІЇ

Вступ

Основним джерелом даних про повітряну обстановку в системі контролю повітряного простору є системи радіолокаційного спостереження (СРЛС). Системи радіолокаційного спостереження забезпечують незалежне спостереження та визначають місце розташування повітряного об'єкта (ПО) за допомогою засобів наземного базування. Прикладом незалежного спостереження є первинні оглядові радіолокатори (ПОРЛ) [1 – 3], вторинні оглядові радіолокатори (ВОРЛ) [2 – 6], системи ідентифікації за ознакою «свій-чужий» (ІСЧ) (Identification Friend or Foe) (IFF) [7 – 9], а також багатопозиційні радіолокатори (БПРЛ). Багатопозиційні радіолокатори, залежно від джерела отримання сигнальних даних, можуть базуватися як на первинному, так і на вторинному оглядових радіолокаторах. БПРЛ, що базується на базі ПОРЛ [10 – 13], має передавач, що випромінює зондувальний сигнал, а ехо-сигнали приймають приймальні (невипромінюючі) пункти, які рознесені на деяку відстань. В даний час широкого поширення набувають БПРЛ, що базуються на принципі Multiple-input multiple-output (MIMO) [14 – 16] технології. Використання сигналів запиту (СЗ) літакових відповідачів вторинної радіолокації (ВРЛ) та ІСЧ систем дозволяє створювати багатопозиційні системи радіолокаційного спостереження, які отримали назву MLAT [16 – 18] або WAM [19 – 23]. При цьому слід зазначити, що є можливість визначення координат ПО при випромінюванні сигналу запиту як своїм запитувачем, так і при випромінюванні сигналів запиту іншими запитувачами, що входять в мережу систем ВОРЛ.

БПРЛ, що базуються на базі ВОРЛ (ІСЧ), залежно від площі територіального обслуговування поділяються на Multilateration (MLAT) [16 – 18] та Wide Area Multilateration (WAM) [18, 20 – 23].

В даний час спостерігається тенденція поєднання MLAT у «широко зонові» (Wide Area Multilateration) інтегровані системи [21 – 24]. Одна з головних переваг пасивної локації, що характерно для MLAT і WAM – можливість виявляти навіть такі цілі, що важко помічаються, як літаки, обладнані покриттями, що поглинають зондуючі сигнали, і засобами протирадарного маскування.

При залежному кооперативному спостереженні розташування визначається на борту ПО. Ці інформаційні дані передаються підсистемі локального спостереження поряд з можливими додатковими даними, використовуючи як свої засоби передачі інформації, так і супутникові канали передачі інформації. Прикладом залежного спостереження є концепція залежного автоматичного спостереження (Automatic dependent surveil-lance – ADS) [25-29]. ADS – концепція, заснована на наявності двосторонніх ліній передачі даних "повітря-земля", за якими інформаційні дані про ПО, включаючи місцезнаходження, час та інші дані автоматично передається на землю відповідному споживачеві.

Виходячи з наведеного, можна зробити висновок, що всі системи кооперативного спостереження являють системи передачі даних за принципом запит-відповідь [30 – 34]. Справді, вони містять канал передачі сигналів запиту і канал передачі сигналів відповіді. Для кодування інформації в цих системах застосовуються примітивні інтервально-часові та позиційні коди [35 – 39], що суттєво знижує інформаційну ємність каналів передачі даних, що розглядаються [40 – 45].

Принципи та методи реалізації багатопозиційного спостереження повітряного простору у системі контролю повітряного простору

Багатопозиційні радіолокаційні системи [12, 13, 46 – 51] широко застосовуються для оцінки розташування об'єктів у просторі і стали серйозними конкурентами традиційних радіолокаційних систем огляду повітряного простору. Залежно від масштабу завдань системи мультилатерації діляться на локальні, за якими закріпилася назва MLAT-систем, і глобальні, які називаються WAM-системами.

У системах MLAT розташування ПО визначається на основі оцінки відстаней об'єкта до довільного числа опорних радіонавігаційних точок, в яких розміщені приймачі, здатні приймати сигнали, що випромінюються літаковим відповідачем ВОРЛ. Слід розрізняти активний та пасивний режими роботи систем БПРЛ. В активному режимі запит на борт надсилається передавачем самої системи в одному з форматів A/C/S вторинної радіолокації. У пасивному режимі запит на борт надходить від стороннього джерела, яким може бути один із ВОРЛ. У цьому випадку, оскільки джерело сигналу запиту ніяк не синхронізовано з системою, приймачі опорних радіонавігаційних точок здійснюють прослуховування ефіру, виявлення сигналу відповіді з борту та вимірювання псевдодальностей, подібно супутниковим навігаційним системам. Можна стверджувати, що MLAT – це технологія, що дозволяє визначати розташування літаків або інших транспортних засобів без використання спеціального, додаткового обладнання, передаючи при цьому мінімальний обсяг даних [17, 18]. Процес визначення розташування ПО заснований на різниці в часі приходу сигналу, випромінюваного об'єктом (ПО) у напрямку приймальних станцій системи MLAT (TDOA – Time Difference of Arrival – різниця у часі приходу). Система MLAT служить альтернативою класичним станціям радіолокації, так як вирішує завдання перекриття великої території за допомогою приймальних станцій, які можна розташувати на місцевості та нарощувати їх кількість. Крім цього, система адаптується в місцях зі складним рельєфом, за рахунок низьких витрат на її встановлення та обслуговування. Інформаційні дані про координати ПО оновлюються кожну секунду, що підвищує ситуаційну поінформованість диспетчерів, а це у свою чергу підвищує безпеку польотів, пропускну здатність та ефективність.

При цьому слід зазначити, що система MLAT забезпечує високу точність визначення місця розташування ПО і має таку перевагу, як відсутність "мертвих" зон, які притаманні класичним станціям радіолокації.

Однак при реалізації системи MLAT необхідно враховувати такі фактори:

- конфігурація (розташування приймальних станцій та їх кількість) впливає на точність позиціонування ПО;

- розміщення приймальних станцій повинно здійснюватися з урахуванням можливості забезпечення електроживленням і технічним обслуговуванням.

Приймальні станції багатопозиційної системи спостереження приймають сигнали відповідачів ПО, декодують їх і передають на сервер-концентратор повідомлення, що містять декодовану відповідь і час отримання сигналу. Щоб визначити місцезнаходження ПО необхідно зафіксувати час отримання сигналу кожної станції. Для визначення моменту надходження сигналу на приймаючі станції, системі потрібен єдиний опорний час. Зазвичай це досягається одним із двох способів:

1) всі отримані сигнали направляються на центральну обробну станцію для отримання часової позначки за загальним годинником. У цьому випадку система повинна обчислити час проходження повідомлення між кожною приймальною станцією та центральною станцією та внести відповідні корективи. Система передає повідомлення між центральною та приймальними станціями для контролю та коригування часу проходження;

2) годинники на всіх приймачах синхронізують за загальним опорним часом, зокрема, за глобальними навігаційними супутниковими системами GNSS (Global Navigation Satellite Systems), або з використанням передавача у відомому місці [52 – 54]. Відстань між таким передавачем і станціями, що приймають, відома, так що за допомогою відстеження часу

надходження сигналів від цього передавача на кожну приймальну станцію можна вносити корективи з метою підтримки синхронізації годинників приймачів.

Завдання визначення розташування об'єкта на площині або в просторі полягає у обчисленні геометричних величин, що характеризують його розташування. До цих величин відносяться довжина шляху поширення радіохвиль від об'єкта або дальність та напрямок на цей ПО. Для визначення координат використовується, як правило, різницево-далекомірний метод. Координати визначаються за різницям моментів приходу сигналу в рознесені приймальні пункти. У цьому випадку визначення місця розташування ПО можна здійснювати за сукупністю наявних вимірів.

У загальному випадку визначення параметрів траєкторного руху ПО здійснюється при вирішенні рівнянь, що описують дальність, які можна представити в наступному виді:

$$R_i = c\tau_i(t) = \sqrt{(x_i - x)^2 + (y_i - y)^2 + (z_i - z)^2}, \quad (1)$$

де D_i – геометрична дальність від приймального пункту до ПО; x, y, z – координати розташування ПО; $\tau_i(t) = t_{i+1} - t_i$ – тривалість часового інтервалу між моментами часу t_{i+1} та t_i (час затримки сигналу); c – швидкість поширення радіохвиль.

Як правило, виміряне значення дальності (1) містить помилку вимірювання, що дозволяє D_i подати наступним чином:

$$D_i = D_{ist.i} + \Delta D_i,$$

де $D_{ist.i}$ – справжнє значення дальності ПО до i-го приймального пункту; ΔD_i – помилка виміру дальності, яку можна надати наступним виразом:

$$\Delta D_i = \Delta D_{\text{sinh},i} + \Delta D_{sl.i} + \Delta D_{trop,i}, \quad (2)$$

де $\Delta D_{\text{sinh},i}$ – систематична похибка, обумовлена нестабільністю бортового еталону часу та частоти; $\Delta D_{sl.i}$ – випадкова складова помилки виміру дальності; $\Delta D_{trop,i}$ – похибка, обумовлена рефракцією в тропосфері.

Похибку вимірювання (2) можна представити в наступному виді:

$$\Delta D_i = \Delta D_{post,i} + \Delta D_{fl,i}; \quad \Delta \dot{D}_{post,i} = 0; \quad \Delta \dot{D}_{fl,i} = -\frac{1}{\tau_{Di}} \Delta D_{fl,i} + \frac{1}{\tau_{Di}} w_{Di},$$

де $\Delta D_{post,i}$ – постійна складова похибки; $\Delta D_{fl,i}$ – флуктуаційна складова похибки; τ_{Di} – час кореляції; w_{Di} – формуючий білий гаусівський шум з відомими характеристиками.

У багатопозиційній системі спостереження (рис. 1) вимірюються незалежні значення τ_{01}, τ_{02}, τ_{03} різниці часу поширення сигналів від ПО до центрального (опорного) пункту через рознесені пункти прийому (RP1, RP2, RP3).

Для визначення розташування ПО необхідно обчислити дві координати x_{ao}, y_{ao}. Вихідними даними для обчислення координат ПО є координати периферійних станцій x_i, y_i і різниця дальностей ΔD на незалежних базах d_{01}, d_{02}, d_{03}:

$$\Delta D_{1,2} = \sqrt{(x_2 - x_{vo})^2 - (y_2 - y_{vo})^2} - \sqrt{(x_1 - x_{vo})^2 - (y_1 - y_{vo})^2}.$$

Координати периферійних станцій отримуємо за допомогою карти, а саме: геодезичні довготу L і широту B.

Геодезичні координати переводяться з геодезичної в прямокутну декартову геоцентричну систему координат:

$$\begin{vmatrix} x \\ y \\ z \end{vmatrix} = \begin{vmatrix} (N+h)\cos B\cos L & 0 & 0 \\ 0 & (N+h)\cos B\sin L & 0 \\ 0 & 0 & (N+h)-e^2 N\sin B \end{vmatrix},$$

де x, y, z – координати станції у прямокутній геоцентричній системі координат; h – висота над поверхнею еліпсоїда; $e=\sqrt{a^2-b^2}/a$ – ексцентриситет земного еліпсоїда; $N=a\left(1-e^2\sin^2 B\right)^{-1/2}$ – радіус кривизни першого вертикалу; $a=6\,378\,136$ м, $b=6\,356\,777$ м.

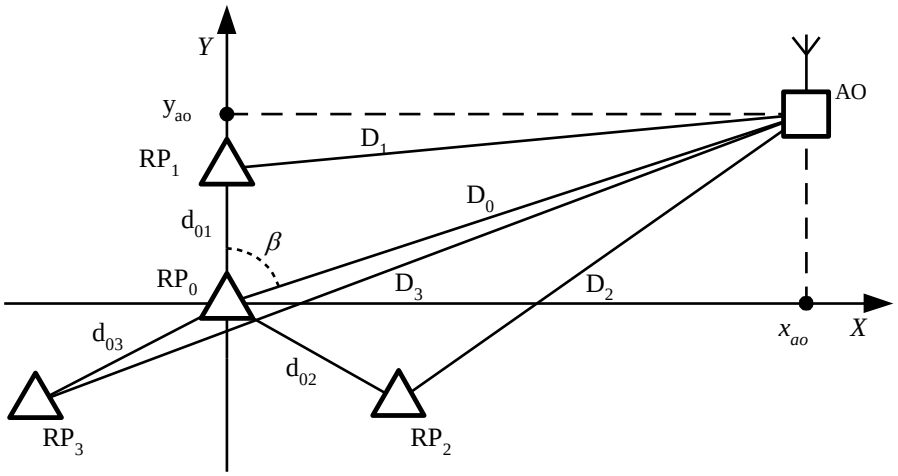


Рис. 1. Конфігурація різницево-далекомірної системи

Завдяки цим розрахункам отримуємо прямокутні координати для оцінки просторового розташування станцій. Вони використовуються для визначення розташування об'єктів у межах поля аеродрому, інші вирішують завдання навігації ПО у галузі простору, що має протяжність у сотні кілометрів на поверхні Землі та десятки кілометрів над цією поверхнею.

Одним із завдань при створенні систем мультилатерації є синтез алгоритмів оцінки розташування ПО у двовимірному (MLAT-системи) або тривимірному (WAM-системи) просторі. Прийнято виділяти три класи методів оцінки розташування у багатопозиційних системах: статистичні, чисельні та алгебраїчні. Статистичні методи враховують випадковий характер оцінок параметрів сигналів і припускають синтез оцінок розташування на основі методу максимальної правдоподібності. Ці методи найбільш близькі до оптимальних, проте вони не дозволяють отримати пряме рішення і вимагають застосування оптимального пошуку екстремуму досить складної цільової функції у просторі, розмірність якого дорівнює кількості координат об'єкта. Численні методи також використовують методи оптимального пошуку розв'язання деякої оптимізаційної задачі, проте на відміну від статистичних методів пошук проходить у просторі меншої розмірності при простій цільовій функції. Оцінки, одержувані цими методами, у загальному випадку є зміщеними та неоптимальними у статистичному сенсі. Алгебраїчні методи не враховують імовірнісний характер даних, проте вони є прямими, оскільки дозволяють отримати оцінки координат ПО рішенням деякої лінійної системи рівнянь. Останнє робить зазначені методи особливо привабливими для практичного застосування, незважаючи на те, що методи цієї категорії не можуть претендувати на оптимальність. Таким чином, алгоритм оцінки розташування ПО в системах MLAT повинен бути комбінацією алгоритмів, що належать зазначеним категоріям, що дозволить поєднувати високу точність і обчислювальну ефективність.

Показники якості оцінки точності розташування повітряних об'єктів системами багатопозиційного спостереження повітряного простору

Системи багатопозиційного спостереження повітряного простору складаються з кількох розподілених наземних приймальних станцій та їх точність оцінки координат повітряних об'єктів істотно залежить від геометричного розподілу приймальних станцій (Geometrical Dilution of Precision) (GDOP) та від закону зміни висоти (Horizontal Dilution of Precision) (HDOP). Можна стверджувати, що MLAT та WAM – це метод локалізації гіперболи або гіперболоїду. В цьому випадку точність оцінки координат повітряних об'єктів пов'язана з помилкою вимірювання різниці часу запізнення (TDOA [22, 54]), а також геометричного розташування приймальних пунктів багатопозиційної системи і може бути оцінена так:

$$\sigma_s = \sigma_T G,$$

де σ_s – точність позиціонування системи MLAT; σ_T – точність вимірювання TDOA [22, 54]; G – геометричний розподіл приймальних станцій GDOP [54].

GDOP визначає схему розташування станції і впливає на точність позиціонування всієї багатопозиційної системи. Саме ця обставина вказує на те, що спосіб зменшення значення GDOP дуже важливий для контролю точності всієї багатопозиційної системи. Він визначає набір рівнянь для вимірювання різниці у часі прибуття сигналів на рознесені приймальні пункти багатопозиційної системи. Якщо припустити, що $\vec{x} = \left\| r_x \quad r_y \quad r_z \right\|^T$ – вектор просторового розташування ПО, $\vec{x}_i = \left\| r_{xi} \quad r_{y_i} \quad r_{z_i} \right\|^T$ – вектор положення i-ї наземної приймальної станції багатопозиційної системи, в якій є N приймальних станцій. У цьому випадку для N приймальних станцій матрична форма сформована за допомогою набору вищенаведених співвідношень для вимірювання часу набуває виду

$$\vec{T}_m = \vec{T}_0 + \frac{\vec{r}}{c} + \vec{n}, \tag{3}$$

де c – швидкість поширення сигналу; $\vec{T}_m$ – виміряне значення часу, протягом якого сигнал досягне приймальної станції; $\vec{T}_0$ – час передачі сигналу повітряним об'єктом; $\vec{r}$ – відстань від повітряного об'єкта до приймальної станції; $\vec{n}$ – шум виміру.

Якщо припустити, що середнє значення шумів вимірювання дорівнює нулю і вони не залежать один від одного, то матриця коваріаційного виразу (3) набуває виду

$$\vec{P}_n = E\left[\vec{n} \cdot \vec{n}^T \right].$$

У аналізованих багатопозиційних системах, зазвичай, використовується алгоритм різниці у часі прибуття (TDOA) для гіперболічної локалізації. Отже для того, щоб у виразі (3) виключити загальний параметр T_0, розглянемо різницю в часі для набору рівнянь:

$$T_{m(i-1)} - T_{mi} = \left(r_{i-1} - r_i\right) \Big/ c + \left(n_{i-1} - n_i\right),$$

де i знаходиться в діапазоні $2...N$. Це відповідає $(N-1)$ формулам різниці в часі прибуття сигналів на приймальні пункти багатопозиційної системи, що розглядається.

Використовуючи векторну матрицю для виразу значень різниці шуму виміру в багатопозиційній системі, що розглядається, можна записати:

$$\begin{Vmatrix} n_1 - n_2 \\ n_1 - n_2 \\ . \\ n_1 - n_2 \end{Vmatrix} = \begin{Vmatrix} 1 & -1 & 0 & ... & 0 \\ 0 & 1 & -1 & ... & 0 \\ . & . & . & ... & . \\ 0 & 0 & 0 & .. & 1 & -1 \end{Vmatrix} \begin{Vmatrix} n_1 \\ n_2 \\ . \\ n_N \end{Vmatrix} = \vec{H}\vec{n} .$$

У цьому випадку коваріаційна матриця різниці в часі прибуття сигналів на приймальні пункти може бути визначена з виразу

$$\vec{P}_\Delta = E\left\| \left(\vec{H}\vec{n}\right)\left(\vec{H}\vec{n}\right)^T \right\| = \vec{H}P_n\vec{H}^T .$$

За допомогою методу найменших квадратів, а також методу лінійної оцінки вимірювання та локалізація різниці в часі коваріаційної матриці отримуємо співвідношення

$$\vec{P}_x = E\left\| \left(\hat{x} - x\right)\left(\hat{x} - x\right)^T \right\| = c^2 \left\| F^T T^T \left(\vec{H}P_n\vec{H}^T\right)^{-1} YF \right\|^{-1} = \begin{Vmatrix} \sigma_{r_x}^2 & 0 & 0 \\ 0 & \sigma_{r_y}^2 & 0 \\ 0 & 0 & \sigma_{r_z}^2 \end{Vmatrix}, \quad (4)$$

де σ_{r_X}, σ_{r_y}, σ_{r_Z} – стандартні відхилення помилок вимірювання у напрямках координат x, y и z.

Одиничний вектор опорної точки x_0 до приймальної станції записується у такому виді:

$$\vec{F} = \begin{Vmatrix} \frac{r_{x0} - r_{x1}}{r_{01}} & \frac{r_{y0} - r_{y1}}{r_{01}} & \frac{r_{z0} - r_{z1}}{r_{01}} \\ \frac{r_{x0} - r_{x2}}{r_{02}} & \frac{r_{y0} - r_{y2}}{r_{02}} & \frac{r_{z0} - r_{z2}}{r_{02}} \\ . & . & . \\ \frac{r_{x0} - r_{xN}}{r_{0N}} & \frac{r_{y0} - r_{yN}}{r_{0N}} & \frac{r_{z0} - r_{zN}}{r_{0N}} \end{Vmatrix}.$$

У цьому випадку використовуючи вираз (4) і визначення GDOP отримуємо наступний вираз для оцінки GDOP:

$$G = \sqrt{\sigma_{r_x}^2 + \sigma_{r_y}^2 + \sigma_{r_z}^2} . \quad (5)$$

Відповідно похибки визначення горизонтального та вертикального положення описуються за допомогою HDOP та VDOP у вигляді виразів (6) та (7) відповідно

$$H = \sqrt{\sigma_{r_x}^2 + \sigma_{r_y}^2} , \quad (6)$$

$$V = \sqrt{\sigma_{r_z}^2} , \quad (7)$$

де H представляє HDOP; V представляє VDOP.

Слід зазначити, що для широкосмугових маршрутів та зони терміналу HDOP контролює точність горизонтальної локалізації, а VDOP – вертикальну точність локалізації. Чим більше значення HDOP та VDOP, тим нижче буде точність локалізації повітряного об'єкта.

Порівняльний аналіз якості вирішення координатного завдання системами широкозонового багатопозиційного спостереження

Як правило, відомі системи широкозонового багатопозиційного спостереження для оцінки координат повітряних об'єктів використовують різницево-далекомірний метод. Однак реалізація систем WAM дозволяє використовувати інші методи оцінки розташування повітряних об'єктів, що випромінюють сигнали відповіді за каналом вторинної радіолокації. Розрізняють три основні способи визначення координат об'єктів, що випромінюють у зазначеному радіодіапазоні: кутомірний, різницево-далекомірний, кутомірно-різницево-далекомірний, кутомірно-сумарно-далекомірний.

При кутомірному методі встановлюється тільки напрямок ПО за допомогою двох (або більше) приймальних пунктів, рознесених на відстань b. Для визначення координат ПО у тривимірному просторі необхідно вимірювати не менше трьох кутових координат. У двох пунктах слід виміряти два азимути та один кут місця або два кути місця та один азимут.

Нехай виміряні два азимути та один кут місця (рис. 2).

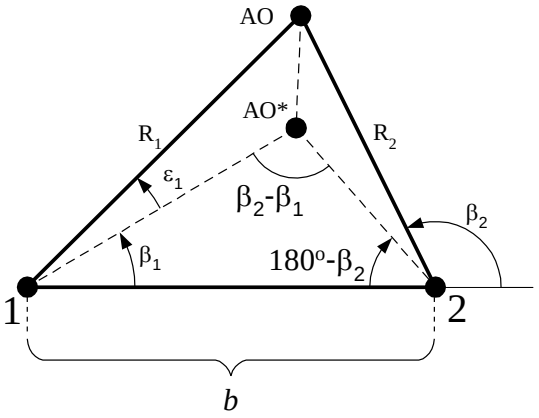


Рис. 2. Визначення похилої дальності за двома азимутами та одним кутом місця

В даному випадку можна показати, що

$$R_1 = \frac{b\sin\beta_2}{\cos\varepsilon_1 \cdot \sin(\beta_2 - \beta_1)}; \quad R_2 = \sqrt{b^2 + R_1^2 - 2bR_1\cos\varepsilon_1\cos\beta_1}.$$

Якщо виміряні два кути місця і один азимут. В цьому випадку маємо:

$$R_2 = R_1\frac{\sin\varepsilon_1}{\sin\varepsilon_2}. \; R_1^2\left(\frac{\sin^2\varepsilon_1}{\sin^2\varepsilon_2} - 1\right) + 2r_1 b\cos\varepsilon_1\cos\beta_1 - b^2 = 0., \tag{8}$$

З (8) знаходимо

$$R_1 = \frac{-b\cos\varepsilon_1\cos\beta_1 + b\sqrt{\cos^2\varepsilon_1\cos^2\beta_1 + \left(\frac{\sin^2\varepsilon_1}{\sin^2\varepsilon_2} - 1\right)}}{\frac{\sin^2\varepsilon_1}{\sin^2\varepsilon_2} - 1}.$$

Кутомірно-різницево-далекомірний метод поєднує в собі кутомірний і різницево-далекомірний методи. Він полягає у визначенні напрямків та різниці відстаней від радіо-

випромінюючого об'єкта до пункту радіотехнічної системи. При цьому треба мати щонайменше два приймальних пункти (рис. 3).

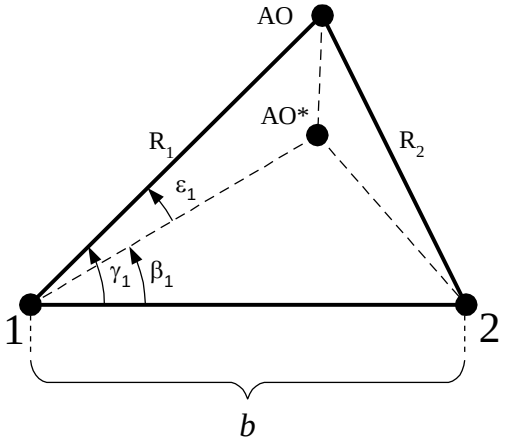


Рис. 3. Кутомірно-різницево-далекомірний метод визначення похилих дальностей

Наступні формули дозволяють обчислити похилі дальності кутомірно-різницево-далекомірним методом при різних визначеннях різниці відстаней від ПО до приймального пункту:

$$R_1 = \frac{b^2 - \Delta R_2^2}{2\left(b\cos\varepsilon_1 \cdot \cos\beta_1 + \Delta R_2\right)}, \quad R_2 = \frac{b^2 + \Delta R_2^2 + 2b\Delta R_2 \cos\gamma_1}{2\left(b\cos\varepsilon_1 \cdot \cos\beta_1 + \Delta R_2\right)};$$

або

$$R_1 = \frac{b^2 - \Delta R_2^2}{2\left(b\cos\varepsilon_1 \cdot \cos\beta_1 - \Delta R_1\right)}, \quad R_2 = \frac{b^2 + \Delta R_1^2 - 2b\Delta R_1 \cos\gamma_1}{2\left(b\cos\varepsilon_1 \cdot \cos\beta_1 - \Delta R_1\right)};$$

де $R_2 = R_1 + \Delta R_2$ або $R_2 = R_1 + \Delta R_2$.

Представлені методи оцінки координат ПО, що випромінюють сигнали відповіді каналами вторинної радіолокації, відносяться до основних.

Проведемо порівняльний аналіз розглянутих вище методів розв'язання координатного завдання системою WAM. Для проведення порівняльної оцінки різних методів вирішення завдання інформаційного забезпечення розглядатимемо наступний вектор стану ПО:

$$\vec{W} = \left\| x \quad y \right\|^T.$$

Крім того, будемо вважати, що похибка оцінки точності місцеположення ПО, що входить до нього, має нульове середнє значення і наступну матрицю коваріацій вимірювань оцінюваних координат ПО:

$$\vec{P} = \left\| \begin{matrix} \sigma_x^2 & \sigma_{xy} \\ \sigma_{xy} & \sigma_y^2 \end{matrix} \right\|^T. \tag{9}$$

Точність вирішення координатного завдання аналізованими методами будемо характеризувати площею еліпсів похибок оцінювання вектора стану $\vec{W}$, яка визначається як корінь квадратний з детермінанта матриці коваріації, що в загальному випадку еквівалентна HDOP:

$$S = \sqrt{\det \vec{P}} = \sqrt{\sigma_x^2\sigma_y^2 - \sigma_{xy}^2}.$$

Для порівняння точнісних характеристик різних методів вирішення координатної задачі будемо обчислювати квадратні корні з детермінантів коваріаційних матриць, що відображають площу еліпсів похибок, тобто:

$$\mu = P_2 / P_1 . \tag{10}$$

З урахуванням (9) вираз (10) можна записати як

$$\mu = \sqrt{(\sigma_{x_2}^2 \sigma_{y_2}^2 - \sigma_{x_2 y_2}^2) / (\sigma_{x_1}^2 \sigma_{y_1}^2 - \sigma_{x_1 y_1}^2)} . \tag{11}$$

Отримаємо вирази для коваріаційних матриць розглянутих вище методів розв'язання задачі інформаційного забезпечення системами WAM.

Для кутомірного методу вектор спостережуваних параметрів $\vec{\alpha} = \|\beta_1 \quad \beta_2 \quad \beta_3\|^T$ включає три азимути ПО із рознесених пунктів прийому системи WAM. Перерахунок кутових похибок у похибки положення дає такі результати:

$$\frac{1}{\sigma_x^2} = \left(1 - \rho_{xy}^2\right) H_{1i}, \quad \frac{1}{\sigma_y^2} = \left(1 - \rho_{xy}^2\right) H_{2i}, \quad \rho_{xy} = -\left(\sum_{i=1}^{3} \frac{(x - x_i)(y - y_i)}{r_i^4 \sigma_{\beta_i}^2} \right) \Big/ \sqrt{H_{1i} H_{2i}} . \tag{12}$$

де $H_{1i} = \sum_{i=1}^{3} \frac{(y - y_i)^2}{r_i^4 \sigma_{\beta_i}^2}$; $H_{2i} = \sum_{i=1}^{3} \frac{(x - x_i)^2}{r_i^4 \sigma_{\beta_i}^2}$; $r_i = \sqrt{(x - x_i)^2 + (y - y_i)^2}$.

На рис. 4, на підставі обчислень виразів (12), представлено лінії рівної площі еліпсів похибок за результатами рівноточної пеленгації з трьох пунктів прийому, розташованих на одній прямій, рівній дальності від центрального пункту прийому. Наведені розрахунки показують, що похибки оцінки координат збільшуються з віддаленням ПО від бази та від нормалі до бази.

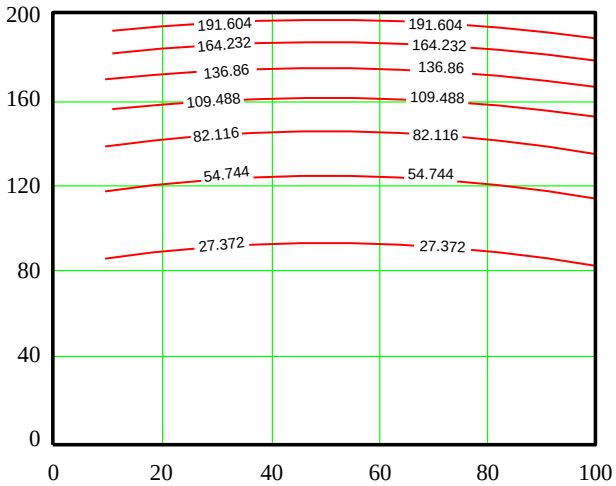


Рис. 4. Оцінка точності кутомірного методу

Фізично низька точність кутомірного методу пояснюється низькою точністю вимірювання кутових координат, а швидке зростання похибок при віддаленні від лінії бази – збільшенням похибок визначення площинних координат при віддаленні від приймального пункту при постійній точності вимірювання кутових координат.

Для кутомірно-далекомірного методу оцінки координат ПО вектор спостережуваних параметрів $\vec{\alpha} = \|r \quad \beta\|^T$ характеризує дві полярні координати, що визначаються за пунктом прийому системи WAM, а вектор стану – дві декартові координати на площині $\vec{W} = \|x \quad y\|^T$. Припустимо, що вимірювання параметрів вектора параметрів, що спостерігаються, здійснюються з нульовим середнім значенням і дисперсіями вимірюваних параметрів σ_r^2 та σ_β^2. Також будемо вважати, що похибки вимірювань дальності r та β азимуту малі відносно дійсних значень вимірюваних величин.

При зазначених припущеннях похибки вимірювання координат повітряних об'єктів мають нульові середні значення, а вираз, що визначає еліпс помилок, можна записати як

$$\frac{1}{\sigma_x^2} = \left(1-\rho_{xy}^2\right)\left[\frac{x^2}{r^2\sigma_r^2} + \frac{y^2}{r^4\sigma_\beta^2}\right],\ \frac{1}{\sigma_y^2} = \left(1-\rho_{xy}^2\right)\left[\frac{x^2}{r^4\sigma_\beta^2} + \frac{y^2}{r^2\sigma_r^2}\right],\ \rho_{xy} = -\frac{xy\left(\frac{1}{\sigma_r^2} - \frac{1}{r^2\sigma_\beta^2}\right)}{\sqrt{H_3 H_4}}, \qquad (13)$$

де $H_3 = \frac{x^2}{\sigma_r^2} + \frac{y^2}{r^2\sigma_\beta^2}$; $H_4 = \frac{x^2}{r^2\sigma_\beta^2} + \frac{y^2}{\sigma_r^2}$.

На рис. 5, на підставі обчислень за виразом (13), представлено лінії рівної площі еліпсів помилок за результатами кутомірно-далекомірних вимірів. Представлені розрахунки показують значне поліпшення точності вимірювання координат ПО при використанні кутомірно-далекомірного методу.

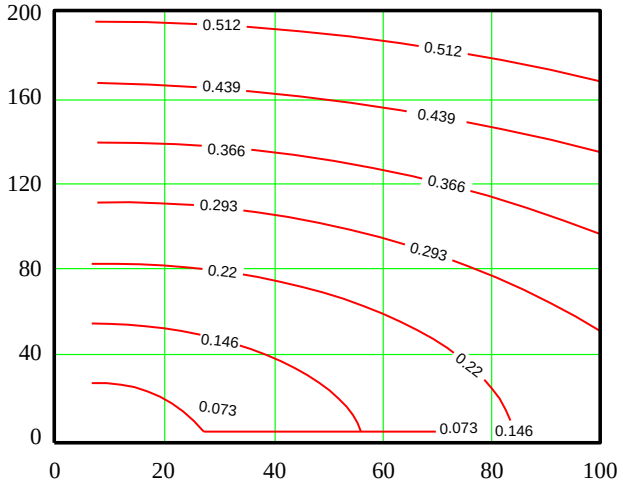


Рис. 5. Оцінка точності кутомірно-далекомірного методу

На рис. 6 представлено порівняльні показники якості вимірювання координат кутомірним та кутомірно-далекомірним методами.

Результати розрахунків (рис. 6) показують, що використання активних систем WAM дозволяє реалізувати вимірювання координат ПО на одному приймальному пункті та підвищити точність вимірювання координат в десятки-сотні разів.

До недоліків кутомірно-далекомірного методу відноситься низька енергетична прихованість, що обумовлена просторовим поєднанням запитувача ВОРЛ та приймального пункту. Для збереження енергетичної скритності ВОРЛ переходять до кутомірно-сумарно-далекомірного методу.

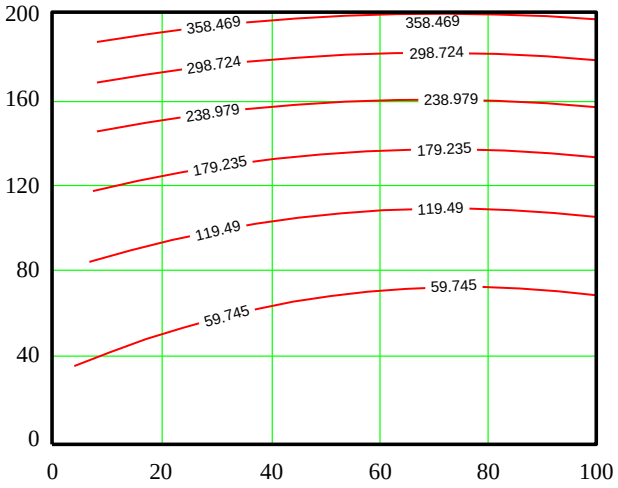


Рис. 6. Порівняльна оцінка точності кутомірного та кутомірно-далекомірного методу

В кутомірно-сумарно-далекомірному методі наземний запитувач рознесений на відстань бази b із приймальним пунктом, що дозволяє зберегти основну перевагу системи – енергетичну скритність. Координатна задача вирішується на приймальному пункті системи WAM за однією з двох множин параметрів, що вимірюються: (ρ,Θ_r) або (ρ,Θ_T), де $\rho = R_r + R_T$ – сумарна відстань за маршрутом запитувач-ПО-приймальний пункт, R_r – відстань від запитувача до ПО, R_T – відстань від ПО до приймального пункту, Θ_r, Θ_T – азимут ПО, виміряний відповідно на пунктах випромінювання та прийому системи WAM. Таким чином, рознесення запитувача та приймального пункту виключає демаскування системи WAM та розширює кількість множин первинних вимірювань. Зазначимо, що реалізація кутомірно-сумарно-далекомірного методу обчислення координат ПО можлива завдяки використанню несанкціонованого запиту літакового відповідача (ЛВ).

Розрахуємо точність вимірювання площинних декартових координат ПО при використанні першої та другої множин первинних вимірювань у припущенні фіксованих похибок вимірювань. Припустимо, що результати вимірів полярних координат ρ, Θ_r, Θ_T спотворені білим гаусовим шумом з нульовими середніми значеннями σ_r^2 та дисперсіями $\sigma_{\Theta r}^2$ $\left(\sigma_{\Theta T}^2\right)$. Вважатимемо, що похибки вимірювань ρ та Θ_r (Θ_T) малі відносно їхніх істинних значень.

При використанні першої множини вимірювань (ρ,Θ_r) полярні координати ρ та Θ_r виміряні WAM, перераховуються в координати прямокутної системи X та Y за наступними виразами:

$$X = \frac{\rho^2 \cos\Theta_r + \rho b}{2\left(b\cos\Theta_r + \rho\right)}, \quad Y = \frac{\left(\rho^2 + b^2\right)\sin\Theta_r}{b\cos\Theta_r + \rho}.$$

При зазначених припущеннях похибки вимірювання декартових координат X та Y мають нульові середні значення, а їх дисперсії і коваріація становлять:

$$\sigma_x^2 = \frac{\left(H_1^2\sigma_r^2 + H_2^2\sigma_\Theta^2\right)}{H_3^4}, \ \sigma_y^2 = \frac{\left(H_4^2\sigma_r^2 + H_5^2\sigma_\Theta^2\right)}{H_3^4}, \ \sigma_{xy}^2 = \frac{\left(H_1H_4\sigma_r^2 + H_2H_5\sigma_\Theta^2\right)}{H_3^4},$$

де $H_1 = 2\rho b\cos^2\Theta_r + \left(\rho^2 + b^2\right)\cos\Theta_r$, $H_2 = \left(b^2 - \rho^2\right)\rho\sin\Theta_r$, $H_3 = 2\left(b\cos\Theta_r + b\right)$,

$$H_4 = \rho^2 \sin 2\Theta_r + \left(\rho^2 + b^2\right)\cos\Theta_r,\ H_5 = \left(\rho^2 + b^2\right)\left(\rho\cos\Theta_r + b\right).$$

При використанні другої множини вимірювань $\left(\rho, \Theta_T\right)$ декартові координати ПО X та Y розраховуються на підставі виразів:

$$X = \frac{b/2 - 0.5\rho\cos\Theta_T}{\left(b/\rho\cos\Theta_T - 1\right)}, \quad Y = \frac{\left(b^2/2\rho\right)\sin\Theta_T}{b/\rho\cos\Theta_T - 1}. \tag{14}$$

Якщо припустити, що похибки визначення декартових координат ПО за виразами (14) мають нульові середні значення, тоді їх дисперсії та коваріації становлять:

$$\sigma_x^2 = \frac{b\cos\Theta_T}{2} - b\rho\cos^2\Theta_T + \left(\frac{\rho^2\cos\Theta_T}{2}\right)^2 \sigma_r^2 + \frac{b^2}{2}\rho\sin\Theta_T$$

$$-\left(\frac{\rho^2\cos\Theta_T}{2}\right)^2 \sigma_\Theta^2 \frac{1}{\left(b\cos\Theta_T - \rho\right)^4};$$

$$\sigma_y^2 = \frac{\rho^2\sin\Theta_T}{2} - \frac{b\rho^2\sin\Theta_T}{2} + \left(\frac{\rho^2\cos\Theta_T}{2}\right)^2 \sigma_r^2 + \frac{b^2}{2}\rho\sin\Theta_T -$$

$$-\left(\frac{\rho^2\cos\Theta_T}{2}\right)^2 \sigma_\Theta^2 \frac{1}{\left(b\cos\Theta_T - \rho\right)^4};$$

$$\sigma_{xy} = \left\{\left[\left(\frac{b^2\cos\Theta_T}{2} - b\rho\cos^2\Theta_T + \frac{\rho^2\cos\Theta_T}{2}\right)\times\right.\right.$$
$$\left.\left.\times\left(\frac{\rho^2\sin\Theta_T}{2} - \frac{b\rho\sin 2\Theta_T}{2} + \frac{b^2\sin\Theta_T}{2}\right)\right]\sigma_r^2 + \left[\left(\frac{b^2\rho\sin\Theta_T}{2} - \frac{\rho^3\sin\Theta_T}{2}\right)\times\right.$$
$$\left.\left.\left(\frac{b^3}{2} - \frac{b}{2}\right)\rho^2 + \left(\frac{\rho^3}{2} - \frac{b^2}{2}\right)\rho\cos\Theta_T\right]\sigma_\Theta^2\right\}$$
$$\times\frac{1}{\left(b\cos\Theta_T - \rho\right)^4}.$$

Для реалізації кутомірно-сумарно-далекомірного методу на приймальному пункті системи WAM необхідно знати момент випромінювання сигналів запиту, що істотно ускладнює технічну реалізацію системи WAM. Однак наявність засобів формування та передачі синхросигналів дозволяє в даний час створити синхронну мережу з ВОРЛ і приймальних пунктів системи WAM. Таким чином, можна стверджувати, що аналізована структура системи WAM найбільш ефективна, оскільки дозволяє реалізувати досить високу точність вимірювання координат ПО за рахунок несанкціонованого використання ЛВ і реалізувати енергетично приховану систему WAM. Реалізувати переваги високої точності вимірювання координат ПО за рахунок несанкціонованого використання ЛВ та необхідності створення синхронної мережі можливо за рахунок кутомірно-різницево-далекомірного методу оцінки координат ПО.

В кутомірно-різницево-далекомірному методі система WAM включає два приймальні пункти, рознесені на відстань бази b, та винесений запитувач, який може не входити до складу системи WAM. Запитувач ВОРЛ випромінює сигнали запиту без імпульсу подавлення бічних пелюсток через слабоспрямовану антенну систему та забезпечує несанкціонований запит літакового відповідача у всьому просторі вирішення координатної задачі системою

WAM. Вектор вимірюваних параметрів включає один азимут ПО та різницю відстаней $\Delta r = r - r_1$ від літакового відповідача до приймальних пунктів. Тому кутомірно-різницево-далекомірній системі WAM не потрібно знати ні просторових координат запитувача, ні моменту випромінювання сигналів запиту.

Припустимо, що результати вимірювань азимуту та різниці відстаней спотворені білим гаусовим шумом з нульовими середніми значеннями та дисперсіями σ_β^2 та $\sigma_{\Delta r}^2$. Вважатимемо, що похибки вимірювань β та Δr малі відносно їхніх істинних значень.

При зазначених припущеннях похибки визначення декартових координат ПО мають нульові середні значення, а еліпс помилок можна визначити з формул:

$$\frac{1}{\sigma_x^2} = \left(1-\rho_{xy}^2\right)\left[\frac{1}{\sigma_{\Delta r}^2}\left(\frac{b}{r_1}-\frac{x\Delta r}{rr_i}\right)^2+\frac{y^2}{r^4\sigma_\beta^2}\right],\quad \frac{1}{\sigma_y^2} = \left(1-\rho_{xy}^2\right)\left[\frac{1}{\sigma_{\Delta r}^2}\left(\frac{y\Delta r}{rr_i}\right)^2+\frac{x^2}{r^4\sigma_\beta^2}\right],$$

$$\rho_{xy} = \frac{\frac{1}{\sigma_{\Delta r}^2}\left(\frac{b}{r_1}-\frac{x\Delta r}{rr_i}\right)\frac{y\Delta r}{rr_1}+\frac{xy}{r^4\sigma_\beta^2}}{\sqrt{\left[\frac{1}{\sigma_{\Delta r}^2}\left(\frac{b}{r_1}-\frac{x\Delta r}{rr_i}\right)^2+\frac{y^2}{r^4\sigma_\beta^2}\right]\left[\frac{1}{\sigma_{\Delta r}^2}\left(\frac{y\Delta r}{rr_i}\right)^2+\frac{x^2}{r^4\sigma_\beta^2}\right]}}.$$

Лінії рівної площі еліпсів похибок за результатами кутомірно-різницево-далекомірному вимірі, розраховані на підставі згаданих виразів, наведено на рис. 7.

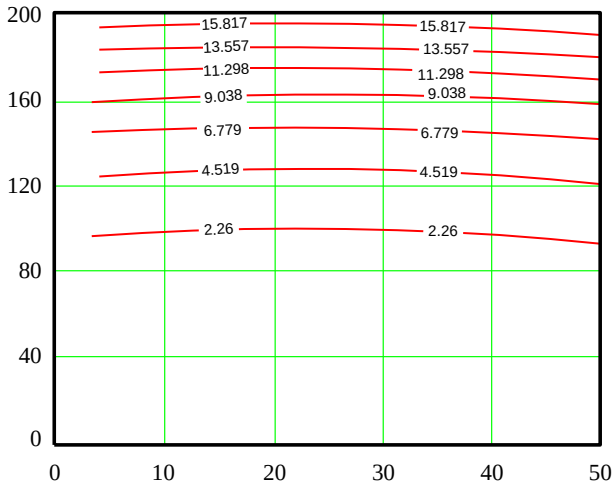


Рис. 7. Точність кутомірно-різницево-далекомірного методу

З рис. 7 видно, що кутомірно-різницево-далекомірний метод WAM забезпечує вирішення координатної задачі з прийнятною точністю, що в п'ять-десять разів вище, ніж кутомірний метод. Крім того, виключення запитувача зі складу системи WAM дозволяє одночасно зберегти енергетичну скритність системи WAM при відносно нескладній технічній реалізації. Аналогічні результати можна отримати з аналізу точності інших методів вирішення координатної задачі системами WAM із несанкціонованим запитом літакового відповідача. Таким чином, літаковий відповідач ВОРЛ є доступним джерелом інформації для виявлення ПО та визначення їх координат системами WAM зацікавленою стороною. Для цього можуть використовуватися наявні повністю пасивні системи WAM.

Висновки

Можливості систем WAM значно зростають при використанні принципів побудови ВОРЛ, як несинхронної мережі, та літакового відповідача, як відкритої одноканальної системи масового обслуговування з обслуговуванням першого, правильно прийнятого сигналу запиту. Несанкціонований запит літакового відповідача дозволяє перейти від повністю пасивних методів виявлення та визначення координат повітряного об’єкта до активно-пасивних, що забезпечують збільшення точності розв'язання координатного завдання у десятки-сотні разів зі збереженням енергетичної скритності системи WAM. Отримані результати, з одного боку, свідчать про необхідність застосування в сучасних системах WAM несанкціонованого запиту літакового відповідача ВОРЛ, а з іншого – показують повну відсутність енергетичної скритності існуючих ВОРЛ.

За результатами проведеного дослідження можна зробити наступні висновки:

- використання активних систем WAM значно розширює кількість методів розв'язання задач інформаційного забезпечення споживачів системи контролю повітряного простору;

- несанкціоноване використання літакових відповідачів ВОРЛ дозволяє визначити оцінку координат повітряного об’єкта як однопозиційним, так і багатопозиційним методами;

- порівняльний аналіз методів вирішення координатної задачі оцінки розташування повітряного об'єкта показав, що точність оцінки координат повітряного об’єкта в системі WAM, що розглядається, значно вище точності вимірювання координат в існуючих системах WAM.

Список літератури:

1. A. Koutny and M. Pelant, "Multi-channel degarbling method for SSR replies", 2017 18th International Radar Symposium (IRS), 2017. doi: 10.23919/irs.2017.8008171.

2. M. Abdalla, M. Barbary, M. Amin and M. El-Ghonami, "Design and Implementation of Proposed Low-Cost Dual-Channel IF Receiver for SSR", 2020 12th International Conference on Electrical Engineering (ICEENG), 2020. doi: 10.1109/iceeng45378.2020.9171699.

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

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

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

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

7. I. Svyd, I. Obod, O. Maltsev, I. Shtykh, G. Maistrenko and G. Zavolodko, "Comparative Quality Analysis of the Air Objects Detection by the Secondary Surveillance Radar", 2019 IEEE 39th International Conference on Electronics and Nanotechnology (ELNANO), 2019. doi: 10.1109/elnano.2019.8783539.

8. Á. Jarama, J. López-Araquistain, G. Miguel and J. Besada, "Complete Systematic Error Model of SSR for Sensor Registration in ATC Surveillance Networks", Sensors, vol. 17, no. 10, p. 2171, 2017. doi: 10.3390/s17102171.

9. O. Peker and D. Akdur, "A Method for Elimination of False IFF Target Reports by Using ISLS and RSLS Techniques", 2019 Signal Processing Symposium (SPSympo), 2019. doi: 10.1109/sps.2019.8881951.

10. L. Bowden, "The story of IFF (Identification Friend or Foe)", IEE Proceedings A Physical Science, Measurement and Instrumentation, Management and Education, Reviews, vol. 132, no. 6, p. 435, 1985. doi: 10.1049/ip-a-1.1985.0079.

11. E. El-Badawy, W. EL-Masry, M. Mokhtar and A. Hafez, "A secured chaos encrypted mode-S aircraft identification friend or foe (IFF) system", 2010 4th International Conference on Signal Processing and Communication Systems, 2010. doi: 10.1109/icspcs.2010.5709756.

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

13. І. Обод, І. Свид, О. Мальцев. Обробка даних радіолокаційних систем спостереження повітряного простору : навчальний посібник. Харків : Друкарня Мадрид, 2021. 255 с.

14. Q. He, N. Lehmann, R. Blum and A. Haimovich, "MIMO Radar Moving Target Detection in Homogeneous Clutter", IEEE Transactions on Aerospace and Electronic Systems, vol. 46, no. 3, pp. 1290-1301, 2010. doi: 10.1109/taes.2010.5545189.

15. Q. He and R. Blum, "Diversity Gain for MIMO Neyman–Pearson Signal Detection", IEEE Transactions on Signal Processing, vol. 59, no. 3, pp. 869-881, 2011. doi: 10.1109/tsp.2010.2094611.

16. J. Liu, J. Han, Z. Zhang and J. Li, "Target detection exploiting covariance matrix structures in MIMO radar", Signal Processing, vol. 154, pp. 174-181, 2019. doi: 10.1016/j.sigpro.2018.07.013.

17. S. Pleninger, "The Testing of MLAT Method Application by means of Usage low-cost ADS-B Receivers", MAD – Magazine of Aviation Development, vol. 2, no. 7, p. 8, 2014. doi: 10.14311/mad.2014.07.02.

18. S. Lo and P. Enge, "Capacity Study of Multilateration (MLAT) based Navigation for Alternative Position Navigation and Timing (APNT) Services for Aviation", Navigation, vol. 59, no. 4, pp. 263-279, 2012. doi: 10.1002/navi.25.

19. M. Garcia, R. Mueller, E. Innis and B. Veytsman, "An enhanced altitude correction technique for improvement of WAM position accuracy", 2012 Integrated Communications, Navigation and Surveillance Conference, 2012. doi: 10.1109/icnsurv.2012.6218375.

20. I. Obod, I. Svyd, O. Maltsev, G. Zavolodko and S. Leonov, "WAM Systems: Comparative Analysis of Information Support Quality", 2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T), 2020. doi: 10.1109/picst51311.2020.9468085.

21. J. Stefanski, "Asynchronous wide area multilateration system", Aerospace Science and Technology, vol. 36, pp. 94-102, 2014. doi: 10.1016/j.ast.2014.03.016.

22. D. He, X. Lu, W. Wang and J. Su, "Analysis of Wide Area Multilateration Localization Accuracy Under Different Stations Layout ond Aircraft Height", DEStech Transactions on Engineering and Technology Research, no., 2017. doi: 10.12783/dtetr/iceta2016/7068.

23. M. Leeson, Error Analysis for a Wide Area Multilateration System, Qinet-iQ/C&IS/ADC/520896/7/19, 2006.

24. G. de Miguel Vela, J. B. Portas and J. G. Herrero, "Correction of propagation errors in Wide Area Multilateration systems," 2009 European Radar Conference (EuRAD), 2009, pp. 81-84.

25. J. Florez Zuluaga, J. Vargas Bonilla, J. Ortega Pabon and C. Suarez Rios, "Radar Error Calculation and Correction System Based on ADS-B and Business Intelligent Tools", 2018 International Carnahan Conference on Security Technology (ICCST), 2018. doi: 10.1109/ccst.2018.8585728.

26. B. Syd Ali, W. Ochieng, A. Majumdar, W. Schuster and T. Kian Chiew, "ADS-B System Failure Modes and Models", Journal of Navigation, vol. 67, no. 6, pp. 995-1017, 2014. doi: 10.1017/s037346331400037x.

27. S. Ramasamy, R. Sabatini and A. Gardi, "Cooperative and non-cooperative sense-and-avoid in the CNS+A context: A unified methodology", 2016 International Conference on Unmanned Aircraft Systems (ICUAS), 2016. doi: 10.1109/icuas.2016.7502676.

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

29. I. Obod, I. Svyd, O. Maltsev, O. Vorgul, G. Maistrenko and G. Zavolodko, "Optimization of the Quality of Information Support for Consumers of Cooperative Surveillance Systems", Data-Centric Business and Applications, pp. 133-155, 2020. doi: 10.1007/978-3-030-43070-2_8.

30. I. Obod, I. Svyd, O. Maltsev, G. Maistrenko, O. Zubkov and G. Zavolodko, "Bandwidth Assessment of Cooperative Surveillance Systems", 2019 3rd International Conference on Advanced Information and Communications Technologies (AICT), 2019. doi: 10.1109/aiact.2019.8847742.

31. I. Obod, I. Svyd, O. Maltsev, O. Vorgul, G. Maistrenko and G. Zavolodko, "Optimization of Data Transfer in Cooperative Surveillance Systems", 2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), 2018. doi: 10.1109/infocommst.2018.8632134.

32. I. Svyd, I. Obod, O. Maltsev, T. Okachova and G. Zavolodko, "Optimal Request Signals Detection in Cooperative Surveillance Systems", 2019 IEEE 2nd Ukraine Conference on Electrical and Computer Engineering (UKRCON), 2019. doi: 10.1109/ukrcon.2019.8879840.

33. J. Qumar, S. Christopher and R. Bhattacharjee, "Target detection with transmitters identity waveform for multi-dynamic radar scenario", 2017 IEEE Calcutta Conference (CALCON), 2017. doi: 10.1109/calcon.2017.8280730.

34. I. Svyd, I. Obod, O. Maltsev, O. Vorgul, I. Vorgul and I. Shevtsov, "Method for Increasing the Interference Immunity of the Channel for Measuring of the Short-Range Navigation Radio System", 2022 IEEE 16th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), 2022. doi: 10.1109/tcset55632.2022.9767069.

35. I. Svyd, I. Obod, O. Maltsev, O. Vorgul, V. Chumak and A. Sierikov, "Analysis of the Impact of Interference on the Time Position of Signals in Requesting Airspace Observation Systems", 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T), 2021. doi: 10.1109/picst54195.2021.9772138.

36. I. Svyd, I. Obod, O. Maltsev, O. Vorgul, V. Chumak and B. Bakumenko, "Estimation of the Spatial Coordinates of Air Objects in Synchronous Radar Networks for Airspace Observation", 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T), 2021. doi: 10.1109/picst54195.2021.9772227.

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

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

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

40. І.І. Обод, В.В. Шевцова. Відносна пропускна спроможність запитальних систем передачі інформації системи контроля повітряного простору // Системи обробки інформації. 2013. № 2(109). С. 74-76.
41. V. Zhyrnov, S. Solonskaya, and I. Shubin, “Evaluation of radar image processing efficiency based on intelligent analysis of processes”, RT, vol. 4, no. 207, pp. 83–88, 2021. doi: 10.30837/rt.2021.4.207.09.
42. Обод И.И. Помехоустойчивые системы вторичной радиолокации. Москва : ЦИНТ, 1998. 118 с.
43. І.І. Обод, В.В. Шевцова. Пропускна спроможність відповідачів запитальних систем передачі польотної інформації // Системи обробки інформації. 2013. № 1(108). С. 105-108.
44. И.И. Обод. Управление потоками сигналов в несинхронных сетях запросных систем вторичной локации // Радиоэлектроника и информатика. 1998. № 2. С. 4-5.
45. И.И. Обод. Сравнительная оценка помехоустойчивости несинхронных и синхронных сетей запросных систем вторичной локации // Вестник ХГПУ. 1998. № 15. С. 58-61.
46. И.И. Обод, В.В. Глущенко, И.В. Коваль. Методы повышения помехоустойчивости самолетных ответчиков запросных систем вторичной локации // Вестник ХГПУ. 1999. № 34. С. 84-86.
47. И.И. Обод. Повышение эффективности систем управления воздушного движения за счет реализации разнесенных систем вторичной радиолокации // Радиоэлектроника и информатика. 1997. Вып. 1. С. 63-64.
48. Б.В. Бакуменко, І.І. Обод. Методи підвищення завадозахищеності запитувальних радіотехнічних систем // Системи обробки інформації. 2006. № 9(58). С. 10-12.
49. І.І. Обод, О.О. Стрельницький, В.А. Андрусевич. Структура та показники якості обробки інформації систем спостереження повітряного простору // Системи обробки інформації. 2013. № 8 (115). С. 80-83.
50. M. K. Abdul-Hussein, O. Strelnytskyi, I. Obod, I. Svyd and H. Alrikabi, "Evaluation of the Interference’s Impact of Cooperative Surveillance Systems Signals Processing for Healthcare", International Journal of Online and Biomedical Engineering (iJOE), vol. 18, no. 03, pp. 43-59, 2022. doi: 10.3991/ijoe.v18i03.28015
51. М. Ткач, «Оцінка відносної пропускної здатності літакових відповідачів вторинних радіолокаційних систем спостереження повітряного простору», Радіотехніка, № 207, 2021, С. 123-131.
52. W.C. Young; Ming-Ten Tsai; Li-Min Chuang. Air traffic control system management. Proceedings of the IEEE 2000 National Aerospace and Electronics Conference. NAECON 2000. Engineering Tomorrow (Cat. No.00CH37093). doi: 10.1109/NAECON.2000.894952.
53. Jiang Chaoshu; Liu Changzhong; Wang Xuegang. GPS synchronized wide area multilateration system. 2009 International Conference on Communications, Circuits and Systems. DOI: 10.1109/ICCCAS.2009.5250465
54. Y. Sun, F. Zhang and Q. Wan, "Wireless sensor network-based localization method using TDOA measurements in MPR", IEEE Sensors J., vol. 19, no. 10, pp. 3741-3750, Jan. 2019.

Надійшла до редколегії 30.05.2022

Відомості про авторів:

Свид Ірина Вікторівна – кандидат технічних наук, доцент, завідувач кафедри мікропроцесорних технологій і систем, Харківський національний університет радіоелектроніки, Україна; email: iryna.svyd@nure.ua; ORCID: http://orcid.org/0000-0002-4635-6542

Семенець Валерій Васильович – доктор технічних наук, професор, професор кафедри мікропроцесорних технологій і систем, Харківський національний університет радіоелектроніки, Україна; email: valery.semenets@nure.ua; ORCID: https://orcid.org/0000-0001-8969-2143

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

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

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

Даценко Олександр Олександрович – аспірант кафедри мікропроцесорних технологій і систем, Харківський національний університет радіоелектроніки, Україна; email: oleksandr.datsenko@nure.ua; ORCID: https://orcid.org/0000-0002-6685-0070

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

УДК 621.396.677.494 **DOI:10.30837/rt.2022.2.209.17**

А.І. КОВАЛЕНКО, канд. техн. наук, С.В. ТІТОВ, канд. техн. наук,
О.В. ТІТОВА, канд. техн. наук, О.С. ЧОРНА, канд. техн. наук

ОЦІНКА ВИМОГ ДО ПАРАМЕТРІВ СИГНАЛІВ ПРИ V-ПОДІБНОМУ РОЗПОДІЛІ ЧАСТОТ У МАТЕМАТИЧНІЙ МОДЕЛІ БАГАТОПОЗИЦІЙНОЇ СИСТЕМИ ВИПРОМІНЮВАЧІВ

Вступ

Подальший розвиток ефективних радіотехнічних систем різного призначення, наприклад: засобів локації ближньої дії, спеціальних систем зв'язку між об'єктами в заданих локальних областях простору, систем передачі енергії НВЧ-променем та формування в локальній області простору високої щільності електромагнітної енергії – стало можливим завдяки використанню фокусування електромагнітного випромінювання [1 – 5].

При цьому найбільші можливості та гнучкість управління параметрами сфокусованого електромагнітного випромінювання (ЕМВ) забезпечуються за допомогою різних систем випромінювачів, наприклад, багатопозиційної системи випромінювачів (БСВ). Як відомо, можливі різні способи управління фокусуванням ЕМВ, класифікація яких дана у [6, 14]. Аналіз різних методів управління просторовим розподілом струмів по апертурі БСВ для формування просторово-часових імпульсів (ПЧІ) у заданій точці спостереження, проведений у [5, 6], показав, що найбільш ефективні методи фокусування ЕМВ на основі взаємоузгодженого просторово-фазово-частотного (ПФЧ) та просторово-фазово-частотно-часового управління. А для локалізації ЕМВ у заданому кутовому напрямку без сканування доцільно використовувати методи фокусування на основі ПФЧ-управління з використанням V-подібного закону розподіл частот за апертурою БСВ.

Однак флуктуації параметрів сигналів і антен, що виникають через різні випадкові фактори, обмежують їх потенційні можливості і можуть призвести до істотних змін сфокусованих просторово-часових імпульсів, зниження їх пікової потужності. У зв'язку з цим викликає інтерес вивчення та обґрунтування вимог до параметрів сигналів, що випромінюються, при використанні різних методів фокусування ЕМВ.

Ціль статті – статистичне дослідження впливу різних випадкових та детермінованих змін електричних та конструктивних параметрів антен, систем управління сигналами, що випромінюються, при V-подібному розподілі частот по апертурі БСВ на рівень пікової потужності, тривалість та період повторення сфокусованих імпульсів.

Основні припущення

Як було показано в [6], для формування послідовності сфокусованих ПЧІ необхідно встановити закон розподілу амплітуд, початкових фаз і частот сигналів по апертурі БСВ. При цьому повинні підтримуватись умови синфазного складання полів від усіх випромінюючих елементів у вибраній точці фокусування. Параметри закону ПФЧ управління повинні бути стабільними протягом часу, рівного усередненій тривалості імпульсів на виході випромінювачів при формуванні одиночного ПЧІ, а при формуванні послідовності імпульсів – протягом тривалості цієї пачки ПЧІ. Це накладає певні вимоги до точності та стабільності параметрів закону ПФЧ управління сигналами. Тому виникає необхідність дослідження впливу різноманітних відхилень від заданих значень параметрів закону ПФЧ управління сигналами, що випромінюються, в каналах БСВ при формуванні послідовностей ПЧІ. При цьому необхідно досліджувати також вплив помилок в установці заданої дискретності початкової фази та частоти на характеристики ПЧІ, що формуються.

Вплив типових помилок виготовлення традиційних антен та елементів антенно-фідерного тракту на характеристики поля випромінювання досить добре розглянуто у [1, 8, 9]. Тому розглянемо лише особливості вимог до точності розташування фазових центрів випромінювачів та вимоги до дискретності та точності установки початкових фаз та несучих частот по апертурі БСВ, специфічні для ПФЧ фокусування на основі V-подібних розподілів частот.

Статистичні параметри законів ПФЧ управління фокусуванням ЕМВ (вид закону розподілу помилок, дисперсії та радіуси кореляції помилок) є вихідними величинами щодо статистики поля випромінювання. Однак через велику кількість елементів у каналах випромінювання, видів та джерел нестабільностей досить складно визначити вид закону розподілу помилок параметрів сигналів у кожному каналі БСВ. Враховуючи конструктивну незалежність каналів випромінювання та нехтуючи їх взаємним впливом, надалі припускатимемо, що помилки встановлення параметрів сигналів у каналах БСВ некорельовані та рівноймовірні. Як відомо [10, 11], у разі, коли немає можливості встановити закон розподілу, доцільно прийняти закон рівної ймовірності. Можна показати, що в цьому випадку помилка за рахунок відхилення дійсного закону від обраного закону рівної ймовірності, у гіршому випадку, не перевищить ±20% значення сумарної похибки (якщо розглянута похибка домінує). У першому наближенні це можна пояснити тим, що закон рівної ймовірності займає проміжне положення між модальними та антимодальними законами розподілу.

Розглянемо вплив зазначених нестабільностей на рівень пікової потужності, тривалість та період повторення ПЧІ. Проведемо оцінку максимальних значень помилок параметрів законів ПФЧ управління сигналами, у яких зазначені характеристики сфокусованих ПЧІ змінюються лише на 10 %.

Вимоги до точності розташування фазових центрів випромінювачів

Аналіз виразів для розрахунку щільності потоку потужності, яка створюється багатопозиційною системою випромінювачів у заданій точці простору [5 – 7], показує, що якість фокусування ПЧІ залежить від рівня забезпечення заданих координат фазових центрів джерел випромінювання. Однак при створенні конкретних зразків багатопозиційних радіотехнічних систем можливі помилки у забезпеченні вибраних координат і закони зміни миттєвих фаз не відповідатимуть вимогам когерентного складання сигналів випромінювачів у заданій точці простору $P(x_F, y_F, z_F)$. Тому процес формування послідовності сфокусованих ПЧІ може бути порушений. Для обґрунтування вимог до точності розташування фазових центрів випромінювачів у багатопозиційній системі проведемо математичне моделювання поля випромінювання при використанні V-подібних законів розподілу частот за наявності зазначених помилок.

Вплив помилок розташування фазових центрів окремих джерел випромінювання на нормовану щільність потоку потужності БСВ можна оцінити за виразом

$$\left\langle S(x,y,z,t)\right\rangle = \left\langle \frac{1}{S_{\max}} \left| \sum_{n=-(N-1)/2}^{(N-1)/2} \sqrt{\frac{P_n\, G_n}{4\pi R_n^2}} \exp\left\{ - j \left[2\pi f_{0n} \left(t - \frac{R_n^{\Delta}}{c} \right) + \varphi_{0n} \right] \right\} \right|^2 \right\rangle ; \qquad (1)$$

де P_n і G_n – потужність випромінювання та коефіцієнт посилення окремого джерела випромінювання; $S_{\max}$ – максимальне значення щільності потоку потужності БСВ.

Відстань до точки спостереження від кожного джерела випромінювання з урахуванням помилок розташування фазових центрів

$$R_n^{\Delta} = \sqrt{(x - x_n^{\Delta})^2 + (y - y_n^{\Delta})^2 + (z - z_n^{\Delta})^2} \; ; \qquad (2)$$

де $x_n^{\Delta} = x_n + \Delta x \Psi_1$, $y_n^{\Delta} = y_n + \Delta y \Psi_2$, $z_n^{\Delta} = z_n + \Delta z \Psi_3$ – значення координат фазових центрів джерел випромінювання БСВ з урахуванням помилок; Δx, Δy та Δz – максимальні значення помилок розташування фазових центрів джерел випромінювання; Ψ_1, Ψ_2, Ψ_3 – рівномірно розподілені в межах інтервалу [-1, 1] випадкові числа.

Закон розподілу несучих частот за відсутності помилок має вигляд [6, 7]:

$$f_{0n} = f_0 + |n|\Delta F_n; \tag{3}$$

де $n \in \left[-\frac{N-1}{2}; \ldots 0; \ldots \frac{N-1}{2} \right]$.

Закон розподілу початкових фаз для здійснення когерентного складання полів у вибраній точці фокусування матиме вигляд

$$\varphi_{0n} = -2\pi f_{0n} \left(\frac{z_F}{c} - \frac{R_{Fn}}{c} \right); \tag{4}$$

де $R_{Fn} = \sqrt{(x_F - x_n)^2 + (y_F - y_n)^2 + (z_F - z_n)^2}$ – відстань між точкою фокусування з координатами $P_F(x_F, y_F, z_F)$ та центром n-го джерела випромінювання з координатами (x_n, y_n, z_n).

Оцінки проведемо для випадку: ефективна база БСВ $L_{еф}$ = 1000 м; λ=0,1 м; N=33 та $P_n = 10$ кВт ($P_{вип.} = P_n N = 330$ кВт). Крок частоти між сусідніми джерелами випромінювання становить $\Delta F = 6{,}25$ *МГц* і, відповідно, максимальне рознесення несучих частот дорівнює $\Delta F_{\max} = 100$ *МГц*, що дозволяє формувати послідовність ПЧІ тривалістю $\tau_{ПЧІ}$=10 нс із періодом повторення $T_{ПЧІ}$=160 нс.

Розглянемо сумісне функціонування джерел випромінювання, розподілених за випадковим законом всередині кола з діаметром 1000 м. Як було показано в [6, 7], фокусування ЕМВ в аналізованої малобазової БСВ можливе вже на дальностях, що перевищують у 2 – 4 рази розмір ефективної бази $L_{еф}$. При цьому структура сформованої послідовності ПЧІ змінюється зі збільшенням дальності фокусування [12, 13]. Виходячи з цього, розглянемо вплив помилок розташування фазових центрів випромінювачів на характеристики поля випромінювання БСВ з урахуванням дальності фокусування.

На рис. 1 наведено залежності математичного очікування нормованої щільності потоку потужності випромінювання БСВ від помилок Δx, Δy та Δz відповідно, розраховані за виразом (1) при використанні одноступінчастого V-подібного закону розподілу частот (див. вир. (3)) при зміні дальності до точки фокусування від $z_F = 4{,}0 L_{еф}$ до $z_F = 24{,}0 L_{еф}$. Як видно із рис. 1, *а* вплив помилок розташування випромінювачів по осі 0X на рівень $\overline{S}_н$ більш суттєво позначається при виборі точки фокусування на малих дальностях від апертури БСВ. При цьому зменшення значення $\overline{S}_н$ не перевищує 10% на дальності $z_F = 4{,}0 L_{еф}$ при $\Delta x = 1{,}5\lambda$. Зі збільшенням дальності до точки фокусування вплив помилок розташування випромінювачів по осі 0X стає менш суттєвим і на дальності $z_F = 14{,}0 L_{еф}$ зменшення значення $\overline{S}_н$ на 10% відбувається при $\Delta x = 4{,}0\lambda$. Вибираємо за допустиме значення $\Delta x \le 1{,}5\lambda$. Як видно із рис. 1, *б* вплив помилок розташування випромінювачів по осі 0Y на рівень $\overline{S}_н$ менш суттєвий, ніж вплив помилок розташування випромінювачів по осі 0X.

Аналіз рис. 1, *в* показує, вплив помилок розташування фазових центрів випромінювачів по осі 0Z не залежить від дальності до точки фокусування. Однак, на відміну від попередніх випадків, вплив помилок по осі 0Z є суттєвим і потрібне вживання спеціальних заходів щодо

їх зниження [11, 12]. Область допустимих значень Δz, в якій зменшення значення $\bar{S}_н$ не еревищує 10 %, визначається, як і для Δh у разі плоскої ФАР, тобто. з умови $\Delta z \le \lambda/6$.

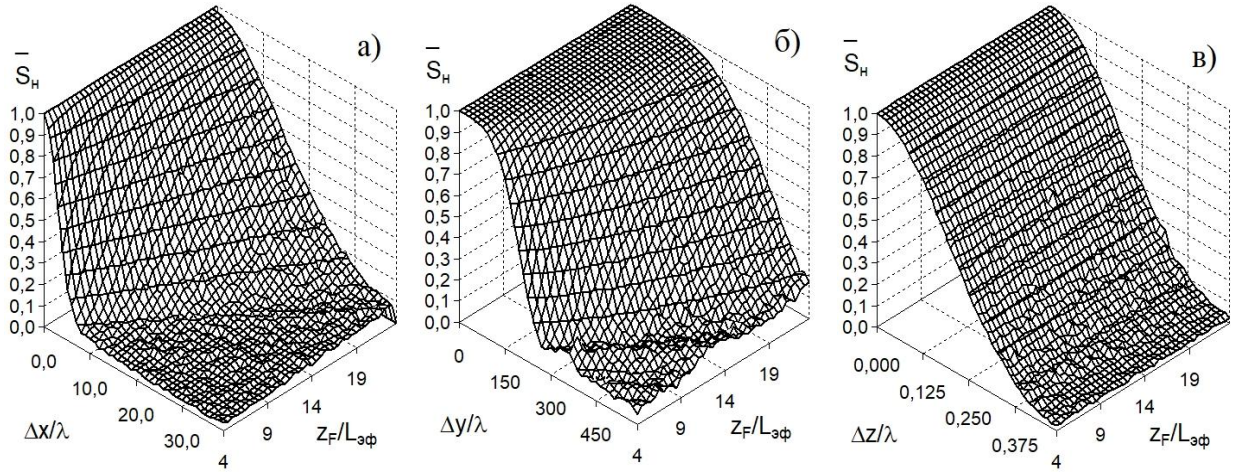


Рис. 1. Залежність математичного очікування нормованої щільності потоку потужності БСВ від помилок розташування фазових центрів: *а*) Δx; *б*) Δy; *в*) Δz

Вимоги до дискретності та точності установки початкових фаз та несучих частот за елементами системи

Розглянемо вплив помилок у встановленні заданих дискретностей несучої частоти та початкової фази у кожному елементі випромінювання на характеристики випромінювання БСВ. Розрахунок значень математичного очікування нормованої щільності потоку потужності проведемо на основі наступного виразу:

$$\left\langle S(x,y,z,t)\right\rangle = \left\langle \frac{1}{S_{\max}} \left| \sum_{n=-\frac{N-1}{2}}^{\frac{N-1}{2}} \sqrt{\frac{P_n G_n}{4\pi R_n^2}} \exp\left\{ -j\left[2\pi f_{0n}^{\Delta}\left(t - \frac{R_n}{c} \right) + \varphi_{0n}^{\Delta} \right] \right\} \right|^2 \right\rangle. \qquad (5)$$

При цьому закон розподілу початкових фаз з урахуванням помилок має вигляд

$$\varphi_{0n}^{\Delta} = -2\pi f_{0n}\left(\frac{z_F}{c} - \frac{R_{Fn}}{c} \right) + \Delta\varphi\Psi_1; \qquad (6)$$

де $\Delta\varphi$ – максимальне значення помилки встановлення початкової фази у кожному джерелі випромінювання; Ψ_1 – випадкова величина, рівномірно розподілена в межах інтервалу [-1, 1].

Одноступінчастий V-подібний закон розподілу несучих частот (див. вир. (3)) можна записати у вигляді

$$f_{0n}^{\Delta} = f_0 + |n|\Delta F + \Delta f\Psi_2; \qquad (7)$$

де Δf – максимальне значення помилки встановлення несучої частоти у кожному джерелі випромінювання; Ψ_2 – випадкова величина, рівномірно розподілена в межах інтервалу [-1, 1].

На рис. 2 наведена залежність математичного очікування нормованого значення щільності потоку потужності випромінювання БСВ від помилок Δφ при зміні дальності до точки фокусування від $z_F = 4{,}0L_{еф}$ до $z_F = 24{,}0L_{еф}$. Як видно із рис. 2, вплив помилок закону

ПФЧ управління сигналами, що випромінюються, не залежить від дальності до точки фокусування. Проте вплив помилок закону ПФЧ управління є суттєвим і потрібне вживання спеціальних заходів щодо їх зменшення [14]. Область допустимих значень Δφ, при якій зменшення значення $\overline{S}_н$ не перевищує 10 %, визначається за умови $\Delta\varphi \le \pi/3$.

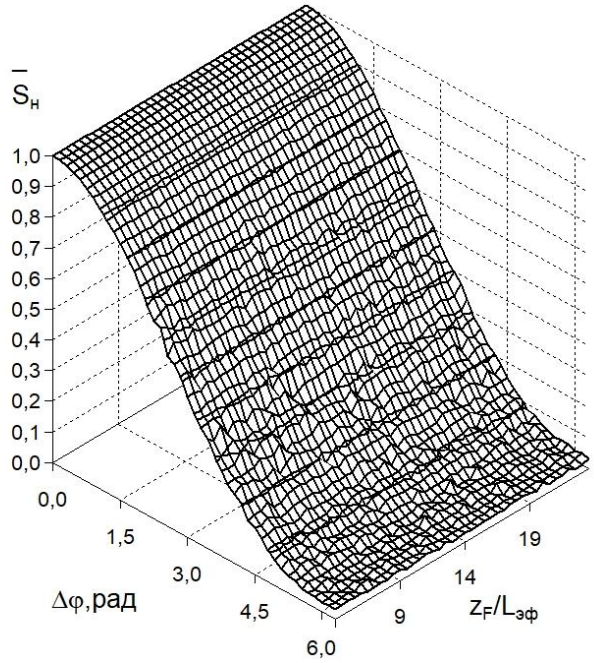


Рис. 2. Залежність математичного очікування нормованої щільності потоку потужності БСВ від помилок Δφ

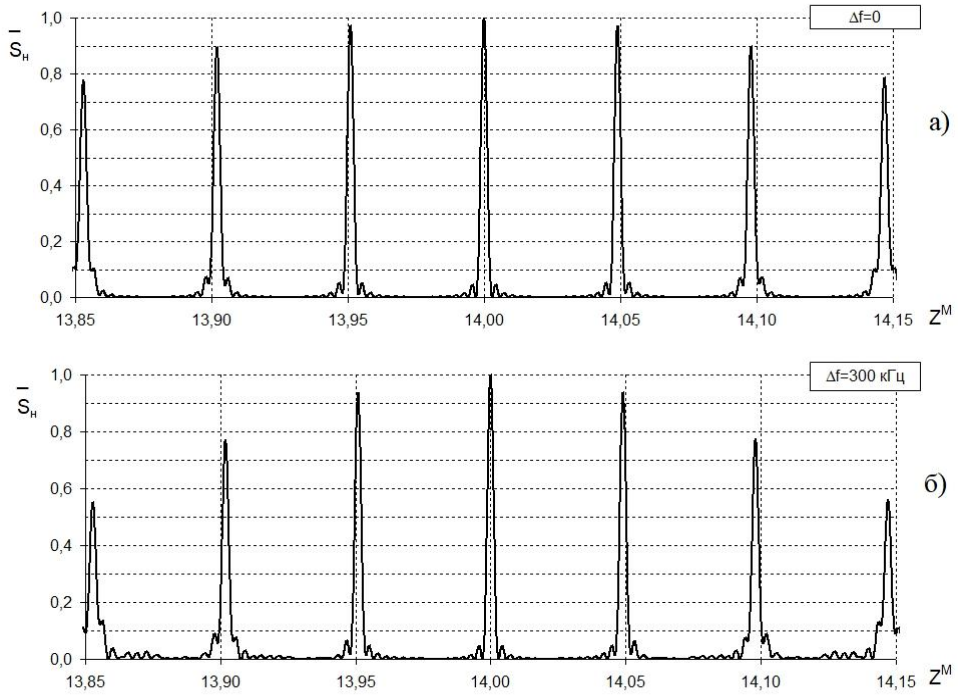


Рис. 3. Залежність математичного очікування нормованої щільності потоку потужності БСВ від помилок Δf: *а*) – Δf=0; *б*) – Δf=300 кГц

Як було показано в [15], на відстанях, порівнянних із розміром бази БСВ, формується пачка ПЧІ обмеженої тривалості. На рис. 3 наведено залежності математичного очікування нормованого значення щільності потоку потужності випромінювання БСВ без помилок в установці заданої дискретності несучих частот Δf=0 та з урахуванням максимального

значення цієї помилки Δf=300 кГц для точки фокусування $z_F = 14{,}0L_{еф}$. Як видно із рис. 3, *б*, вплив помилок установки несучих частот, що наростає з часом, зменшує тривалість пачки ПЧІ, що має враховуватися при здійсненні функціонального ураження бортових радіоелектронних пристроїв на дальностях, порівнянних з $L_{еф}$. Зі збільшенням дальності до точки фокусування вплив помилок установки несучих частот у передаючих каналах БСВ стає аналогічним випадку плоских фазованих антенних решіток. Проведені розрахунки показали, що при 10 %-му зниженні значення щільності потоку потужності БСВ допустимим є $\Delta fT \le 0{,}1$.

Висновки

Вплив помилок розташування випромінювачів у площині X0Y на рівень щільності потоку потужності ЕМВ найбільше позначається в першій половині зони Френеля. Зі збільшенням дальності до точки фокусування $z_F \ge 0{,}5z_d$ вплив цих помилок стає менш суттєвим. Вплив помилок розташування фазових центрів випромінювачів на осі 0Z не залежить від дальності до точки фокусування.

Для БСВ істотним є вплив помилок закону просторово-фазового управління сигналами, що випромінюються, і помилок розташування фазових центрів випромінювачів по осі 0Z. Як і для випадку плоскої фазованої антеної решітки, область допустимих значень цих помилок визначається за умови $\Delta\varphi \le \pi/3$ і $\Delta z \le \lambda/6$.

Вплив помилок установки несучих частот залежить від тривалості випромінювання, оскільки фазові помилки, зумовлені неточністю установки несучих частот радіовипромінювань, наростають з часом. Аналіз помилок установки несучих частот у каналах БСВ показав, що їх вплив не залежить від обраного значення максимального рознесення несучих частот по апертурі та визначається значенням помилки установки несучої частоти в випромінюючих елементах (або абсолютною нестабільністю частоти). Тривалість пачки ПЧІ при якій щільність потоку потужності знижується не більше ніж на 10 % через помилки встановлення несучих частот у випромінюючих елементах вибирається з умови $\Delta fT \le 0{,}1$.

Список літератури:

1. Сазонов Д.М. Антенны и устройства СВЧ. Москва : Высш. шк., 1988. 432 с.
2. Зиолковски Р.В. Новые импульсы направленной электромагнитной энергии // SPIE. Microwave and Particle Beam Sources and Propagation. 1988. Vol. 873.
3. Фельсен Л.В., Хейшан Е. Методы фокусировки луча от распределенных апертур // SPIE. Microwave and Particle Beam Sources and Propagation. 1988. Vol.873.
4. Содин Л.Г. Характеристики импульсного излучения антенн (электромагнитного снаряда) // Радиотехника и электроника. 1992. Т.37, № 5. С. 849-857.
5. Гомозов В.И., Гомозов А.В. Новый метод фокусировки электромагнитных излучений // Антенны. 2001. Вып. 3(49). С. 54-60.
6. Гомозов В.И., Гомозов А.В. Титов С.В. Пространственно-фазово-частотная фокусировка сигналов в плоских ФАР при V-образной дискретизации частот // Радиотехника. 2001. Вып. 122. С. 201-207.
7. Гомозов В.И., Гомозов А.В., Титов С.В. Метод формирования последовательностей сфокусированных пространственно-временных импульсов при использовании многоступенчатого V-образного распределения частот по апертуре плоских ФАР // Радиотехника. 2002. Вып. 130. С. 33-38.
8. Сканирующие антенные системы СВЧ. Т. I ; пер. с англ. ; под ред. Г.Т.Маркова и А.Ф. Чаплина. Москва : Сов. радио, 1966. 536 с.
9. Шифрин Я.С. Вопросы статистической теории антенн. Москва : Сов. радио, 1970. 384 с.
10. Маляревский Н.М. Погрешность измерения вероятностей // Известия вузов. 1962. № 2. С. 73-76.
11. Рабинович Б.Е. Методика суммирования частных погрешностей в области радиотехнических измерений // Вопросы радиоэлектроники. Сер. VI. Радиоизмерительная техника. 1961. Вып. 4. С. 3-20.
12. Линде Д.П. Радиопередающие устройства. Москва : Энергия, 1969. 680 с.
13. Уманский В.С. Усилительный тракт импульсных передающих устройств СВЧ. Москва : Сов. радио, 1973. 256 с.
14. Гомозов А.В., Гомозов В.И., Ермаков Г.В., Титов С.В. Фокусировка электромагнитного излучения и ее применение в радиоэлектронных средствах СВЧ ; под ред. В.И. Гомозова. Харьков : КП «Городская типография», 2011. 330 с.

15. Математическое и информационное обеспечение многоступенчатого V-образного управления частотой пространственно-распределенной передающей системы / С. В. Титов, Е. В. Титова // Системи обробки інформації. Харьков : ХУПС, 2016. Вип. 2(139). С. 63-67.

Надійшла до редколегії 11.05.2022

Відомості про авторів:

Коваленко Андрій Іванович – канд. техн. наук, старший науковий співробітник, Харківський національний університет радіоелектроніки, доцент кафедри системотехніки; Україна; e-mail: andrey.kovalenko@nure.ua; ORCID: https://orcid.org/0000-0003-2882-5082

Тітов Сергій Володимирович – канд. техн. наук, доцент, Харківський національний університет радіоелектроніки, доцент кафедри системотехніки; Україна; e-mail: serhii.titov@nure.ua; ORCID: https://orcid.org/0000-0003-0910-4415

Тітова Олена Вітольдіївна – канд. техн. наук, доцент, Харківський національний університет радіоелектроніки, доцент кафедри інформатики; Україна; e-mail: olena.titova@nure.ua; ORCID: https://orcid.org/0000-0001-8894-2040

Чорна Ольга Сергіївна – канд. техн. наук, Харківський національний університет радіоелектроніки, старший викладач кафедри системотехніки; Україна; e-mail: olha.chorna@nure.ua; ORCID: https://orcid.org/0000-0001-6745-8137

УДК 004.896 **DOI:10.30837/rt.2022.2.209.18**

І.Ш. НЕВЛЮДОВ, д-р техн. наук, С.П. НОВОСЕЛОВ, канд. техн. наук,
О.В. СИЧОВА, канд. техн. наук, С.І. ТЕСЛЮК

ВИЗНАЧЕННЯ КООРДИНАТ МОБІЛЬНОГО РОБОТА У ПРОМИСЛОВОМУ ПРИМІЩЕННІ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ BLE НА ОСНОВІ ДАНИХ RSSI, ОТРИМАНИХ ВІД БАЗОВИХ СТАНЦІЙ

Вступ

Існуючі технології глобального позиціонування, наприклад GPS, а також технології, що використовують засоби мобільного зв'язку (GSM) не можуть бути застосовані в приміщенні де сигнал зі супутників або вишок зв'язку значно знижується, внаслідок ослаблення супутникового сигналу в стінах і перекриттях будівель, або зовсім відсутній.

На сьогодні використовуються проєкти із побудови локальних систем позиціонування на основі спеціалізованих радіочастотних датчиків, наприклад, DW1000 [1], або на основі технології інфрачервоного випромінювання [2].

Вказані системи мають декілька недоліків. Системи на основі DW1000 мають високу вартість (порядку 25 USD за один сенсор), датчики ще недостатньо розповсюджені. Дана технологія визначення відстані ще не має налагоджених бібліотек для використання.

Технологія позиціонування на основі маяків з використанням оптичного інфрачервоного діапазону випромінювання має гарні показники точності визначення позиції, але має суттєвий недолік – перешкоди, які можуть повністю порушити роботу всієї системи. Тому використання даної технології в виробничому приміщенні недоцільно.

Також в процесі локального визначення положення мобільних платформ у промислових приміщеннях можуть бути використані технології бездротових мереж, таких як Bluetooth чи Wi-Fi. В такому випадку найчастіше використовують дані про потужності сигналів Wi-Fi, що можуть прийматися роботом від різних точок доступу. Але у такого методу існує проблема з забезпеченням потрібної точності, значно ускладнюючи реальну інтерференційну картину покриття Wi-Fi.

Таким чином, актуальність даних досліджень пов'язана із вирішенням проблеми локального позиціонування мобільних роботів в приміщенні з точністю до десятків сантиметрів.

Постановка завдання

Метою роботи є визначення локальної позиції мобільного робота за допомогою технології BLE і отриманих від базових станцій даних RSSI.

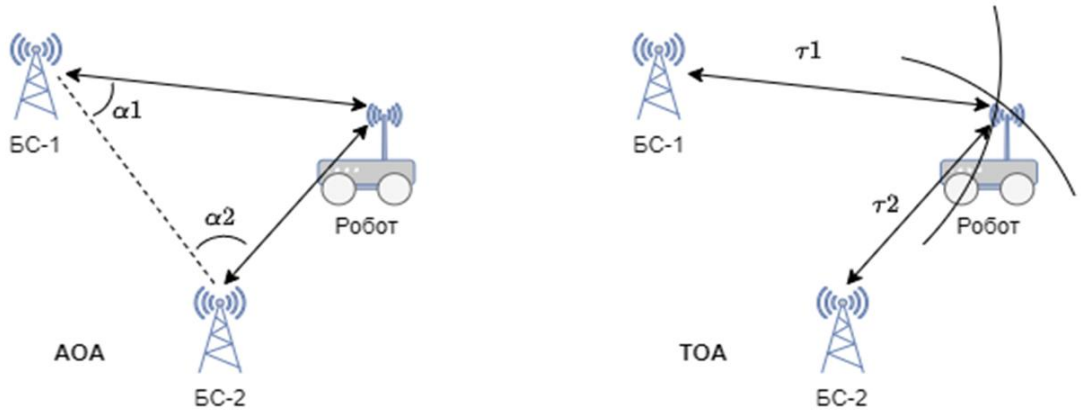
Для досягнення мети необхідно вирішити наступні завдання:

- провести аналіз методів визначення локальної позиції мобільного роботу;
- розробити метод визначення положення мобільного пристрою в просторі на основі отриманих значень RSSI від базових станцій;
- розробити архітектуру програмно-апаратного комплексу;
- розробити метод визначення координати положення мобільного робота в просторі.

Аналіз методів визначення локальної позиції мобільного роботу

В роботі пропонується використовувати технологію BLE (Bluetooth Low Energy) для визначення локальної позиції знаходження мобільного роботу в просторі. Технологія базується на використанні декількох базових станцій в приміщенні та визначенні відстані між мобільним роботом та цими базовими станціями. На основі визначених відстаней методом тріангуляції розраховується актуальне місцезнаходження роботу.

Дана технологія не є новою, але на сьогодні набирає популярності завдяки зростаючої кількості пристроїв із вбудованим модулем BLE та появою дешевих чипів з підтримкою даної технології та розвинутою інфраструктурою для створення програмного забезпечення для них. Відомі декілька методів визначення позиції в просторі [4]. На рис. 1 показані принципи визначення координат за методами AOA і TOA.



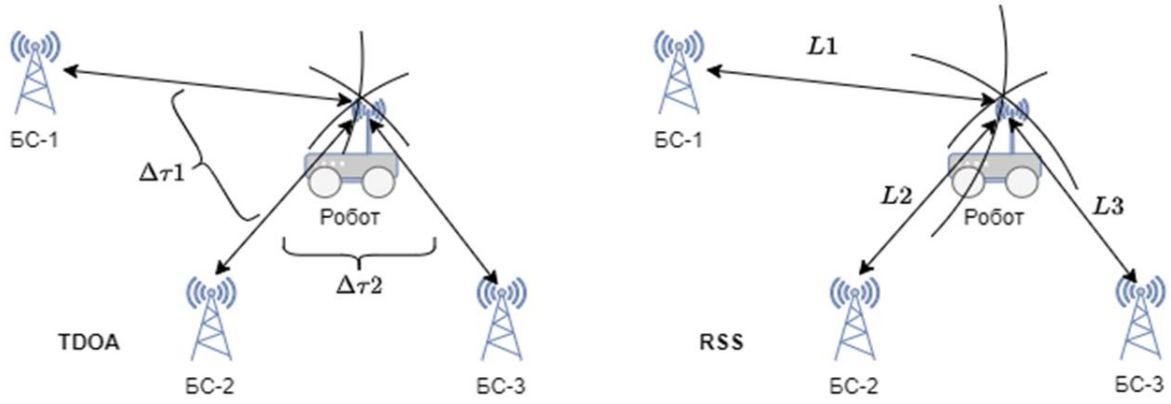
а *б*

Рис. 1. Визначення координат методами: *а* – AOA, *б* – TOA

У методі AOA (Angle of arrival) (рис. 1, *а*) розташування пристрою визначається в межах трикутника, утвореного перетином осей антен трьох базових станцій (метод модифікованої тріангуляції). Базові станції використовують спрямовані антени або антенні масиви для визначення кута вхідних сигналів, що надсилаються мобільним пристроєм.

В системах позиціонування, що використовують метод TOA (Time of Arrival) (рис. 1, *б*) [4], вимірюється час проходження сигналу від пристрою до базової станції. За даним методом відстань до об'єкта розраховується на основі різниці між часом надсилання сигналу і його отримання. У той же час цей підхід вимагає суворого дотримання часу синхронізації часу відправника та одержувача, що досить важко досягти. Одним із різновидів використання даного принципу, є застосування ультра-широкого діапазону (ultra-wideband) смуги вимірювання.

На рис. 2 показані принципи визначення координат за методами TDOA та RSSI.



а *б*

Рис. 2. Визначення координат методами: *а* – TDOA, *б* – RSSI

У системах TDOA (рис. 2, *а*) [4], мобільний пристрій посилає сигнали позиціонування до оточуючих базових станцій, та розраховує часову різницю прибуття отриманих сигналів. Основною перевагою систем TDOA є те, що необхідно лише синхронізувати вимірювальні вузли (базові станції). Ця синхронізація, як правило, здійснюється через локальну мережу.

RSSI (Received Signal Strength Indication) використовується для вимірювання рівня потужності сигналу [3]. Найпростіші схеми розробляються, щоб прийняти вхідний сигнал і

сформувати аналогову вихідну напругу (або відповідний цифровий код, який отримується після подачі цієї напруги на АЦП), пропорційну потужності прийнятого сигналу. Можна використовувати даний показник, щоб оцінити відстань до передавача або до базової станції.

Метод позиціонування, заснований на отриманні даних RSSI (рис. 2, *б*), використовує характеристику розповсюдження радіосигналу (потужність сигналу). Використовуючи правильну модель розповсюдження, можна розрахувати відстані між мобільним пристроєм та базовими станціями, тим самим визначається місцерозташування мобільного роботу. Цей метод працює на невеликих відстанях, але зі збільшенням діапазону помилка зростає через специфіку розповсюдження радіосигналу.

Для вирішення завдання визначення просторового положення мобільного робота у приміщені було обрано метод позиціонування, заснований на отриманні даних RSSI.

Метод визначення положення мобільного пристрою в просторі на основі отриманих значень RSSI від базових станцій

Враховуючи специфіку пристроїв з вбудованим BLE приймачем, наприклад ESP32 та інші, де радіус дії радіосигналу визначається в межах 10 метрів, дану технологію можна застосувати для визначення положення мобільного робота в промисловому приміщенні відносно певної кількості базових станцій.

На рис. 3 подано принцип визначення положення мобільного пристрою в просторі на основі отриманих значень RSSI від базових станцій.

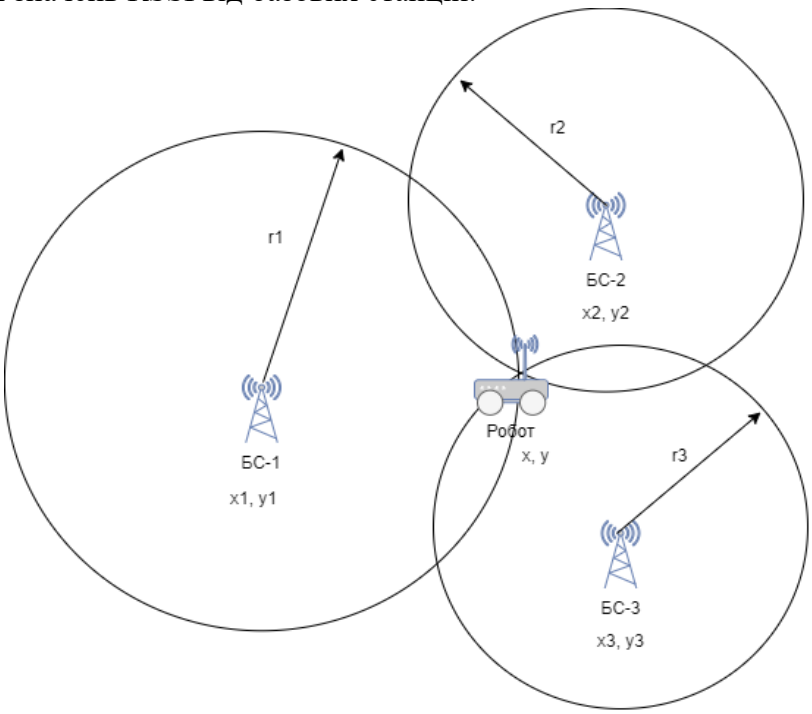


Рис. 3. Визначення положення мобільного пристрою в просторі на основі отриманих значень RSSI від базових станцій

Для визначення місцезнаходження мобільного робота в промисловому приміщенні використовується метод тріангуляції. Цей метод використовується для розрахунку відносного розташування пристрою за допомогою відстаней, отриманих шляхом розрахунків на основі вимірюваних значень RSSI.

Дані тріангуляції показують відстань мобільного пристрою від базових станцій, що побудовані на основі ESP32, використовуючи фіксовані координати станцій (x_n, y_n). Щоб визначити точне положення роботу, цей метод використовує площу перекриття, утворену трьома колами з радіусами у центрі розташування базових станції, що задає область локалізації для виміряних відстаней.

На колах представляють всі можливі місця мобільного пристрою на заданій відстані (радіусу) від базової станції. Таким чином можна розрахувати координати (x, y) розташування мобільного роботу в просторі, що є точкою перехрещення трьох кіл [7].

Координати кожної базової станції задаються на етапі підготовки до експерименту у вигляді констант (наприклад, на рис. 3 це БС-1 (x_1, y_1), БС-2 (x_2, y_2), БС-3 (x_3, y_3)).

Розробка архітектури програмно-апаратного комплексу

Для визначення позиції мобільного пристрою застосовуються базові станції. Мінімально необхідна кількість станцій дорівнює трьом. Кожна станція має автономне джерело живлення. Мобільний пристрій послідовно підключається до всіх станцій, що знаходяться в зоні його видимості. Для цього кожні 5 – 10 секунд відбувається сканування діапазону радіочастот та визначаються пристрої, що відповідають характеристикам базових станцій. Після підключення до станції пристрої обмінюються повідомленнями для визначення потужності радіосигналу за допомогою RSSI. Архітектуру програмно-апаратного комплексу подано на рис. 4.

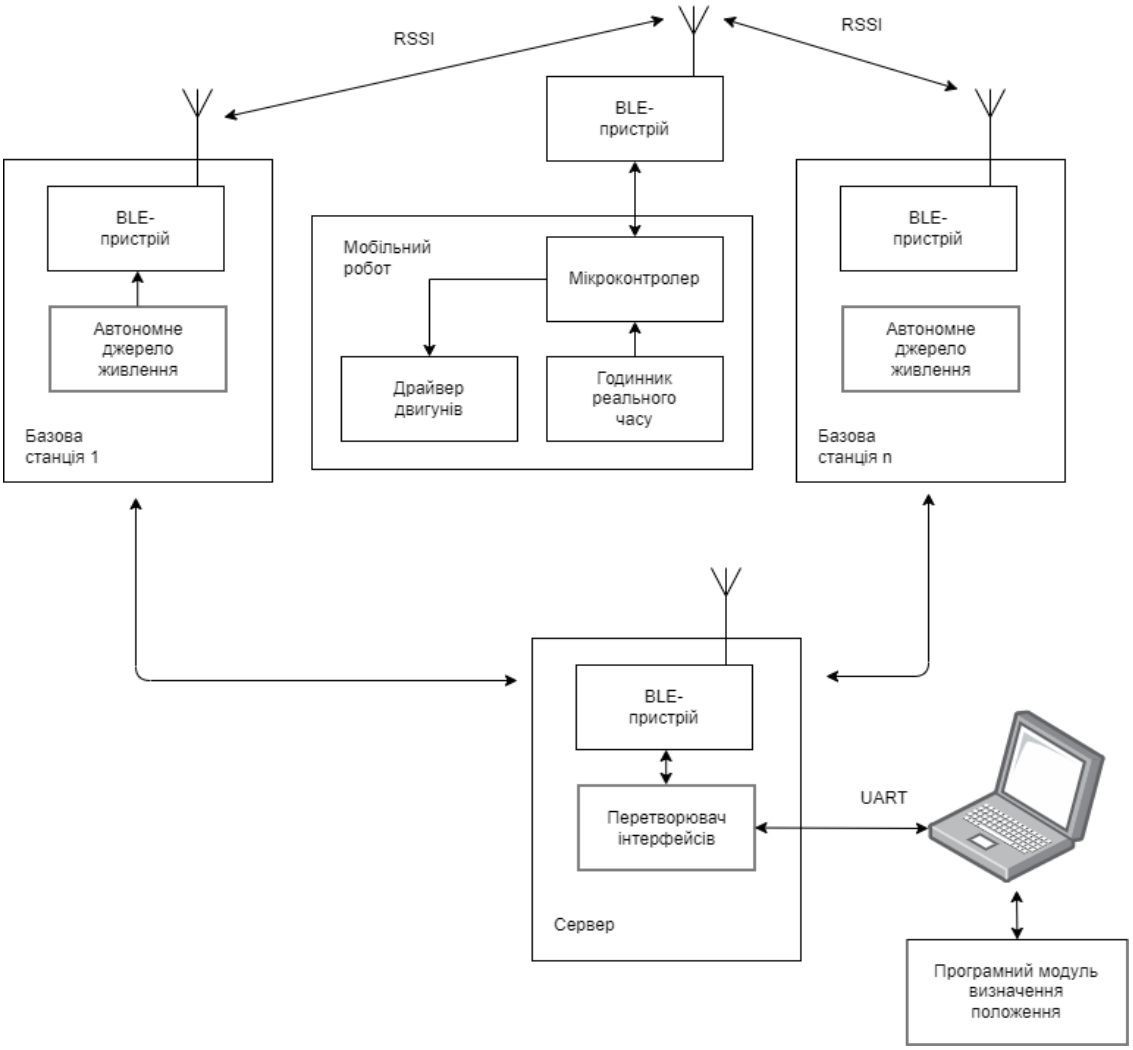


Рис. 4. Архітектура програмно-апаратного комплексу

Кожна базова станція зберігає дані про останній сеанс зв'язку у внутрішній пам'яті. Сервер програмно-апаратного комплексу з певною періодичністю опитує всі наявні базові станції та одержує від них набір даних останніх сеансів.

Кожний набір даних містить ID пристрою, MAC адресу пристрою та базової станції, значення RSSI, що було отримано в процесі сеансу зв'язку. Ці дані за допомогою одного з

інтерфейсів зв'язку, наприклад UART, потрапляють до персонального комп'ютера, де програмний модуль визначає координати місцезнаходження мобільного роботу.

Розрахунок координат положення мобільного робота в просторі

Як показано на рис. 3, щоб розрахувати координати позиції мобільного роботу (BLE-пристрою), необхідні координати центрів трьох кіл ((x_1, y_1), (x_2, y_2),(x_3, y_3)), що є попередньо визначеними координатами базових станцій.

Радіуси кожного кола – це відстань між кожним BLE-пристроєм та роботом. Для кожного кола справедливе рівняння [3, 5]:

$$\begin{cases} (x-x_1)^2+(y-y_1)^2=r_1^2 \\ (x-x_2)^2+(y-y_2)^2=r_2^2 \\ (x-x_3)^2+(y-y_3)^2=r_3^2 \end{cases}. \quad (1)$$

В результаті отримуємо наступні рівняння:

$$\begin{cases} 2x(-x_1+x_2)+2y(-y_1+y_2)=r_1^2-r_2^2-x_1^2+x_2^2-y_1^2+y_2^2 \\ 2x(-x_2+x_3)+2y(-y_2+y_3)=r_2^2-r_3^2-x_2^2+x_3^2-y_2^2+y_3^2 \end{cases}. \quad (2)$$

Перепишемо ці два рівняння, використовуючи константи *A, B, C, D, E, F,* отримаємо систему двох рівнянь:

$$\begin{cases} A_x+B_y=C \\ D_x+E_y=F \end{cases}. \quad (3)$$

Вирішуючи рівняння для *x* та *y*, отримаємо:

$$x=(C\cdot B-F\cdot B)/(E\cdot A-B\cdot D), \quad (4)$$

$$y=(C\cdot D-A\cdot F)/(B\cdot D-A\cdot E). \quad (5)$$

Таким чином, розраховуються координати *x* та *y* у визначеному під час проектування просторі.

Для отримання радіусів r_1, r_2, r_3 необхідно обчислити відстань від мобільного пристрою до відповідної базової станції на основі даних RSSI. Для рішення даної задачі скористуємось рівнянням [6]:

$$L=10^{\left(\frac{P_m-RSSI}{10N}\right)}, \quad (6)$$

де P_m – вимірювана потужність (RSSI) на відстані один метр від передавача; *RSSI* – отримане значення RSSI з базових станцій; $N = 2$.

Необхідно зазначити, що на якість сигналу впливає розташування модулів зв'язку, орієнтація антени, віддаленість базових станцій та мобільного пристрою від стін будівлі, наявність інших пристроїв в ефірі. Важливу роль має частота роботи пристроїв, в нашому випадку це 2,4 ГГц. Також такі перешкоди, як людина в приміщенні, можуть впливати на результати вимірювань відстані між пристроями.

Для збільшення точності позиціонування пропонується використовувати більше базових станцій, ніж мінімально можливе для конкретного типу приміщення.

Висновки

Запропонований метод дозволяє вирішувати задачу визначення локальної позиції мобільного роботу в промисловому приміщенні з використанням модулів радіозв'язку, що

працюють за технологією BLE. В якості таких пристрів в даній роботі пропонується використовувати модулі ESP32. Дистанція від мобільного роботу до базових станцій визначається на основі даних RSSI, що отримуються в результаті «спілкування» двох пристроїв – робота і базової станції. Використовуючи метод тріангуляції, отримано формули для вирішення задачі визначення координат об'єкту, що рухається в просторі. Необхідно враховувати, що значення RSSI дуже нестабільне, тому точність позиціонування буде залежати також від кількості базових станцій та від використаних додаткових програмних інструментів, наприклад, фільтра Калмана.

Список літератури:

1. S. Novoselov, "Wireless Sensor Network for Communication Between Base Stations in the Local Positioning System," 2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), 2018, pp. 383-386, doi: 10.1109/INFOCOMMST.2018.8632140.
2. S. Novoselov and O. Donskov, "Distributed local positioning system using DWM1000 location chip," 2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), 2017, pp. 489-492, doi: 10.1109/INFOCOMMST.2017.8246445.
3. M. E. Rusli, M. Ali, N. Jamil and M. M. Din, "An Improved Indoor Positioning Algorithm Based on RSSI-Trilateration Technique for Internet of Things (IOT)," 2016 International Conference on Computer and Communication Engineering (ICCCE), 2016, pp. 72-77, doi: 10.1109/ICCCE.2016.28.
4. Y. Wang, Xu Yang, Yutian Zhao, Yue Liu and L. Cuthbert, "Bluetooth positioning using RSSI and triangulation methods," 2013 IEEE 10th Consumer Communications and Networking Conference (CCNC), 2013, pp. 837-842, doi: 10.1109/CCNC.2013.6488558.
5. P. S. Dravya, Ujwal K. Holla, K. N. Pushpalatha. (2020). Indoor Navigation System using BLE and ESP32. 10.22214/irjaset.2020.32089.
6. M. Golestanian, H. Lu, C. Poellabauer and J. Kenney, "RSSI-Based Ranging for Pedestrian Localization," 2018 IEEE 88th Vehicular Technology Conference (VTC-Fall), 2018, pp. 1-5, doi: 10.1109/VTCFall.2018.8690714.
7. S. Novoselov and O. Donskov, "Study of mobile device wireless control technology in the visible range of the electromagnetic radiation," 2016 Third International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T), 2016, pp. 123-124, doi: 10.1109/INFOCOMMST.2016.7905355.
8. S. Novoselov, O. Sychova and S. Tesliuk, "Development of the Method Local Navigation of Mobile Robot a Based on the Tags with QR Code and Wireless Sensor Network," 2019 IEEE XVth International Conference on the Perspective Technologies and Methods in MEMS Design (MEMSTECH), 2019, pp. 46-51, doi: 10.1109/MEMSTECH.2019.8817405.
9. I. Nevludov, O. Sychova, A. Andrusevich, S. Novoselov, D. Mospan and V. Mospan, "Simulation of the Sensor Network of Base Stations in a Local Positioning System in Intelligent Industries," 2020 IEEE Problems of Automated Electrodrive. Theory and Practice (PAEP), 2020, pp. 1-6, doi: 10.1109/PAEP49887.2020.9240842.
10. I. Nevliudov, S. Novoselov, O. Sychova and S. Tesliuk, "Development of the Architecture of the Base Platform Agricultural Robot for Determining the Trajectory Using the Method of Visual Odometry," 2021 IEEE XVIIth International Conference on the Perspective Technologies and Methods in MEMS Design (MEMSTECH), 2021, pp. 64-68, doi: 10.1109/MEMSTECH53091.2021.9468008.
11. I. Nevludov, S. Novoselov, O. Sychova, S. Tesliuk. Production Workspace Obstacle Avoidance Mobile Robot Trajectory Modeling 2021: Fifth International Scientific and Technical Conference "COMPUTER AND INFORMATION SYSTEMS AND TECHNOLOGIES" pp.61-62.
12. I. Nevludov, O. Sychova, O. Reznichenko, S. Novoselov, D. Mospan and V. Mospan, "Control System for Agricultural Robot Based on ROS," 2021 IEEE International Conference on Modern Electrical and Energy Systems (MEES), 2021, pp. 1-6, doi: 10.1109/MEES52427.2021.9598560.
13. L. Li, Y. Wu, Y. Ren and N. Yu, "A RSSI Localization Algorithm Based on Interval Analysis for Indoor Wireless Sensor Networks," 2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing, 2013, pp. 434-437, doi: 10.1109/GreenCom-iThings-CPSCom.2013.90.
14. N. N. Sümer, N. Ataklı and O. Kucur, "Using RSSI-Based Bluetooth Low Energy for Indoor Location Detection," 2020 5th International Conference on Computer Science and Engineering (UBMK), 2020, pp. 83-87, doi: 10.1109/UBMK50275.2020.9219422.
15. A. Golestani, N. Petreska, D. Wilfert and C. Zimmer, "Improving the precision of RSSI-based low-energy localization using path loss exponent estimation," 2014 11th Workshop on Positioning, Navigation and Communication (WPNC), 2014, pp. 1-6, doi: 10.1109/WPNC.2014.6843302.

16. J. Wisanmongkol, L. Klinkusoom, T. Sanpechuda, L. Kovavisaruch and K. Kaemarungsi, "Multipath Mitigation for RSSI-Based Bluetooth Low Energy Localization," 2019 19th International Symposium on Communications and Information Technologies (ISCIT), 2019, pp. 47-51, doi: 10.1109/ISCIT.2019.8905164.

17. S. Saxena, A. Pandey and S. Kumar, "A Multistage RSSI-based Scheme for Node Compromise Detection in IoT Networks," 2019 IEEE 16th India Council International Conference (INDICON), 2019, pp. 1-4, doi: 10.1109/INDICON47234.2019.9029092.

18. S. Cortesi, M. Dreher and M. Magno, "Design and Implementation of an RSSI-Based Bluetooth Low Energy Indoor Localization System," 2021 17th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), 2021, pp. 163-168, doi: 10.1109/WiMob52687.2021.9606272.

19. P. Sthapit, H. -S. Gang and J. -Y. Pyun, "Bluetooth Based Indoor Positioning Using Machine Learning Algorithms," 2018 IEEE International Conference on Consumer Electronics – Asia (ICCE-Asia), 2018, pp. 206-212, doi: 10.1109/ICCE-ASIA.2018.8552138.

20. S. Subedi, G. -R. Kwon, Seokjoo Shin, Suk-seung Hwang and Jae-Young Pyun, "Beacon based indoor positioning system using weighted centroid localization approach," 2016 Eighth International Conference on Ubiquitous and Future Networks (ICUFN), 2016, pp. 1016-1019, doi: 10.1109/ICUFN.2016.7536951.

21. A. Noertjahyana, I. A. Wijayanto and J. Andjarwirawan, "Development of Mobile Indoor Positioning System Application Using Android and Bluetooth Low Energy with Trilateration Method," 2017 International Conference on Soft Computing, Intelligent System and Information Technology (ICSIIT), 2017, pp. 185-189, doi: 10.1109/ICSIIT.2017.64.

Надійшла до редколегії 15.05.2022

Відомості про авторів:

Невлюдов Ігор Шакирович – д-р техн. наук, професор, Харківський національний університет радіоелектроніки, завідувач кафедри комп'ютерно-інтегрованих технологій, автоматизації та мехатроніки; Україна; e-mail: igor.nevliudov@nure.ua; ORCID: https://orcid.org/0000-0002-9837-2309

Новоселов Сергій Павлович – канд. техн. наук, доцент, Харківський національний університет радіоелектроніки, професор кафедри комп'ютерно-інтегрованих технологій, автоматизації та мехатроніки; Україна; e-mail: sergiy.novoselov@nure.ua, ORCID: https://orcid.org/0000-0002-3190-0592

Сичова Оксана Володимирівна – канд. техн. наук, Харківський національний університет радіоелектроніки, доцент кафедри комп'ютерно-інтегрованих технологій, автоматизації та мехатроніки; Україна; e-mail: oksana.sychova@nure.ua, ORCID: https://orcid.org/0000-0002-0651-557X

Теслюк Сергій Ігорович – Харківський національний університет радіоелектроніки, старший викладач кафедри комп'ютерно-інтегрованих технологій, автоматизації та мехатроніки; Україна; e-mail: serhii.tesliuk@nure.ua; ORCID: https://orcid.org/0000-0003-0711-9250

УДК 616.833 **DOI:10.30837/rt.2022.2.209.19**

І.В. ПРАСОЛ, д-р техн. наук, О.А. ЄРОШЕНКО

МОДЕЛЮВАННЯ ЗАЛЕЖНОСТІ ІНТЕНСИВНОСТІ ЕЛЕКТРОСТИМУЛЯЦІЇ ВІД ЧАСТОТИ СЛІДУВАННЯ СТИМУЛІВ

Вступ

Електростимуляція полягає у такому впливі імпульсного електричного струму з певним набором параметрів на тіло пацієнта, при якому виникають необхідні позитивні терапевтичні ефекти. Особливо поширена електростимуляція скелетних м'язів. Вона є ефективним методом реабілітації при різних травмах та порушеннях, а також допоміжним способом під час підготовки спортсменів. Існуючі апарати, як правило, мають ряд стандартних режимів, можливості точної підстройки параметрів стимулів обмежені. Це не дозволяє достатньо врахувати індивідуальні особливості пацієнта. У той же час дуже багато залежить від обраного м'яза, його властивостей, віку, статі пацієнта і т.п. Тому досить актуально визначати апріорно деякі параметри стимулів струму, зокрема його частоту.

Сутність дослідження

Розглянемо особливості м'язових скорочень та вплив на них частоти сигналу. Розрізняють поодинокі та тетанічні скорочення. Поодиноке скорочення можна викликати за допомогою короткого прямокутного імпульсу напруги (тривалістю близько 1 мс) [1 – 3]. Викликане цим стимулом скорочення утворюється не відразу, а з деякою часовою затримкою близько 10 мс. Далі відбувається скорочення протягом 30 – 50 мс та розслаблення тривалістю приблизно 50 – 60 мс. Т.ч. одиночне скорочення відбувається загалом за 100 мс (рис. 1). Цей проміжок часу різний для різних м'язів і багато в чому залежить від їх стану [4 – 7].

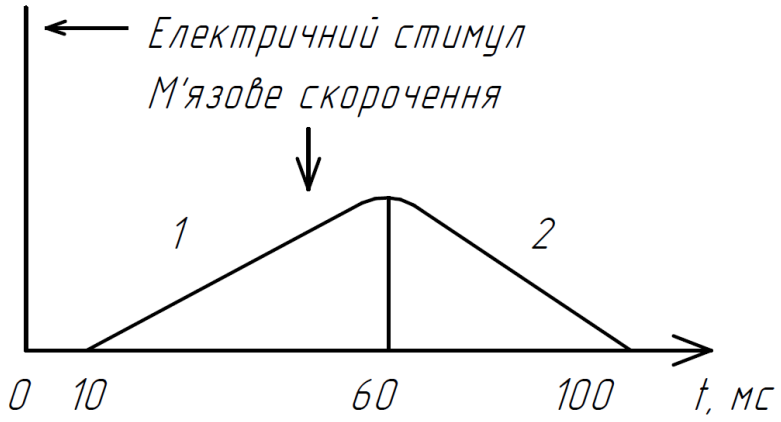


Рис. 1. Одиночне м'язове скорочення: *1* – фаза укорочення; *2* – фаза розслаблення

Тривалість деполяризації потенціалу дії м'язового волокна дорівнює 3 – 5 мс, після чого мембрана відновлює здатність збудження. Час скорочення становить близько 50 мс, тому ще під час скорочення волокно може відповідати на нові стимули. Таке накладання скорочень називається тетанічним (тетанус) [8 – 10]. Воно має місце як в окремому м'язовому волокні, так і м'язі в цілому. Амплітуда тетануса значно більша за амплітуду одиночного скорочення, тому що періодична стимуляція викликає додаткове скорочення, яке підсумовується з попереднім.

Тетанус може бути зубчастим та гладким. Зубчастий тетанус виникає тоді, коли частота стимулів така, що кожен подальший стимул подається після скорочення (фаза укорочення 1), але до тих пір, поки розслаблення ще не закінчилося. Гладкий тетанус з'являється при більшій частоті стимулів, коли частота стимулів така, що кожен наступний стимул подається під час фази укорочення, до початку розслаблення. Так, для розглянутого на рис. 1 випадку зубчастий тетанус спостерігається на частотах 10 – 20 Гц, гладкий – на частотах вище 20 Гц.

Щодо амплітуди скорочень можна сказати таке. Вона мінімальна при одиночному скороченні, збільшується при зубчастому тетанусі та максимальна при гладкому. Однак збільшення амплітуди та сили скорочення з подальшим зростанням частоти зупиняється і збільшення частоти призводить до зменшення амплітуди скорочень. Це називається песимумом реакції у відповідь. Тобто, існує деяка оптимальна частота стимуляції м'яза. Частоти більше оптимальної є песимальними [11 – 13].

Таким чином, оптимум – це гладкий тетанус з максимальною амплітудою при оптимальній частоті подразнення, коли кожен імпульс у послідовності діє на м'яз у фазу екзальтації, коли умови для збудження та підсумовування одиночних скорочень найкращі. Песимум теж гладкий тетанус, але з мінімальною амплітудою при песимальній частоті подразнення, коли кожен імпульс у серії діє на м'яз у фазу відносної рефрактерності, коли умови для збудження та підсумовування одиночних скорочень найгірше. На рис. 2 зображено залежності сили скорочення деякого м'яза від частоти проходження електричних стимулів.

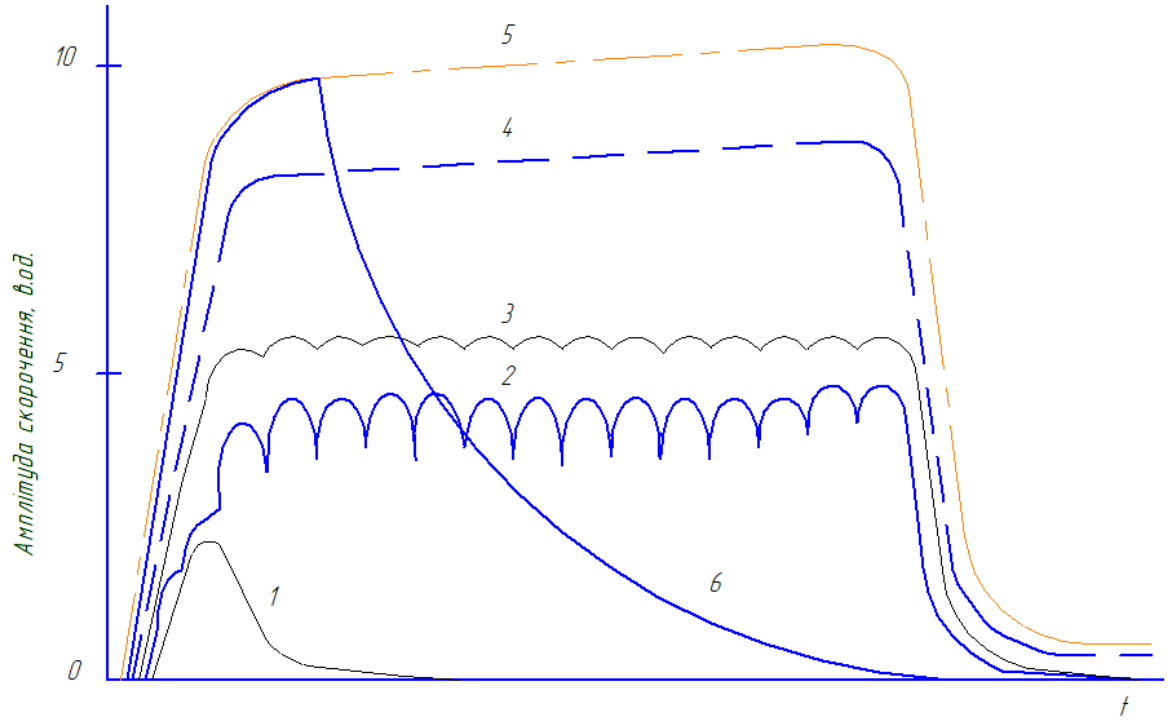


Рис. 2. Залежність сили скорочення м'язів від частоти стимулів:
1 – одиночне скорочення; *2,3* – зубчастий тетанус (частоти стимуляції 12 та 20 Гц відповідно);
4,5 – гладкий тетанус (частоти стимуляції 30 та 50 Гц відповідно); *5* – оптимум;
6 – песимум (частота стимуляції 100 Гц)

У людському організмі частота та режим посилання моторними нейронами нервових імпульсів до м'яза забезпечують асинхронне залучення у процес скорочення більшої чи меншої кількості рухових одиниць та підсумовування їх окремих скорочень.

З урахуванням відомих даних та узагальнюючи все сказане вище, можна отримати наступну якісну безперервну залежність амплітуди скорочення м'яза від частоти стимулюючого сигналу, що представлена на рис. 3.

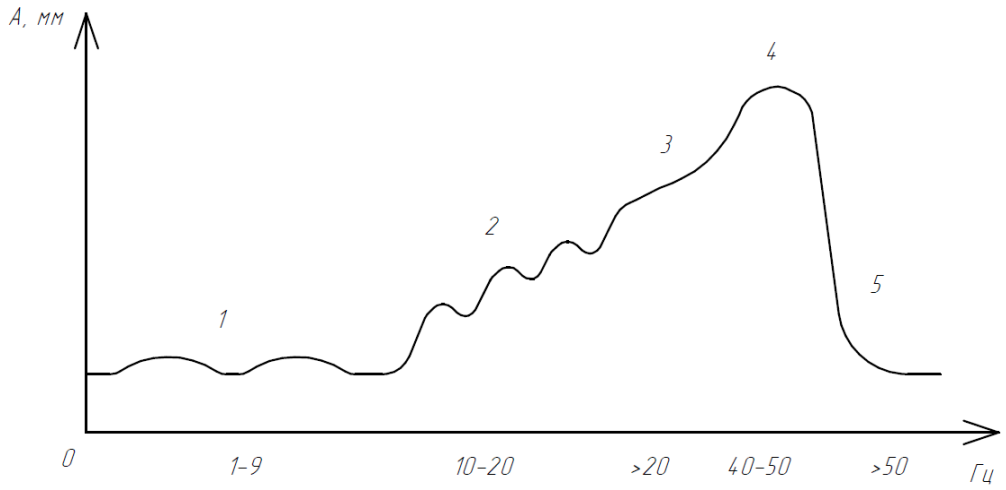


Рис. 3. Якісна безперервна залежність амплітуди скорочення м'яза
від частоти стимулюючого сигналу

Видно, що зі збільшенням частоти стимулів спочатку виникають поодинокі м'язові скорочення (*1*), потім зубчастий тетанус (*2*), гладкий тетанус (*3*) і, нарешті, оптимум (*4*) і песимум (*5*).

У зв'язку з цим виявляється актуальною задача моделювання цих процесів з метою отримання аналітичного виразу, який дозволить апріорно знайти оптимальну частоту стимуляції. Для цього доцільно використовувати підхід типу «чорної скриньки», згідно з яким розглядається тільки взаємозв'язок між вхідними та вихідними змінними, не вдаючись у деталі фізіологічних процесів, що відбуваються в рухових одиницях і всього м'яза в цілому.

На початковому етапі моделювання виконується структурна ідентифікація моделі. Вона полягає у виборі відповідного аналітичного опису.

Таким чином, необхідно отримати деякий аналітичний опис, що встановлює зв'язок між вхідними та вихідними змінними. Позначимо частоту стимулів через f (тоді циклічна частота $\omega = 2\pi f$), амплітуду скорочення через A (у відносних одиницях). Слід знайти певну залежність $A=F(\omega)$, таку, щоб при A і $\omega \geq 0$ вона в діапазоні значень $\omega \geq 0$ і $\omega < 300$ якісно описувала криву на рис. 3, а сама функція F належала до класу r-гладких функцій з порядком гладкості $r \geq 1$, принаймні щоб $F \in C^1(\omega)$.

Тому що на рис. 3 виділено 5 різних областей, очевидно, що функція $A=F(\omega)$ може бути представлена як суперпозиція $F(\omega) = F_1(\omega) + F_2(\omega) + F_3(\omega) + F_4(\omega) + F_5(\omega)$, де $F_i(\omega)$ – деякі безперервні функції частоти.

Використаємо одиничну ступінчасту функцію (функцію Хевісайда), зміщену праворуч по осі часу, яка записується у вигляді

$$1(t-\tau) = \begin{matrix} 1, t \geq \tau, \\ 0, t \leq \tau. \end{matrix} \qquad (1)$$

Функція $1(t-\tau)$ має властивість відсічення, тому множення будь-якої функції $f(t)$ на функцію $1(t-\tau)$ звертає функцію $f(t)$ в нуль при $t < \tau$, і залишає незмінним значення при $t \geq \tau$.

Шляхом додавань 2-х ступінчастих функцій можна отримати вираз для одиничного прямокутного вікна тривалістю τ_n:

$$1(\tau_n) = 1(t-\tau_1) - 1(t-\tau_2), \qquad (2)$$

де τ_1, τ_2 – зрушення по осі часу, що відповідають початку та кінцю одиничного імпульсу.

Таким чином, якщо використовувати дуальне перетворення частоти в час можна отримати наступний опис функції F(ω):

$$F(\omega) = \sum_{i=1}^{5} F_i(\omega) \cdot 1(\tau_{ni}), \tag{3}$$

де $1(\tau_{ni})$ – поодинокі прямокутні функції, відповідні межам ділянок 1 – 5 на осі часу, які отримано дуальним перетворенням осі частот.

Оскільки практичний інтерес становлять лише ділянки 3 та 4, тому що саме вони дозволяють отримати оптимальне значення частоти стимуляції, обмежимося ділянками 3 і 4. Тоді вираз для F(ω) набуває вигляду

$$F_0(\omega) = F(\omega) \cdot 1(\tau_0), \tag{4}$$

де $F_0(\omega)$ – фрагмент вихідної функції, що підлягає моделюванню, $1(\tau_0)$ – одиничне прямокутне вікно, межі якого відповідають діапазону частот від 20 до 60 Гц.

Використовуючи апроксимацію функції Хевісайду у вигляді безперервної функції

$$1(t) \approx \frac{1}{2}(1 + th(kt)) = \frac{1}{1 + e^{-2kt}}, \tag{5}$$

де чим більше k, тим крутіше підйом функції, отримуємо вираз

$$F_0(\omega) = F(\omega) \cdot \frac{1}{2}(1 + th(k\,\tau_0)). \tag{6}$$

Оскільки функція, яка моделюється, F(ω) задана тільки на дискретній множині (m+1) точок $\omega_0, \omega_1, \omega_2, \ldots, \omega_m$, то необхідно мінімізувати зважену середню квадратичну помилку виду

$$\sigma^2 = \sum_{k=0}^{m} r_k \left[F_M(\omega_k) - F(\omega_k)\right]^2, \tag{7}$$

де $r_k > 0$ – деякі апріорі задані ваги; $F_м(\omega_k)$ – значення, які розраховано за моделлю; ω_k – дискретний набір значень частоти.

Як показали дослідження, у даному випадку можна ефективно використовувати поліноміальні функції виду

$$\varphi(\omega) = a_n \omega^n + a_{n-1}\omega^{n-1} + a_1\omega + a_0, \tag{8}$$

де a_i – деякі коефіцієнти; n – ступінь полінома. Тоді завдання зводиться до визначення необхідного ступеня n та визначення значень $a_i (i = \overline{1, n+1})$.

Враховуючи гладкий характер залежності, що моделюється, було випробувано поліноми ступеня від 3 до 5 [14] (рис. 4). Остаточний вибір було зроблено за поліномом ступеня n = 4, який найбільш точно і просто відображає криву електростимуляції (крива 4) і має похідну третього ступеню, що важливо для подальших теоретичних розрахунків.

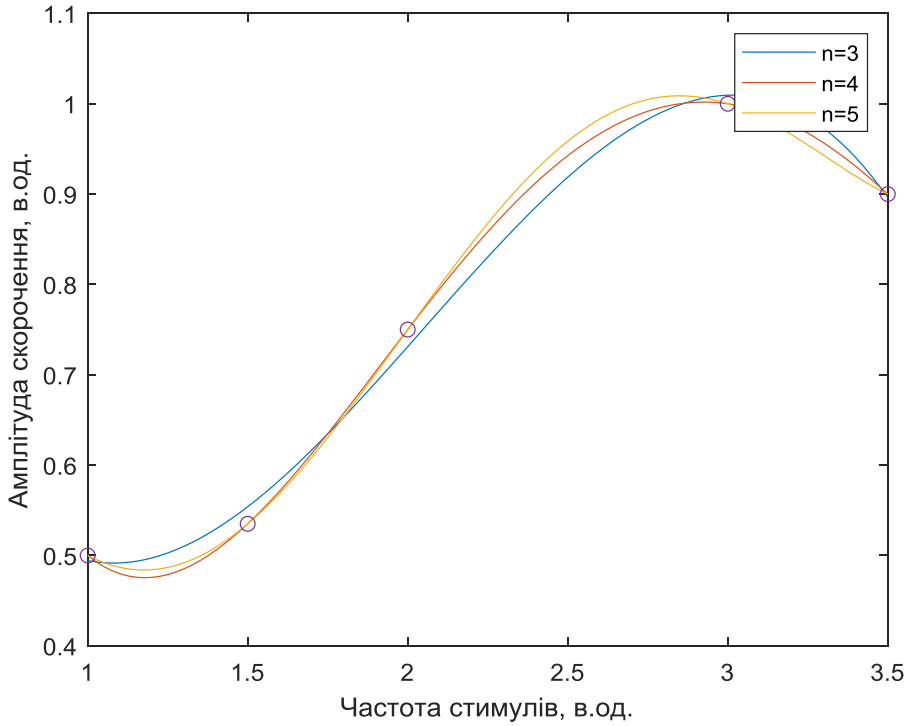


Рис. 4. Визначення оптимального ступеня полінома

Для визначення невідомих коефіцієнтів $a_0,...a_4$ реалізовано процедуру параметричної оптимізації за критерієм мінімальності функції помилки σ:

$$\sigma = \sqrt{\sum_{k=0}^{m}\left[F(\omega_k) - \varphi(\omega_k)\right]} \tag{9}$$

у просторі параметрів, що варіюються, $a_i(i=\overline{0,n})$. Розмірність простору таких параметрів дорівнює 5.

Для знаходження екстремуму цільової функції було використано метод випадкових напрямів. Відповідно до нього з деякої точки x^k простору параметрів, що варіюються, відбувається перехід у наступну точку x^{k+1} з кроком $a_k > 0$ по випадковому напряму $S^k = \left[S_1^k, S_2^k, S_3^k, S_4^k, S_5^k\right]^t$, компонентами якого є S_i^k, випадково розподілені на інтервалі [-1, 1]:

$$x^{k+1} = x^k + a_k S^k. \tag{10}$$

Критерієм зупинки процесу було виконання умови

$$\frac{\left|x^{k+1} - x^k\right|}{\left|x^k\right|} < \grave{}\varepsilon, \tag{11}$$

де ὲ – вектор, компоненти якого є граничні рівні помилки кожного параметра, що варіюються.

В результаті було отримано такий аналітичний вираз для апроксимуючої функції Fм:

$$F_M(\omega) = a_4\omega^4 + a_3\omega^3 + a_2\omega^2 + a_1\omega + a_0, \tag{12}$$

де ω – значення поточної частоти стимулів; $a = (a_0, a_1, a_2, a_3, a_4)$ – вектор параметрів моделі.

Для визначення оптимальної частоти стимулюючого впливу знайдемо першу похідну від функції:

$$F'_M(\omega) = a_1 + 2a_2\omega + 3a_3\omega^2 + 4a_4\omega^3. \quad (13)$$

Відомо, що певна точка ω^* є точкою екстремуму функції $F_м(\omega)$, якщо у цій точці похідна дорівнює нулю, або немає. Тому прирівнюємо $F'_M(\omega)$ нулю, отримуємо рівняння третього ступеня:

$$a_1 + 2a_2\omega + 3a_3\omega^2 + 4a_4\omega^3 = 0 \quad (14)$$

і розв'язуємо його щодо ω, щоб знайти значення оптимальної частоти слідування стимулів.

Перепишемо рівняння (14) у вигляді

$$\omega^3 + c\omega^3 + d\omega + e = 0, \quad (15)$$

де $c = \frac{3a_3}{4a_4}$; $d = \frac{a_2}{2a_4}$; $e = \frac{a_1}{4a_4}$.

Підстановка $\omega = y - \frac{c}{3}$ призводить до «неповного» кубічного рівняння

$$y^3 + py + q = 0, \quad (16)$$

де $p = -\frac{c^2}{3} + d$, $q = 2\left(\frac{c}{3}\right)^3 - \frac{cd}{3} + e$.

Його рішення знаходяться як

$$y_1 = A + B,$$
$$y_{2,3} = -\frac{A+B}{2} \pm i\frac{A-B}{2}\sqrt{3}. \quad (17)$$

де $A = \sqrt[3]{-\frac{q}{2} + \sqrt{Q}}$, $B = \sqrt[3]{-\frac{q}{2} - \sqrt{Q}}$, $Q = \left(\frac{p}{3}\right)^3 + \left(\frac{q}{3}\right)^3$.

У якості A і B беруться будь-які значення кубічного коріння з відповідних комплексних чисел, що задовольняють співвідношенню AB=-p/3. Якщо рівняння (15) дійсне, то (у тих випадках, коли це можливо) слід брати дійсні значення цього коріння. Якщо кубичне рівняння (15) дійсно, то воно має або один дійсний корінь і два сполучені комплексні корені, або три дійсні корені, принаймні, два з яких рівні, або три різні дійсні корені залежно від того, чи буде Q відповідно позитивно, дорівнює нулю або негативно [15].

Результати досліджень

Для знайденого оптимального значення ступеня апроксимуючого полінома n = 4 визначено коефіцієнти полінома a = (1,915 -3,020 2,075 -0,510 0,040). Виходячи з цього побудовано модельну траєкторію (рис. 5), яка адекватна експериментальній кривій електростимуляції на ділянках 3, 4 і 5 (рис. 3). Оцінено точність моделі за допомогою модуля максимального відхилення $\varepsilon = \max|y_i - y_{Mi}|$, де $y_{мі}$ – значення відгуку, розраховані за допомогою моделі, а y_i – експериментально одержані дані. Похибка не перевищує 5%. Розв'язок рівняння (13) із знайденими коефіцієнтами $a_1 – a_4$ дає значення оптимальної частоти стимулюючих сигналів у відносних одиницях ≈ 2,973, що відповідає реальній частоті f^* ≈ 59,46 Гц і збігається з експериментальними даними (60 Гц).

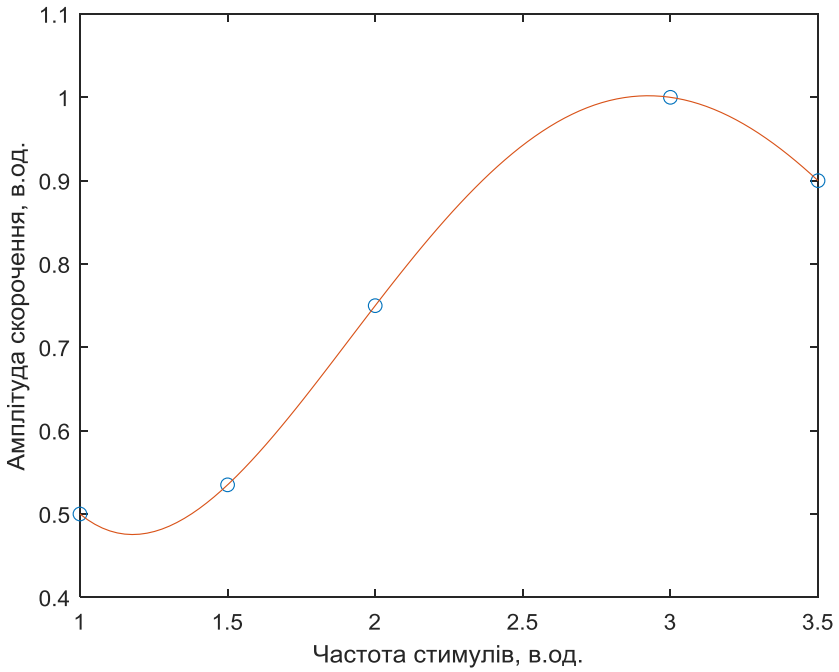


Рис. 5. Модельна траєкторія об'єкту

Перевага такого моделювання полягає також у можливості використовувати дану модель з екстраполяцією результатів, причому така екстраполяція відбувається в ході багаторазових послідовних процедур. За результатами попередньої стимуляції прогнозується подальша поведінка так, щоб оперативно вийди на індивідуальну оптимальну частоту стимуляції. Однак слід враховувати, що при цьому також можлива зміна форми електростимуляційної характеристики – затягування крутості фронтів, зміна значення амплітуди та ін. Тоді слід коригувати модель: у найпростішому випадку визначати нові значення параметрів, більш складному – використовувати структурну ідентифікацію, яка може полягати у зміні ступеня багаточлена або виборі іншої апроксимуючої функції з подальшою ідентифікацією параметрів.

Висновки

Запропоновано аналітичну модель електроміостимуляційної характеристики, яка пов'язує амплітуду скорочення м'язів з частотою стимулів. Модель отримано шляхом апроксимації експериментальної залежності поліномом четвертого ступеня. Знайдено оптимальні значення коефіцієнтів полінома, що забезпечують мінімум помилки моделювання. На цій основі отримано аналітичний вираз для розрахунку оптимальної частоти електричних стимулів. Побудовано модельну траєкторію, порівняння якої з експериментальною кривою електроміостимуляції дозволяє оцінити точність моделі на рівні 95 %. Теоретично знайдено значення оптимальної частоти стимуляції, що збігається з експериментальними даними. Отримані результати можуть бути використані для вибору оптимальних індивідуальних параметрів електростимуляції протягом ряду сеансів реабілітації. Похибка знаходиться в допустимих для практики межах, що дозволяє використовувати таку модель у ході інженерної діяльності при побудові пристроїв адаптивної електростимуляції.

Список літератури:

1. Himori K., Tatebayashi D., Kanzaki K., Wada M., Westerblad H., Lanner J. T. Neuromuscular electrical stimulation prevents skeletal muscle dysfunction in adjuvant-induced arthritis rat // PLoS ONE. 2017. № 12 (6).

2. Шайдук А. М., Останин С. А. Структура спектра электромиосигнала при хаотическом следовании отдельных импульсов // Известия Алтайского государственного университета. 2011. № 69. С. 181-185.

3. Пестриков П. П., Пестрикова Т. В. Измерительная система для регистрации сигналов поверхностной электромиографии мышц предплечья // Электронное научное издание "Ученые заметки ТОГУ". 2019. № 2 (10). С. 173–180.
4. Сафин Д. Р., Пильщиков И. С., Ураксеев М. А., Гусев В. Г. Оценка эффективности различных конструкций электродов и усилителей биосигналов в системах управления протезами // Известия высших учебных заведений. Поволжский регион. Технические науки. 2009. № 2(10). С. 88–101.
5. Шайдук А. М., Останин С. А., Юсупов Е. Р. Экспериментальное обнаружение средней частоты следования миоимпульсов по поверхностной электромиограмме // Журнал радиоэлектроники. 2011. № 9. С. 1–8.
6. Дацок О. М., Прасол І. В., Єрошенко О. А. Побудова біотехнічної системи м'язової електростимуляції // Вісник НТУ "ХПІ". Серія: Інформатика та моделювання. 2019. № 13 (1338). С. 165–175. doi: https://doi.org/10.20998/2411-0558.2019.13.15
7. Yeroshenko O., Prasol I., Datsok O. Simulation of an electromyographic signal converter for adaptive electrical stimulation tasks // Innovative Technologies and Scientific Solutions for Industries. 2021. № 1 (15). P. 113–119. doi: https://doi.org/10.30837/ITSSI.2021.15.113
8. Griffin L., Decker M. J., Hwang J. Y., Wang B., Kitchen K., Ding Z. Functional electrical stimulation cycling improves body composition, metabolic and neural factors in persons with spinal cord injury // Electromyogr Kinesiol. 2009. № 19(4). P. 614–622.
9. Bersch I., Tesini S., Bersch U., Frotzler A. Functional electrical stimulation in spinal cord injury: clinical evidence versus daily practice // Artif Organs. 2015. № 39(10). P. 849–854.
10. Yeroshenko O., Prasol I. Simulation of the electrical signal of the muscles to obtain the electromiosignal spectrum // Technology Audit and Production Reserves. 2022. № 2 (2(64)). P. 16–21. doi: http://doi.org/10.15587/2706-5448.2022.254566
11. Seibt R. Messung muskulärer Ermüdung mittels OEMG bei variierender Kraftanforderung – eine Weiterentwicklung des JASA-Verfahrens // Zbl Arbeitsmed. 2013. № 63. P 270–275. doi: https://doi.org/10.1007/BF03350866
12. Bersch I., Friden J. Electrical stimulation alters muscle morphological properties in denervated upper limb muscles // EBioMedicine. 2021. № 74. P. 1397–1407. doi: http://doi.org/10.1016/j.ebiom.2021.103737
13. Potočnik B., Holobar A. A new optical flow model for motor unit conduction velocity estimation in multichannel surface EMG // Computers in Biology and Medicine. 2017. № 83. P. 59-68. doi: http://doi.org/10.1016/j.compbiomed.2017.02.006
14. Ерошенко О. А., Прасол И. В. Построение полиномиальной математической модели электростимуляции // Інформаційні системи та технології в медицині: III Міжнародна науково-практична конференція: зб. наук. пр. Харків: Нац. аерокосм. ун-т ім. М. Є. Жуковського «Харків. авіац. ін-т». 2021. С. 80-81.
15. Справочник по математике для научных работников и инженеров / Г. Корн, Т. Корн. Москва : Наука, 2003. 832 с.

Надійшла до редколегії 22.04.2022

Відомості про авторів:

Прасол Ігор Вікторович – д-р техн. наук, доцент, Харківський національний університет радіоелектроніки, професор кафедри біомедичної інженерії; Україна; email: igor.prasol@nure.ua; ORCID: https://orcid.org/0000-0003-2537-7376.

Єрошенко Ольга Артурівна – аспірант кафедри біомедичної інженерії, Харківський національний університет радіоелектроніки, асистент кафедри електронних обчислювальних машин; Україна; email: olha.yeroshenko@nure.ua; ORCID: http://orcid.org/0000-0001-6221-7158.

УДК 53.083.912 **DOI:10.30837/rt.2022.2.209.20**

Н.В. ХМІЛЬ, канд. біол. наук, В.Г. КОЛЕСНІКОВ, канд. фіз.-мат. наук,
О.Л. АЛТУХОВ, канд. мед. наук

ОЦІНКА ПОРУШЕНЬ АДАПТАЦІЙНИХ МЕХАНІЗМІВ ПРИ СЕРЦЕВІЙ НЕДОСТАТНОСТІ МЕТОДОМ МІКРОХВИЛЬОВОЇ ДІЕЛЕКТРОМЕТРІЇ

Вступ

Процес адаптації як фундаментальна біологічна закономірність спостерігається на всіх рівнях організації біологічної системи, її спрямованість добре вивчена: від задовільної адаптації, через напругу та виснаження адаптаційних механізмів, до її зриву, що є початком будь-якого захворювання. Тому, якщо навчитися розпізнавати рівень адаптації організму і спрямованість адаптаційного процесу, стає можливим досить ефективно прогнозувати стан здоров'я. Диференціальна діагностика стану напруги адаптаційних механізмів є одним із напрямків сучасної біомедичної інженерії та найбільш складною частиною донозологічної діагностики, яка спрямована на виявлення контингенту осіб зі схильністю до захворювання, на визначення латентних випадків захворювання та захворювань, які важко розпізнаються, а також на оцінку факторів ризику [1].

Серцева недостатність супроводжує найважчі захворювання міокарда – кардіоміопатії – дилатаційну кардіоміопатію (ДКМП), гіпертрофічну кардіоміопатію (ГКМП) та ішемічну кардіоміопатію (ІКМП), що характеризуються дисфункцією скорочувальної та провідної здатності міокарда. Ці захворювання охоплюють різні вікові та соціальні групи, вони мають різну етіологію, від спадкової схильності по аутосомно-домінантному, аутосомно-рецесивному типу успадкування та успадкуванню зчепленого з Х-хромосомою, до перенесеної вірусної інфекції та впливу токсичних речовин і хімічних факторів [2].

Одним із проявів дезадаптації при серцевій недостатності є порушення механізмів реалізації ланцюга "сигнал-функція", тобто мембранно-рецепторних взаємодій, що забезпечують передачу гормонального сигналу в клітину. В умовах фізіологічної норми динамічна структура β-адренорецепторів мембрани кардіоміоцитів проявляється залежно від гомеостазу, дії фармакологічних препаратів, фізіологічного стану та регулюється природними рецепторними стимуляторами та модуляторами [3]. У патогенезі серцевої недостатності, крім наукових доказів про генералізовані порушення мембранних іонних потоків, розглядається концепція дисбалансу синтезу та деградації вторинного месенджера – циклічного аденозинмонофосфату (цАМФ). Активація симпатоадреналової системи, гормональна надстимуляція β-адренорецепторів кардіоміоцитів адреналіном і, як наслідок, надмірне збільшення концентрації цАМФ, призводить до дисфункції та гибелі кардіоміоцитів [4, 5]. Внаслідок порушення системи передачі гормонального сигналу на молекулярно-клітинному рівні спостерігається збільшення розміру лівого шлуночка міокарда та збільшення внутрішньошлуночкового тиску внаслідок периферичної вазоконстрикції та підвищення внутрішньосудинного обсягу. Крім того, гормональна стимуляція адреналіном та норадреналіном може спричинити гіпертрофію міокарда, одночасно обмежуючи здатність коронарних артерій забезпечувати кровопостачання шлуночкової стінки [6]. Огляд літературних даних показав, що аденілатциклазна система (АЦС), загалом, відповідає за розвиток стресу на молекулярно-клітинному рівні, і порушення її функціонування відбиваються на ранніх стадіях розвитку патологічного стану в кардіоміоцитах. Більшість клініко-інструментальних методів діагностики не розкривають патогенетичних механізмів кардіальної патології, і тому питання ранньої діагностики серцевої недостатності, прогноз перебігу захворювання, а також контроль ефективності лікувальних заходів залишається відкритим. На сьогодні розробка моделей тестування певних ланцюгів, залучених в трансмембранній передачі сигналів, актуальна як для діагностичних цілей, так і для вибору шляхів терапевтичного впливу.

Мікрохвильова діелектрометрія області γ-дисперсії іелектричної проникності вільної води є прецизійним методом оцінки гідратації макромолекулярних білкових комплексів мембрани та біологічних рідин [7]. Ефективність застосування цього методу в діагностичному алгоритмі соціально значущих алергодерматозів [8], а також дилатаційної кардіоміопатії [9] підтверджена експериментами в умовах клініки на базі лабораторій алергології та біохімії ДУ «Інститут дерматології та венерології НАМН України» та ДУ «Інститут терапії ім. Л.Т. Малої НАМН України».

Мета роботи – оцінка ефективності мікрохвильової діелектрометрії в алгоритмі донозологічної діагностики серцевої недостатності на основі дослідження діелектричної проникності суспензії еритроцитів в області γ-дисперсії діелектричної проникності вільної води.

Основні положення

В якості моделі для дослідження напруги адаптаційних механізмів при серцевій недостатності були обрані еритроцити, що обумовлено наявністю на їхній мембрані β-адренорецепторів, функціонально та структурно подібних до β-адренорецепторів мембрани кардіоміоцитів міокарда. Досліджувалась суспензія еритроцитів трьох груп пацієнтів: 1) група – пацієнти з підтвердженим діагнозом ДКМП (n=12), ІКМП (n=15); 2) група – пацієнти групи ризику, відібрані на основі анамнезу зі спадковою схильністю (n=23); 3) група – здорові донори (n=30). На попередньому етапі всім хворим та здоровим донорам проводилися рентгенологічні, ультразвукові та клініко-інструментальні дослідження; клінічний діагноз встановлювався на підставі анамнезу та клінічної картини. У всіх обстежених було отримано письмову згоду щодо участі в дослідженні. При виконанні роботи дотримувалися принципів та рекомендацій, прописаних у Гельсінській декларації прав людини та відповідних законах України про охорону здоров'я пацієнтів, моральні та етичні стандарти.

Моделювання напруги адаптаційних механізмів проводилося *in vitro* шляхом тестування мембранних β-адренорецепторів еритроцитів селективними стимуляторами, блокаторами та модуляторами клітинної відповіді за методикою, описаною в науковій роботі [10].

Вимірювання діелектричної проникності еритроцитів проводилося за допомогою апаратурно-реєструючого комплексу на базі НВЧ-діелектрометра (модифікація А-17) (рис. 1). Фіксована частота генерації діода Ганна f = 37,7 ГГц, яка належить області γ-дисперсії діелектричної проникності вільної води, при накладенні змінного електромагнітного поля, сприяє вимірюванню гідратації рецепторних макромолекулярних комплексів – вільної, або об'ємної води та зв'язаної води, яка є «реплікою» конформаційній структурі білків мембрани.

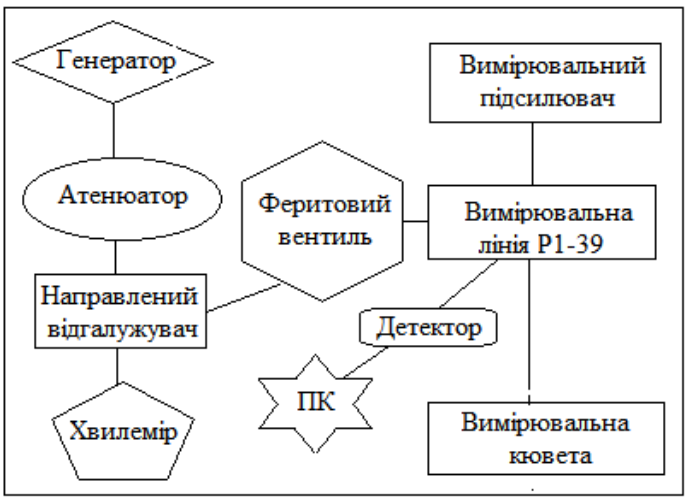


Рис. 1. Блок-схема апаратурно-реєструючого комплексу, модифікованого для вимірювання діелектричної проникності суспензії клітин та біологічних рідин

До складу генераторної частини НВЧ-діелектрометра входить генератор Ганна, атенюатор, направлений відгалужувач, хвилемір та феритовий вентиль. Вимірювальна частина

НВЧ-діелектрометра включає вимірювальну лінію з вимірювальною кюветою і вимірювальний підсилювач. Конструкція та розміри елементів вимірювальної кювети, а саме розміри, товщина та матеріал віконець кювети, висота робочого об'єму розраховані на основі експериментальних даних, а також результатів математичного моделювання на основі розв'язання задачі розсіювання електромагнітних хвиль [11]. Схема вимірювальної хвилевідної кювети без спеціальних затискачів та посадкових штифтів наведено на рис. 2.

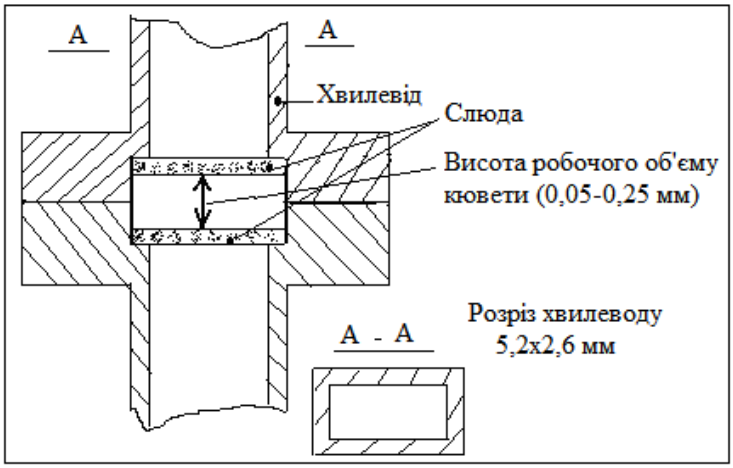


Рис. 2. Схема робочої частини хвилеводної вимірювальної кювети

У процесі діелектричних вимірювань знімали розподіл електричного поля за допомогою вимірювальної лінії Р1-39 шляхом пересування зонда вздовж щілини вимірювальної лінії. На рис. 3 представлена схема хвилеводу на ділянці від вимірювальної лінії до кювети для розрахунку розподілу поля стоячої хвилі у хвилеводі.

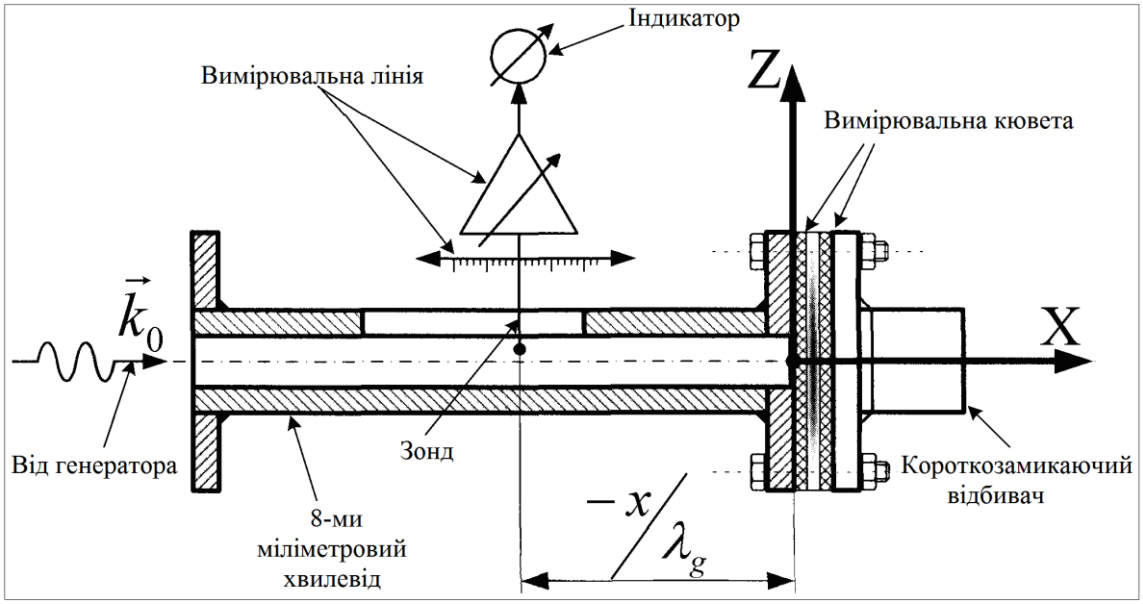


Рис. 3. Вимірювальна секція експериментальної установки, що складається з вимірювальної кювети, хвилеводної вимірювальної лінії та короткозамикального (КЗ) хвилеводного відбивача НВЧ-діапазону. Показано обрану систему координат (*X, Z*) та положення зонда по осі *X* вимірювальної лінії відносного вхідного вікна вимірювальної кювети, нормовану на довжину хвилі у хвилеводі $\lambda_g(x/\lambda_g)$. *k0* – хвильове число, що характеризує напрямок руху хвилі та періодичність поширення хвилі у просторі

Реєстрація та обробка експериментальних даних забезпечувалася персональним комп'ютером (ПК). Реєстрація електромагнітного відгуку від біологічної системи еритроцитів проводилася на ділянках спектра електромагнітного поля вільних від шумових спектрів навколишнього фону. Електромагнітний відгук – це сигнал, отриманий від суспензії еритроцитів, який реєструється на виході детектора хвилеводної лінії Р1-39. Сигнал надходив з детектора

хвилеводної лінії Р1-39 на підсилювач, з виходу якого через аналого-цифровий перетворювач (АЦП) подавався на персональний комп'ютер (ПК). В якості детектора використовувався діод 3А123 кристалічно-планарної структури з бар'єром Шоттки [12, 13]. Відносна похибка за ε' склала ±0,5 %, абсолютна похибка за ε', після відповідної обробки із застосуванням програм накопичення та фільтрації, становила ±0,008 х 10^{-12} Ф/м.

Інтерпретація отриманих експериментальних даних полягала в тому, що процес взаємодії біорегуляторів з біологічною системою супроводжується збільшенням або зменшенням відносної кількості вільної води, що призводить до зміни реальної частини комплексної діелектричної проникності ε'. Вимірювання комплексної діелектричної проникності хвилевідним методом потребує також вимірювання уявної частини ε'', але ці вимірювання пов'язані зі значною доробкою вимірювальної бази.

Отримані результати опрацьовували статистично. Проведено розрахунки середнього арифметичного (M), стандартного відхилення (m). За допомогою непараметричного U-критерію Манна – Уітні визначали вірогідність отриманих результатів. Відмінності вважали статистично значущими за $p < 0,05$. Статистичну обробку результатів вимірювань проводили з використанням пакета прикладних програм Excel, Statistika 6.0 [14] та SigmaStat3.5.

Результати експериментальних спостережень та їх аналіз

Експериментальне дослідження суспензії еритроцитів хворих пацієнтів показало різницю в параметрах діелектричної проникності відносно практично здорових донорів (рис. 4, 5). У випадку групи пацієнтів з підтвердженим діагнозом ДКМП реєстрували нівелювання дії гормонального стимулятора – адреналіну внутрішньоклітинним модулятором ПГЕ2, що проявилося в значному зменшенні відносної кількості вільної води – $\Delta\varepsilon' = 0,008 \pm 0,008$ х 10^{-12} Ф/м. Подібний захист мембрани еритроцитів проявився також і при комбінованій дії адреналіну та корданумy: $\Delta\varepsilon' = 0,105 \pm 0,008$ х 10^{-12} Ф/м; цей ефект характерний для еритроцитів практично здорових донорів [15]. Одночасна дія трьох біологічних регуляторів (адреналін, ПГЕ2 та корданум) призвела до суттєвої блокади β-адренорецепторів, щоб протистояти надмірній активації адреналіном при пошкодженій регуляції АЦС, при цьому $\Delta\varepsilon'$ склала $0,026 \pm 0,008$ х 10^{-12} Ф/м (рис.4).

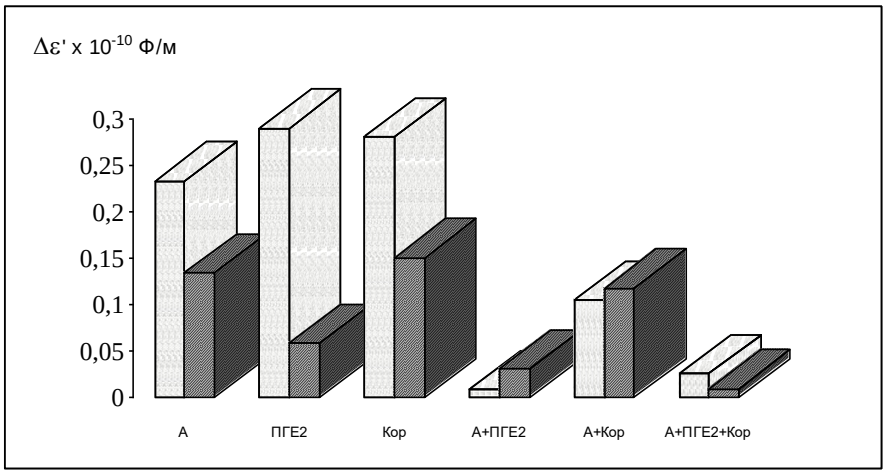


Рис. 4. Зміна діелектричної проникності від еритроцитів хворих на ДКМП (n=12, гістограми сірого кольору) та пацієнтів групи ризику (n=23, заштриховані гістограми) при специфічній стимуляції, модуляції та блокаді β-адренорецепторів мембрани клітин відносно зразків еритроцитів практично здорових донорів: А – адреналін, ПГЕ2 – простагландин Е2, Кор – корданум. (абсолютна похибка за всіма значеннями ε' становить ±0,008 х 10^{-12} Ф/м). Відмінності за ε' відносно до показників контрольних зразків вірогідні ($p < 0,05$).

Зміна діелектричної проникності суспензії еритроцитів групи ризику була менш вираженою, але також спостерігалася тенденція до блокування β-адренорецепторів, особливо при комбінованій дії адреналіну, ПГЕ2 та корданумy, $\Delta\varepsilon' = 0,009 \pm 0,008$ х 10^{-12} Ф/м. Аналізуючи

діелектричну проникність суспензії еритроцитів групи ризику, слід зазначити формування передумов до зміни в функціонуванні АЦС та розвитку серцевої недостатності, яку супроводжує ДКМП.

В умовах ІКМП ефекти блокування β-адренорецепторів – ПГЕ2 та корданумом були виражені слабше ніж при ДКМП, різниця в діелектричній проникності у випадку комбінованої дії адреналіну та ПГЕ2 склала $\Delta\varepsilon' = 0{,}088 \pm 0{,}008 \times 10^{-12}$ Ф/м, для випадку потрійної системи (А+ПГЕ2+Кор) $\Delta\varepsilon' = 0{,}008 \pm 0{,}008 \times 10^{-12}$ Ф/м (рис. 5). Тенденція до проявів серцевої недостатності внаслідок ІКМП також спостерігалася, як і при ДКМП, особливо при застосуванні потрійної системи (А+ПГЕ2+Кор), при цьому $\Delta\varepsilon'$ склала $0{,}009 \pm 0{,}008 \times 10^{-12}$ Ф/м

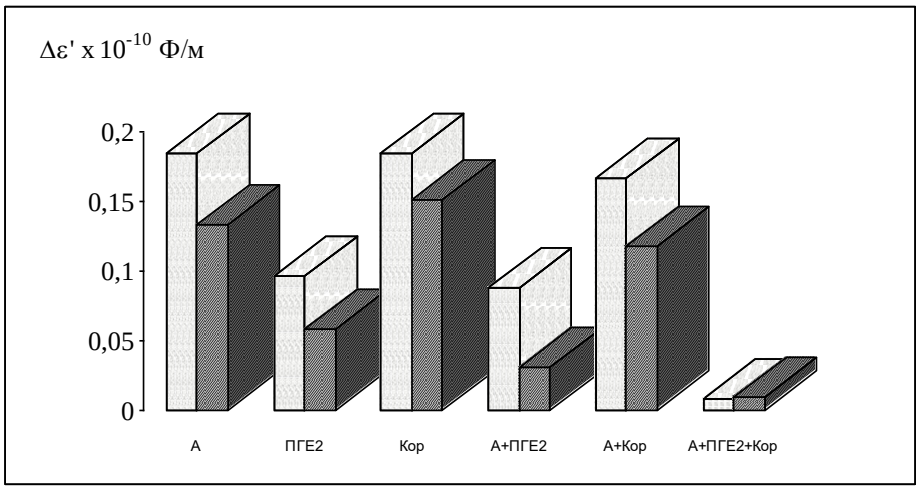


Рис. 5. Зміна діелектричної проникності від еритроцитів хворих на ІКМП (n=15, гістограми сірого кольору) та пацієнтів групи риску (n=23, заштриховані гістограми) при специфічній стимуляції, модуляції та блокаді β-адренорецепторів мембрани клітин відносно зразків еритроцитів практично здорових донорів: А – адреналін, ПГЕ2 – простагландин Е2, Кор – корданум (абсолютна похибка за всіма значеннями ε' становить $\pm 0{,}008 \times 10^{-12}$ Ф/м). Відмінності за ε' відносно до показників контрольних зразків вірогідні ($p < 0{,}05$)

Таким чином, підхід на основі тестування селективними стимуляторами та блокаторами β-адренорецепторів внутрішньоклітинної сигнальної системи в області γ-дисперсії діелектричної проникності вільної води є ефективним для прогнозування змін на молекулярно-клітинному рівні, які є провісниками швидкоплинних процесів, що можуть привести до серцевої недостатності.

Висновки

Мікрохвильова діелектрометрія може бути запропонована як один із чутливих методів в алгоритмі донозологічної діагностики серцевої недостатності, при цьому параметр діелектричної проникності є надійним критерієм в розробці превентивних заходів для своєчасного попередження дисфункції міокарда.

Перспектива тестування порушень молекулярно-клітинних механізмів у клінічних умовах пов'язана із розробкою алгоритмів індивідуальної форми терапевтичної корекції при серцевій недостатності.

Список литературы:

1. Маракушин Д.І., Чернобай Л.В., Ісаєва І.М., Кармазіна І.С., Ващук М.А., Алексеєнко Р.В., Булініна О.Д., Зеленська Г.М. Функціональні резерви організму як показник ефективності регуляторних процесів, що забезпечують адаптацію організму до дії факторів навколишнього середовища // Український журнал медицини, біології та спорту. 2020. Т. 5, №1(23). С. 21–28.

2. Maron B.J, Towbin J.A., Thiene G., Antzeevitch C., Corrado D., Arnett D., Moss A.J., Seidman C.E., Young J.B. Contemporary definitionsnand classification of the cardiomyopathies: an American heart association scientific statement from the council on clinical cardiology, heart failure and transplantation committee; quality of care and outcomes research and functional genomics and translational biology interdisciplinary working groups; and council on epidemiology and prevention // Circulation. 2006. Vol. 113, No 14. P. 1807–1816.

3. Motiejunaite J., Amar L., Vidal-Petiot E. Adrenergic receptors and cardiovascular effects of catecholamines // Annales Endocrinologie (Paris). 2021. Vol. 82, No 3-4. P. 193–197.
4. Boularan C., Gales C. Cardiac cAMP: production, hydrolysis, modulation and detection // Frontiers in Pharmacology. 2015. Vol. 6.(203). Режим доступу: https://www.frontiersin.org/article/10.3389/fphar.2015.00203
5. Martin J.Lohse, Stefan Engelhardt, Thomas Eschenhagen. What is the role of β-adrenergic signaling in heart failure? // Circulation Research. 2003. Vol. 93. P. 896–906.
6. Хроническая сердечная недостаточность: достижения, проблемы, перспективы / Л.Т. Малая и др. Харьков : Торсинг, 2002. 768 с.
7. Солошенко Э.Н., Кондакова А.К., Колесников В.Г., Хмель Н.В., Шевченко З.М., Ярмак Т.П., Беляев Г.М. Исследование параметров гидратации и поверхностного натяжения плазмы крови больных ограниченной склеродермией // Дерматология и венерология. 2015. № 1(67). С. 69–74.
8. Солошенко Е.Н., Кондакова А.К., Хміль Н.В., Колесніков В.Г. Діагностичне значення методу визначення діелектричної проникності крові для виявлення сенсибілізації до пеніциліну G і цефтріаксону // Дерматология и венерология. 2021. № 2 (92). С. 25–30.
9. Хмель Н.В., Алтухов А.Л., Колесников В.Г., Алтухов А.А. Визуализация трансдукции клеточного сигнала методом микроволновой диэлектрометрии при дилатационной кардиомиопатии // Бионика интеллекта. 2020. №1(94). С. 91–99.
10. Щеголева Т.Ю., Колесников В.Г., Древаль Н.В., Будянская Э. Н., Зюганова Л. Ф. Анализ ключевых механизмов систем регуляции клеток для разработки экспресс-тестов индивидуальных особенностей организма при популяционных исследованиях // Експериментальна і клінічна медицина. 2004. №1. С. 89–93.
11. Исследование диэлектрических характеристик биообъектов в миллиметровом диапазоне радиоволн / Т. Ю. Щеголева. Киев : Наук. думка, 1996. 187 с.
12. Древаль Н.В., Колесніков В.Г., Камєнєв Ю.Ю., Філімонова А.О. Спосіб визначення впливу на біологічний об’єкт. Патент на корисну модель № 17488, МПК A61N 5/02, дата публікації 15.09.2006. Бюл. №9.
13. Древаль Н. В. Применение миллиметровых и субмиллиметровых радиоволн и их комбинации в исследовании биологических объектов : дис. … канд. биол. наук: 03.00.02 / Древаль Наталия Владимировна. Симферополь. 2009. 163 с.
14. Статистический анализ медицинских данных: применение пакета прикладных программ STATISTIKA / О. Ю. Реброва. Москва : МедиаСфера, 2000. 312 с. Режим доступа: https://www.studmed.ru/view/rebrova-oyu-statisticheskiy-analiz-medicinskih-dannyh_0149fe87d1d.html.
15. Хміль Н.В. Дослідження електромагнітного сигналу клітин методом мікрохвильової діелектрометрії при ділатаційній кардіоміопатії / Н.В. Хміль, В.Г. Колесніков, О.Л. Алтухов // Матеріали 9-ї Міжнар. наук.-техн. конф. «Інформаційні системи та технології» ІСТ-2020, 17-20 листопада, Харків. С. 115–118.

Надійшла до редколегії 02.05.2022

Відомості про авторів:

Хміль Наталія Володимирівна – канд. біол. наук, Харківський національний університет радіоелектроніки, доцент кафедри біомедичної інженерії, Україна; email: nataliia.khmil@nure.ua; ORCID: https://orcid.org/0000–0001–7916–5921

Колесніков Володимир Григорович – канд. фіз.-мат. наук, Інститут радіофізики та електроніки ім. О Я. Усикова Національної академії наук України, старший науковий співробітник, Україна; email: kolesnik@ire.kharkov.ua; ORCID: https://orcid.org/0000–0001–7822–4774

Алтухов Олександр Леонідович – канд. мед. наук, ДУ “Національний інститут терапії імені Л. Т. Малої Національної академії медичних наук України”, завідувач рентгенологічного відділення, Україна; email: therapy@amnu.gov.ua

УДК 621.7.075 **DOI:10.30837/rt.2022.2.209.21**

Є.А. РАЗУМОВ-ФРИЗЮК, канд. техн. наук, Д.В. ГУРІН, Д.О. НІКІТІН,
Р.Є. СТРІЛЕЦЬ, Д.С. БЛИЗНЮК

МОДЕЛЮВАННЯ ШНЕКОВОГО ЕКСТРУДЕРА ДЛЯ FFF 3D ДРУКУ

Вступ

В наш час технології адитивного тривимірного прототипування постійно розвиваються. Однією з найпопулярніших технологій 3D друку є технологія FFF – Fused filament fabrication («виробництво способом наплавлення ниток»). У якості матеріалу для принтерів, що функціонують за цією технологією, використовується філамент – прутки діаметром 1,75 або 2,85 мм, що виготовлені з термопластів. Вартість філаменту може бути досить значною у порівняні з сировиною, з якої він виробляється. Тому досить перспективним є напрямок розробки для 3D принтерів шнекових екструдерів, які у якості матеріалу використовують гранульовані термопласти або подрібнену вторсировину. На даний час промислові підприємства не виробляють шнекові екструдери. Існує лише декілька проєктів, що використовують стандартні шнеки та циліндри для термопласти-автоматів і не є оптимізовані для умов 3D друку. Автори пропонують моделювання шнекового екструдеру, якій відповідає основним вимогам адитивного виробництва за технологією FFF.

Вибір шнека

При розробці шнекового екструдера для 3D принтера необхідно:

- максимально зменшити масогабаритні параметри екструдера, що дозволить збільшити швидкість друку через зменшення маси та як наслідок інерційності каретки екструдера, а також зменшити вартість координатної системи 3D принтера через зменшення необхідної жорсткості всієї конструкції;
- забезпечити необхідну лінійну продуктивність шнекового екструдера, яка повинна перевищувати максимальну швидкість друку 3D принтера (швидкість переміщення екструдера в робочому режимі).

Зображення шнека представлено на рис. 1.

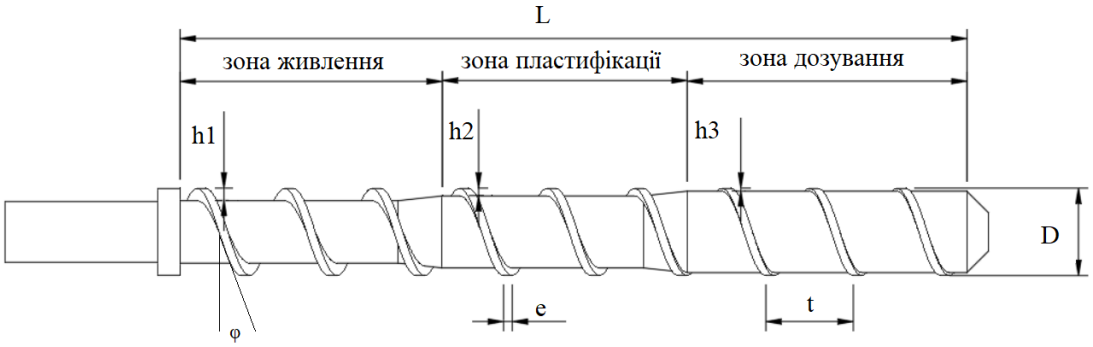


Рис. 1. Шнек екструдера

Основні геометричні параметри шнека:

- діаметр D;
- довжина L;
- крок гвинтової нарізки t;
- глибина каналу по зонах (глибина нарізки) h;
- ширина гребеня витка e;

- величина зазору між гребенем шнека та внутрішньою стінкою циліндра δ;
- кут підйому гвинтової лінії нарізки шнека φ;зонність;
- число заходів нарізки шнека λ (найчастіше λ = 1) [4, 5].

Для переробки термопластів зазвичай застосовуються циліндричні шнеки з постійним кроком та змінною глибиною гвинтового каналу. Вони порівняно прості у виготовленні та забезпечують високу продуктивність. Діаметр шнеків вітчизняних екструдерів регламентований ГОСТом 14773 та становить розмірний ряд: 20; 32; 45; 63; 90; 125; 160; 200; 320; 450; 630 мм. Чим більший діаметр шнека, тим вища продуктивність екструдера. Довжина шнеків *L* характеризується її відношенням до діаметра *D* (*L/D*). Це співвідношення може змінюватися в інтервалі 8 – 40 [2, 6]. Значення *D* та *L/D* є основними характеристиками одношнекового екструдера та вказуються у його марці. Для мінімізації масогабаритних параметрів екструдера вибрано шнек марки ЧП 20х8. Цей шнек має найменші серед стандартних шнеків розміри та масу, що значно впливає на швидкість переміщення екструдера в режимі друку через найменшу інерцію та навантаження на крокові двигуни осей *X* та *Y*.

Для перевірки достатності продуктивності даного екструдера необхідно розрахувати лінійну продуктивність шнекового екструдера, тобто. довжину дроту пластику, який екструдується за одну секунду. Ця величина залежатиме від діаметра встановленого сопла (передбачається використовувати сопла з діаметром від 1 до 5 мм). Отримане значення лінійної продуктивності має перевищувати максимальну швидкість друку екструдера 3D принтера, заявлену в технічному завданні, для екструдера, що розглядається, максимальна швидкість друку (переміщення екструдера в робочому режимі) повинна становити 50 мм/с.

Для визначення лінійної продуктивності шнека запропоновано формулу [1]:

$$L = \frac{4Q}{\pi d^2}, \tag{1}$$

де L – лінійна продуктивність екструдера, см/хв.; Q – об'ємна продуктивність, см^3/ хв; d – діаметр використовуваного сопла, см.

Екструдер передбачається розробляти одношнековий, без зони дегазації, однозахідний, зі змінною глибиною спірального каналу (зі змінною глибиною нарізки), що спричинено зниженням масогабаритних характеристик та вартості виготовлення екструдера.

Розрахунок параметрів шнека

Необхідно розрахувати параметри шнека для подальшого моделювання екструдера. Оскільки обраний шнек зі змінною глибиною спірального каналу, то насамперед необхідно визначити розміри зон живлення, пластифікації та дозування. Їхні розміри є стандартними для різних пластмас. Для подальшого розрахунку вибрано наступні співвідношення розмірів зон шнека представленій у табл. 1.

Таблиця 1

Зона живлення	Зона пластифікації	Зона дозування
0,25L	0,35L	0,4L

Для обраної довжини шнека 160 мм зона живлення має розмір 40 мм, зона пластикації – 56 мм, зона дозування – 64 мм.

Далі необхідно розрахувати або вибрати зі стандартних усі параметри шнека, представлені рис. 1.

Крок гвинтової нарізки *t* шнека рекомендується приймати постійним по довжині шнека (для шнеків зі змінною глибиною нарізки), він вибирається в діапазоні [1, 3]:

$$t = (0{,}8...1{,}2)D \tag{2}$$

Зазвичай крок приймається рівним діаметру шнека, тобто $t = D$, що відповідає куту підйому гвинтового каналу 17°42, що одночасно забезпечує гарне живлення екструдера матеріалом та знижує вартість виробництва шнека.

Глибина гвинтового каналу шнека.

Глибини гвинтового каналу шнека *h* у різних зонах визначаються за формулами [2, 6]:

$$h_1 = (0{,}12...0{,}16)D \tag{3}$$

де h_1 – глибина гвинтового каналу у зоні живлення.

Так як екструдер передбачається використовувати для друку різними матеріалами, коефіцієнт формули обраний усереднений 0,14. Величина гвинтового каналу в зоні живлення становить 2,8 мм:

$$h_3 = 0{,}5\left[D - \sqrt{D^2 - \frac{4h_1}{i}\left(D - h_1\right)}\right], \tag{4}$$

де h_3 – глибина гвинтового каналу у зоні дозування; i – ступінь стиснення матеріалу.

Ступінь стиснення матеріалу є величиною, що вибирається зі стандартного для кожного полімеру діапазону. У зв'язку з розробкою екструдера для різних матеріалів ступінь стиснення вибирається рівним 4, так як ця величина потрапляє в діапазони всіх пластиків, які планується використовувати: ABS, PLA, PET, PC тощо. Розмір гвинтового каналу у зоні дозування становить 0,621мм;

$$h_2 = h_1 - \frac{h_1 - h_3}{L} L_0, \tag{5}$$

де h_2 – глибина гвинтового каналу у зоні пластикації, мм; L – довжина шнека, мм; L_0 – довжина шнека до зони стиснення, мм;

$$L_0 = L - L_H, \tag{6}$$

L_H – довжина напірної частини шнека, мм.

$$L_H = (0{,}4...0{,}6)L. \tag{7}$$

Приймаємо L_H = 0,5 L. Відповідно до розрахунків глибина гвинтового каналу в зоні пластикації становить 1,71 мм.

При виборі товщини витка *e* (ширини гребеня) необхідно враховувати, що збільшення товщини витка призводить до підвищення витрати потужності, а зменшення її – до утворення значного потоку витоку через проміжок між внутрішньою поверхнею матеріального циліндра та зовнішньою поверхнею витка шнека. Ширину гребеня витка шнека рекомендується приймати

$$e = (0{,}06...0{,}1)D. \tag{8}$$

У зв'язку з тим, що шнек для екструдера обраний максимально короткий, збільшення товщини витка не може значно підвищити витрату потужності, а витік через проміжок між шнеком і циліндром призведе до некоректної роботи екструдера – недоекструзії, проблем з відкатами (retrack), таким чином слід вибирати максимально допустиму товщину витка, що становить 2 мм.

Радіальний проміжок між внутрішньою поверхнею матеріального циліндра і зовнішньою поверхнею витка шнека рекомендується приймати

$$\delta = (0,002...0,005)D. \quad (9)$$

Зменшення радіального проміжку призводить до підвищення вартості виготовлення шнека і циліндра у зв'язку зі зменшенням допусків, але водночас призводить до зменшення витоку матеріалу і як наслідок підвищення якості друку. Радіальний проміжок вибирається рівним 0,04 мм.

Розробка тривимірної моделі екструдера

Визначальний вплив на продуктивність екструдера має дозувальна зона шнека. Ефективність дозуючої зони залежить від геометричних параметрів самого шнека. Віддача ж шнекового екструдера в цілому залежить не тільки від геометричних розмірів шнека та числа обертів, але й значною мірою від конструкції голівки, що формує [7].

На основі гідродинамічного підходу до аналізу взаємодії робочих органів з матеріалом, що переробляється, в дозуючій зоні екструдера прийнято розглядати три складові потоку руху розплаву:

- потік розплаву, що рухається міжвитковим простором у напрямку від зони завантаження до зони дозування вздовж осі шнека; виникає внаслідок обертання шнека щодо циліндра;
- потік розплаву, що рухається у протилежному напрямку, що викликано перепадом тиску P по довжині шнека;
- потік витоку, що рухається в проміжку між зовнішньою поверхнею витків шнека та внутрішньою поверхнею матеріального циліндра у напрямку від зони дозування.

Подібний поділ на три потоки в каналі шнека слід вважати умовним, так як протитечії практично не існує, а має деяке обмеження прямого потоку, що виникає в результаті опору сопла [8, 9]. Сопло – це знімний технологічний інструмент, призначений для екструзії пластмаси у процесі 3D друку.

Об'ємна продуктивність екструдера, залежно від опору сопла та конструкції дозуючої зони, може бути виражена співвідношенням

$$Q = \frac{AK}{K + B + C} n; \quad (10)$$

де Q – об'ємна продуктивність, см^3/хв; K – коефіцієнт опору сопла екструдера, см^3; n – частота обертання шнека, хв$^{-1}$; A – постійна прямого потоку, см^3; B – постійна зворотного потоку, см^3; C – постійна потоку витоків, см^3.

Значення постійних прямого потоку A, зворотного B та потоку витоків C визначаються наступним чином:

$$A = \frac{\pi^3 (t - \lambda e)\sigma}{a + t^2 b}; \quad (11)$$

$$B = \frac{\pi t (t - \lambda e)}{12 L_H \left(a + t^2 b\right)}; \quad (12)$$

$$C = \frac{\pi D \delta^3 t^2}{10 e L_H \sqrt{\pi^2 D^2 + t^2}}; \quad (13)$$

де D – зовнішній діаметр шнека, см; t – крок нарізки шнека, см; e – ширина гребеня нарізки, см; λ – кількість заходів; δ – величина проміжку між гребенем шнека та внутрішньою стінкою циліндра, см; L_H – довжина зони дозування, см; σ, a, b – коефіцієнти, що характеризують конструкцію шнека зі змінною глибиною нарізки визначаються за такими формулами:

$$\sigma = 1 - \frac{6,9D}{2\left(h_2 - h_3\right)} \lg \frac{h_2}{h_3} + \frac{D^2}{2h_2h_3}; \quad (14)$$

$$a = \frac{\pi^2}{h_2 h_3}\left[\frac{D\left(h_2 + h_3\right)}{2h_2h_3} - 1\right]; \quad (15)$$

$$b = \frac{2,3}{(h_2 - h_3)D^3} lg \frac{h_2(D+d_3)}{h_3(D+d_1)} + \frac{2h_2h_3 + (h_2+h_3)2D}{2D^2h_2^2h_3^2}; \quad (16)$$

де d_1 – діаметр осердя (валу) шнека під завантажувальною вірвою, см:

$$d_1 = D - 2h_1; \quad (17)$$

d_3 – діаметр сердечника шнека у зоні дозування, см:

$$d_3 = D - 2h_3. \quad (18)$$

За результатами розрахунків отримано:

- σ = 153,789;
- a = 19452,553;
- b = 11,892.

В результаті постійний прямий потік A = 0,439 см^3.

Постійна зворотного потоку B = 6,038·10^{-6} см^3.

Постійна потоку витоків C = 1,524·10^{-8} см^3.

Для розрахунку об'ємної продуктивності екструдера також необхідно визначити опір сопла [1, 10]. Основною геометричною характеристикою сопла є її загальний коефіцієнт опору К, який визначається як сума коефіцієнтів опору окремих простих по геометрії ділянок k_1, k_2…k_i за допомогою рівняння

$$K = \frac{1}{\frac{1}{k_1} + \frac{1}{k_2} + ... + \frac{1}{k_i}}, \quad (19)$$

де k_1, k_2 … k_i – приватні коефіцієнти опору ділянок каналу із простою геометричною формою. При розрахунку K сопло умовно розбивають на ділянки, що відрізняються конфігурацією, і для кожної ділянки визначають частковий коефіцієнт опору.

Для розрахунку коефіцієнта опору сопла екструдера необхідно розглянути розроблену тривимірну модель сопла представлену на рис. 2.

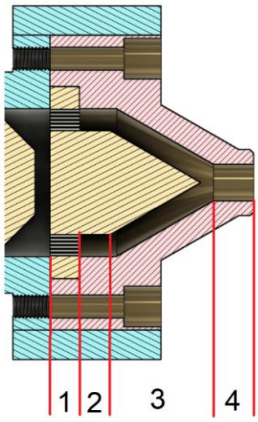


Рис. 2. Схематичне зображення сопла шнекового екструдера

Сопло можна розділити на чотири ділянки для коефіцієнта опору.

Перша ділянка – елементи фільтрації, він призначається для очищення розплаву від різноманітних твердих включень, що неминуче потрапляють у матеріал на різних стадіях його виробництва та транспортування, а також від неповністю проплавлених у каналі черв'яка частинок матеріалу, які іноді з'являються на виході з цього каналу при роботі екструдера. На таких шнекових пристроях встановлюють сито-змінні фільтрувальні пристрої. Весь набір сіток підтримується решіткою, ділянка встановлюється між циліндром і соплом, що служить для спрямування потоку розплаву, що виходить із останнього витка шнека. Вона є сталевим диском товщиною приблизно 1/5 діаметра циліндра. Для екструдера, що описується, товщина складе 4 мм. При розрахунку коефіцієнта опору в голівці опорір у решітці та фільтрі також повинні враховуватися. Коефіцієнт опору фільтра, см^3:

$$K_{\phi} = \frac{nFd_0^2}{32\delta_{\phi}}, \quad , \tag{20}$$

де n – кількість фільтрувальних елементів; F – площа фільтрувального елемента, см^2; δ_{ϕ} – товщина фільтруючих елементів, см.

Для фільтра вибрано середню сітку з діаметром дроту. d = 0,16 мм та розміром вічок d_o = 0,025 см; кількість сіток приймаємо n = 3; площа фільтрувального елемента F = 1,608 см^2; товщина фільтруючих елементів $\delta_ф = 2dn = 2 \cdot 0{,}16 \cdot 3 = 0{,}096$ см; коефіцієнт опору фільтра $K_ф$ = 0,0000586.

Коефіцієнт опору решітки, см^3:

$$K_p = \frac{\pi z d_0^4}{128\delta_p}, \quad , \tag{21}$$

де z – кількість отворів у решітці; d_0 – діаметр отворів, см; $\delta_р$ – товщина решітки, см.

Товщина решітки обрана $\delta_р$ = 0,3 см, діаметр отворів d_0 = 0,04 см, кількість отворів у решітці z = 552. Коефіцієнт опору решітки дорівнює $K_р$ = 0,0001156.

Друга ділянка сопла являє собою кільцевий циліндричний канал, коефіцієнт опору визначається за формулою

$$K_2 = \frac{\pi}{8L}\left[R_H^4 - R_B^4 - \frac{\left(R_H^2 - R_B^2\right)^2}{\ln\frac{R_H}{R_B}}\right], \quad , \tag{22}$$

де L – довжина ділянки, 5 см; $R_н$ – зовнішній радіус, 1,004 см; $R_в$ – внутрішній радіус, 0,704 см.

Кінцевий циліндричний канал представлено на рис. 3.

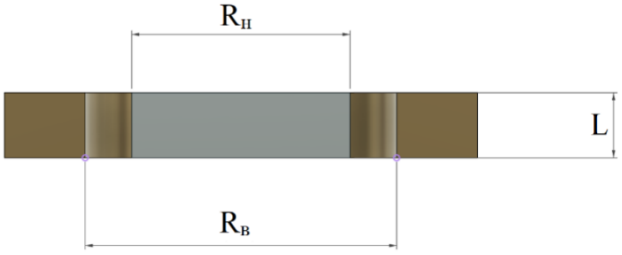


Рис. 3. Кільцевий циліндричний канал

K_2 = 0,0024782.

Третя ділянка сопла є конічним кільцевим каналом, коефіцієнт опору визначається за формулою

$$K_3 = \frac{\pi\left(R_1\delta_1 - R_2\delta_2\right)}{6Lm}, \tag{23}$$

де R_1 – середній радіус конуса на вході, см; R_2 – середній радіус конуса на виході, см; δ_1 – зазор конічного кільцевого каналу на вході, см; δ_2 – зазор конічного кільцевого каналу на виході, см; L – довжина ділянки, см; m – коефіцієнт, що визначається за формулою

$$m = \frac{2{,}3\left(R_1 - R_2\right)^2}{\left(R_1\delta_2 - R_2\delta_1\right)} \lg\frac{R_1\delta_2}{R_2\delta_1} - \frac{\left(R_1 - R_2\right)\left(\delta_1 - \delta_2\right)}{\left(R_1\delta_2 - R_2\delta_1\right)\delta_1\delta_2} - \frac{\delta_1^2 - \delta_2^2}{2\delta_1^2\delta_2^2}. \tag{24}$$

Конічний кільцевий канал представлено на рис. 4.

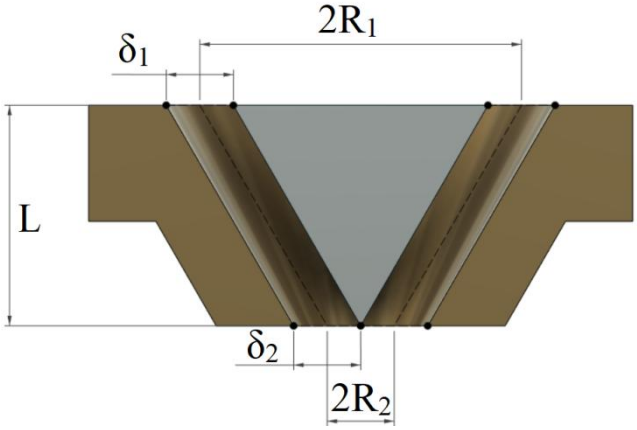


Рис. 4. Конічний кільцевий канал

У запропонованій конструкції коефіцієнт m = 19,3067, а коефіцієнт опору третьої ділянки дорівнює K_3 = 0,004697

Четверта ділянка являє собою циліндричний круглий канал, коефіцієнт опору визначається за формулою

$$K_4 = \frac{\pi d^4}{128L}, \tag{25}$$

де d – діаметр отвору циліндра, см; L – довжина ділянки, см.

Циліндричний круглий канал представлено на рис. 5.

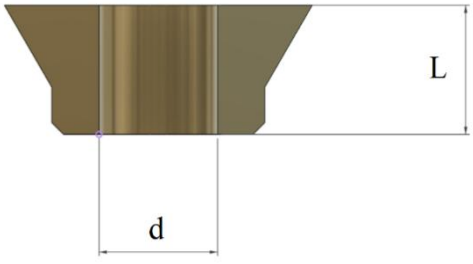


Рис. 5. Циліндричний круглий канал

Відповідно до першого варіанта аналізованої конструкції (сопло 5 мм) K_4 = 0,003068, з другим (сопло 1 мм) $K_4 = 4{,}9 \cdot 10^{-6}$.

Відповідно до конструкції сопла, загальний коефіцієнт опору K розраховується за формулою

$$K = \frac{1}{\frac{1}{k_ф} + \frac{1}{k_p} + \frac{1}{k_2} + \frac{1}{k_3} + \frac{1}{k_4}}, \quad (26)$$

$K = 37{,}513 \cdot 10^{-6}$ для сопла діаметром 5 мм та $K = 4{,}34 \cdot 10^{-6}$ для сопла діаметром 1 мм.

Підставляючи отримані значення в формулу (10) і вибравши максимальну частоту обертання шнека n = 480 хв$^{-1}$, визначимо максимальну об'ємну продуктивність екструдера. Вибір частоти обертання шнека обумовлений тим, що в якості приводу буде використаний кроковий двигун. Відповідно до вироблених розрахунків об'ємна продуктивність Q=181,4418 см^3/хв для сопла діаметром 5 мм; і Q=87,9923 см^3/хв – для сопла діаметром 1 мм. Отриманий результат використовуємо для визначення максимальної лінійної продуктивності екструдера (1).

Для сопла діаметром 5 мм максимальна лінійна продуктивність екструдера становитиме L=924,075 см/хв=154 мм/с.

Для сопла діаметром 1 мм максимальна лінійна продуктивність екструдера становитиме L=11203,528 см/хв=1867,2 мм/с.

Для обох варіантів діаметра сопла набуте значення значно перевищує максимальну швидкість переміщення екструдера в робочому режимі, яка повинна становити 50 мм/с, що дозволить зменшити частоту обертання крокового двигуна, який є приводом екструдера, та використовувати додатково редуктор (наприклад, планетарний) для збільшення крутного моменту.

Висновки

Проведено розробку конструкції шнекового екструдеру для використання в FFF 3D принтерах. Розраховано основні параметри шнеку та циліндру. Розроблено конструкції сопел з отворами 1 та 5 мм. Проведено розрахунок лінійної продуктивності розробленого шнекового екструдеру, результат підтвердив можливість 3D друку із запланованою швидкістю 50 мм/с.

Запропонована конструкція має дві основні переваги у порівнянні із стандартними рішеннями. Шнековий екструдер дозволяє знизити собівартість деталей, що виготовляються за технологією FFF за рахунок використання гранульованих термопластів або подрібненої вторсировини, як наслідок зниження вартості матеріалу. Також з'являється можливість друку соплами великого діаметру. Стандартні сопла зазвичай не перевищують діаметр 1,2 мм, це обмеження викликано, насамперед, діаметрами стандартного філаменту, які становлять 1,75 або 2,85 мм. Запропонований шнековий екструдер дозволяє друкувати значно більшими діаметрами сопла, що у свою чергу прискорює виготовлення деталей великих розмірів.

Список літератури:

1. Басов Н.И., Ким В.С., Скуратов В.К. Оборудование для производства объемных изделий из термопластов. М. : Машиностроение, 1972. 217 с.
2. Радченко Л.Б. Переробка термопластів методом екструзії. Київ,1999. 214 с.
3. Ogorkiewicz R. M. (1977). The Engineering Properties of Plastics, Oxford University Press.
4. Kalpakjian S. and Schmid S.R. (2008). Manufacturing Processes for Engineering Materials, 5th ed., Pearson Education.
5. Tim A. Oswald, Juan Pablo Hernandez-Ortiz (2009), Polymer processing [www.books.google.uk (online) Available, http://books.google.co.uk/books].
6. Rauwendaal C. Polymer extrusion. 5th ed. Munich: Carl Hanser Verlag, 2014. 950 p. doi: 10.3139/978156990539

7. Donovan R. C. A theoretical melting model for plasticating extruders // Polymer Engineering and Science. 1971. Vol. 11, Issue 3. P. 247–257. doi: 10.1002/pen.760110313
8. Analysis of a Single Screw Extruder with a Grooved Plasticating Barrel – Part I: The Melting Model / Alfaro J. A. A., Grün-schloß E., Epple S., Bonten C. // International Polymer Processing. 2015. Vol. 30, Issue 2. P. 284–296. doi: 10.3139/217.3021
9. Сокольський О.Л., Івіцький І.І., Олексишен В.О. Моделювання течії розплавів полімерів за наявності низьков'язкого пристінного шару // Вісник НТУУ "КПІ імені Ігоря Сікорського". Сер.: Хімічна інженерія, екологія та ресурсозбереження. 2019. N 1. С. 35-40. DOI: 10.20535/2617-9741.1.2019.171033
10. Wilczyński K. J., Lewandowski A., Wilczyński K. Experimental study of melting of polymer blends in a starve fed single screw extruder // Polymer Engineering & Science. 2016. Vol. 56, Issue 12. P. 1349–1356. doi: 10.1002/pen.24368.

Надійшла до редколегії 07.05.2022

Відомості про авторів:

Разумов-Фризюк Євгеній Анатолійович – канд. техн. наук, доцент, Харківський національний університет радіоелектроніки, доцент кафедри комп'ютерно-інтегрованих технологій, автоматизації та мехатроніки, Україна; e-mail: ievgenii.razumov-fryziuk@nure.ua; ORCID: https://orcid.org/0000-0001-7426-3805

Гурін Дмитро Валерійович – старший викладач кафедри комп'ютерно-інтегрованих технологій, автоматизації та мехатроніки, Харківський національний університет радіоелектроніки Україна; e-mail: dmytro.gurin@nure.ua; ORCID: https://orcid.org/0000-0002-2272-5227

Нікітін Дмитро Олександрович – аспірант кафедри комп'ютерно-інтегрованих технологій, автоматизації та мехатроніки; Харківський національний університет радіоелектроніки Україна; E-mail: dmytro.nikitin@nure.ua; ORCID: http://orcid.org/0000-0002-5591-4438

Стрілець Роман Євгенійович – аспірант кафедри комп'ютерно-інтегрованих технологій, автоматизації та мехатроніки; Харківський національний університет радіоелектроніки Україна; e-mail:roman.strilets@nure.ua; ORCID: https://orcid.org/0000-0001-5123-8703

Близнюк Данило Сергійович – аспірант, старший лаборант кафедри комп'ютерно-інтегрованих технологій, автоматизації та мехатроніки; Харківський національний університет радіоелектроніки Україна; e-mail: danylo.blyzniuk@nure.ua; ORCID: https://orcid.org/0000-0002-3041-1885

УДК 621.317 **DOI:10.30837/rt.2022.2.209.22**

Ю.Є. ХОРОШАЙЛО, канд. техн. наук, Н.Я. ЗАЙЧЕНКО,
О.Б. ЗАЙЧЕНКО, канд. техн. наук

УДОСКОНАЛЕННЯ СПЕКТРОСКОПІЧНОГО МЕТОДУ ВИЗНАЧЕННЯ КОЕФІЦІЄНТА ЗАЛОМЛЕННЯ МАТЕРІАЛУ ЗРАЗКА ФІЛАМЕНТУ ДЛЯ 3D ДРУКУ В ТЕРАГЕРЦОВОМУ ДІАПАЗОНІ

Вступ

Основною проблемою терагерцової спектроскопії та даного дослідження зокрема є протиріччя між швидким розвитком засобів терагерцової спектроскопії та відставанням моделей, що використовуються у терагерцевій спектроскопії, тоді як сусідня мікрохвильова область має набір готових моделей. У статті розглянуто актуальну проблему неруйнівної дефектоскопії філаменту для 3D друку. Предметом дослідження є процес визначення коефіцієнта заломлення матеріалу філаменту для 3D друку з урахуванням перевідбиттів від протилежних стінок, що досліджується методом терагерцової спектроскопії у часовій області. Перевідбиття від протилежних стінок називаються ефектом Фабрі – Перо, при цьому інтерференційні члени, що виникли через перевідбиття від стінок, традиційно враховуються додаванням і надаються у вигляді ряду. Недоліком моделі у вигляді простого додавання є відкидання членів ряду вище за четвертий, що призводить до неточності моделі. Моделі, побудовані на описі стоячої хвилі в мікрохвильовому тракті з уточненнями, перенесені на нову область терагерцовой спектроскопії в часовій області. Наукова цінність полягає у підвищенні точності за рахунок обліку інтерференційних членів. Аналогія між ефектом Фабрі – Перо, що використовується в терагерцевій спектроскопії, з перевідбиттями в мікрохвильовому багатозондовому мультиметрі дозволила запропонувати такі рекомендації. По-перше, оскільки фазова відстань між датчиками в мікрохвильовому мультиметрі подібна до товщини досліджуваного зразка в терагерцовой спектроскопії, отже, можна підібрати таку товщину зразка, щоб інтерференційні члени компенсувалися; по-друге, можна просте підсумовування сигналів на виході зі зразка замінити алгоритмічною обробкою, умовою для цього є існування крім основного сигналу в часовій області реєстрованих сигналів відлуння значно меншої амплітуди, отже, можна побудувати систему рівнянь і шляхом її вирішення визначити шукані параметри коефіцієнта заломлення матеріалу зразка філаменту.

Аналіз останніх досліджень та публікацій

В статті [1] представлено метод максимальної правдоподібності для оцінки параметрів у терагерцовій часовій спектроскопії, отримано функцію імовірності для параметризованої функції частотної характеристики. Метод забезпечує оцінки параметрів, які перевищують інші широко використовувані методи, і забезпечує надійне вимірювання. Це відбувається завдяки статистичній обробці і використанню універсального методу найменших квадратів. Також розроблено просту модель шуму, яка параметризована трьома домінуючими джерелами. Продемонстровано метод із застосуванням до характеризування параметрів речовини.

Пористість та неоднорідність 3D-друкованих полімерних зразків досліджували за допомогою терагерцової спектроскопії у часовій області та аналізували вплив налаштувань 3D-принтера. Набір зразків PETG був надрукований на 3D-принтері шляхом систематичного зміни параметрів принтера, включаючи товщину шару, діаметр сопла, товщину нитки (рядка філамента), екструзію та малюнок друку. Їх ефективні показники заломлення та коефіцієнти втрат були виміряні та порівняні з показниками твердого PETG. Пористість розраховували за показником заломлення. Дифракційна особливість спостерігалася в спектрі втрат усіх 3D-друкованих зразків і використовувалася як ознака неоднорідності. Було знайдено оптимальне співвідношення налаштувань принтера, де пористість і неоднорідність були зведені до мінімуму [2].

Терагерцова спектроскопія у часовій області (THz-TDS) є перевіреним методом, за допомогою якого можна отримати комплексні показники заломлення матеріалів оскільки інформацію про фазу та амплітуду можна отримати з вимірювань. Однак попередня обробка даних вручну все ще необхідна, а параметри матеріалу вимагають ітераційної підгонки, що призводить до складності, втрати точності та невідповідності між вимірюваннями. В якості альтернативи можна використовувати наближення, щоб уможливити аналітичне вилучення, але зі значною жертвою точності. Автори статті досліджують використання методів машинного навчання для інтерпретації спектроскопічних даних THz-TDS шляхом навчання з великими наборами даних змодельованих взаємодій світло-речова, що призводить до обчислювальної ефективної штучної нейронної мережі для вилучення параметрів матеріалу. Навчена модель покращує точність аналітичних методів, які потребують наближення, при цьому її легше реалізувати та швидше запускати, ніж ітераційні методи пошуку кореня. Ми припускаємо, що нейронні мережі можуть усунути багато поширених перешкод, пов'язаних з аналізом даних THz-TDS, таких як розгортання фази, вікно часової області, повільний час обчислень і точність вилучення в діапазоні низьких частот [3].

Метод терагерцової спектроскопії у часовій області

Оскільки терагерцова спектроскопія у часовій області використовується в основному для характеристики матеріалів, велика кількість літератури присвячено питанням виділення параметрів, тобто розрахунку оптичних параметрів досліджуваних матеріалів за їх терагерцовими спектрами пропускання. Як і інші спектрометри, вимірювання терагерцової спектроскопії у часовій області вимагають порівняння між даними, записаними зі зразком, розміщеним на шляху променя, та еталонними даними, записаними з вилученим зразком. Перші вимірювання діелектричних проникностей матеріалів були продемонстровані незабаром після винаходу терагерцової спектроскопії у часовій області.

Принцип роботи терагерцового спектрометра показаний на рис.1

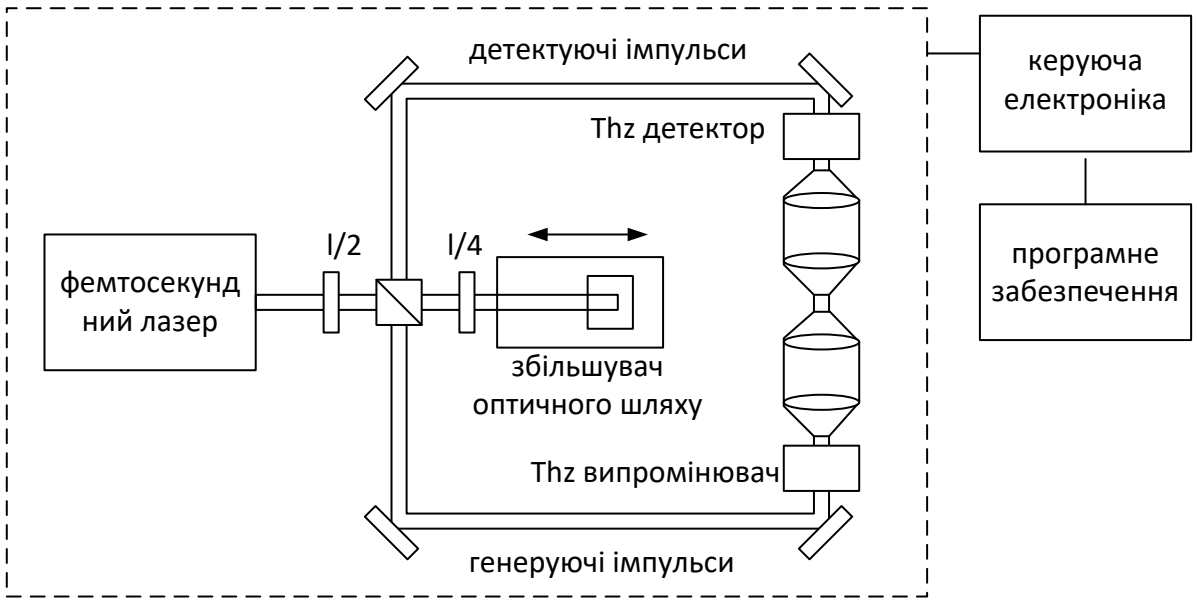


Рис. 1. Терагерцова спектрометрична установка

У цьому спектрометрі лазерний промінь поділяється на два промені: генеруючий і детектуючий. Ці промені проходять різні оптичні шляхи до випромінюючої та приймальної антен відповідно. Один оптичний тракт має змінну довжину для контролю затримки імпульсу, що надходить на відповідну антену (рис.1). Після того, як імпульс генерується в випромінюючій антені, «виявлений» імпульс дозволяє відповідній антені виміряти напруженість електричного поля. Змінюючи оптичну затримку, вимірювання проводяться в потрібний час.

Пізніше з цих моментів часу за допомогою перетворення Фур'є отримують частоти. Коли досліджуваний зразок поміщають в прилад, прийнятий сигнал змінюється. Для отримання інформації про властивості матеріалу порівнюють два отримані спектри.

Порівняльний аналіз графічних, аналітичних та метрологічних моделей для терагерцових та мікрохвильових вимірювальних приладів для визначення параметрів матеріалів

Звичайно терагерцові спектрометри порівнюють з векторними аналізаторами кіл. Відомо, що скалярні дванадцятиполюсні аналізатори кіл мають такий же функціонал, як векторні аналізатори кіл, але відрізняються принципом дії, більш прості, надійні та значно дешевші, що є їх перевагою. Багатозондовий мікрохвильовий мультиметр представляє з себе різновид скалярного аналізатора кіл.

Багатозондові мікрохвильові мультиметри крім потужності і коефіцієнта відбиття навантаження також використовуються для вимірювання діелектричної проникності і коефіцієнта заломлення діелектричних матеріалів. Спроби екстраполювати мікрохвильові мультиметри на терагерцовий діапазон не можна вважати вдалими, адже зменшення розмірів хвилеводних компонентів приладів є межею для просування мультиметрів у галузь терагерцових коливань. Але подібність тим не менше є. Мета цього підрозділу довести існування подібності між методами та моделям для обох частотних діапазонів терагерцового та мікрохвильового.

Основним рівнянням терагерцової спектроскопії є залежність показника заломлення від різних параметрів, у тому числі від товщини зразка:

$$n(\omega) = n_0 - \frac{c}{\omega l}\arg\left\{H\left(\omega\right)\right\}, \tag{1}$$

де c – швидкість світла, l – товщина зразка, n_0 – коефіцієнт заломлення у повітрі, ω – кутова швидкість, H – співвідношення подане нижче [1]

$$H\left(\omega\right) = \frac{4n(\omega)n_0}{\left[n(\omega)+n_0\right]^2}\exp\left\{-k(\omega)\frac{\omega l}{c}\right\}\exp\left\{-j\left[n(\omega)-n_0\right]\frac{\omega l}{c}\right\}, \tag{2}$$

$k(\omega)$ – коефіцієнт згасання

$$\arg\left\{H\left(\omega\right)\right\} = -\left[n(\omega)-n_0\right]\frac{\omega l}{c}. \tag{3}$$

Показники заломлення навколишнього вільного простору та діелектрика позначаються $\hat{n}_0 = 1$ і $\hat{n}_s$ відповідно. Крім того, $E_0\left(\omega\right)$ – падаюча хвиля; θ_i – кут падіння; θ_t – кут заломлення. Відстань поширення l_θ визначається з товщини зразка l і дорівнює $1/\cos(\theta_t)$. Стрілки показують проміжні шляхи розповсюдження, згруповані в передачу, 1, 2, 3,..., і відбиття, $1', 2', 3'$... (рис. 2).

На рис. 2 показано, що промінь $E_0\left(\omega\right)$, який входить справа зверху під деяким кутом до поверхні зразка, частково відбивається (1 на рисунку), а частково проходить крізь зразок до протилежної грані зразка, де він розділяється на два промені; той який відбився, йде в напрямку правої грані, другий промінь, який вийшов через напівпрозору стінку зразку наліво ($1'$), далі відбувається аналогічним чином розділення проміня на правій грані з отриманням проміня 2 і проміня, який прямує до лівої грані, і т. ін.

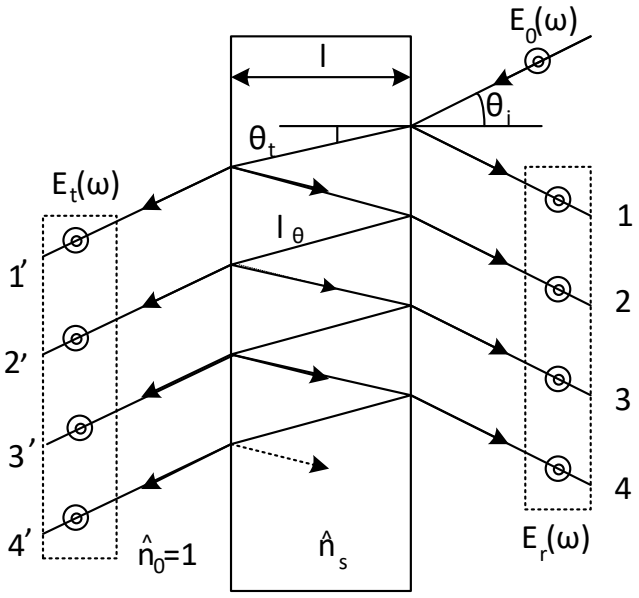


Рис. 2. Модель поширення хвилі в однорідній діелектричній пластинці

Під час просування шляхом відбиття накопичуються коефіцієнти відбиття коефіцієнти передавання. Визначення коефіцієнта передавання τ та відбиття ρ для хвилі яка падає з вільного простору

$$\tau = \frac{2}{1+\hat{n}_s}, \quad \rho = \frac{1-\hat{n}_s}{1+\hat{n}_s}$$

Визначення коефіцієнта передавання τ' та відбиття ρ' для хвилі яка падає та відбивається від другого боку зразка

$$\tau = \frac{2\hat{n}_s}{\hat{n}_s+1}, \quad \rho = \frac{\hat{n}_s-1}{\hat{n}_s+1}$$

Таким чином,

шлях відбиття	множник
1	ρ
2	$\tau\tau'\rho' \exp\left[-2j\hat{n}_s \frac{\omega l}{c}\right]$
3	$\tau\tau'\rho'^3 \exp\left[-4j\hat{n}_s \frac{\omega l}{c}\right]$
4	$\tau\tau'\rho'^5 \exp\left[-6j\hat{n}_s \frac{\omega l}{c}\right]$
5	...

(4)

Аналогічні формули існують для шляху передавання [4].

У випадку нормального падіння, де $\theta_i = 0$, всі шляхи передачі (відбиття) перекриваються і $l_\theta = l$. Таким чином, загальна передана хвиля є результатом складання хвиль всіх проміжних шляхів передачі.

$$E_t(\omega) = \tau\tau' \cdot \exp\left[- j\hat{n}_s(\omega)\frac{\omega c}{l} \right] \cdot$$
$$\cdot \left\{ 1 + \rho'^2 \cdot \exp\left[-2 j\hat{n}_s(\omega)\frac{\omega c}{l} \right] + \rho'^4 \cdot \exp\left[-4 j\hat{n}_s(\omega)\frac{\omega c}{l} \right] + ... \right\} \cdot E_0(\omega) =$$
$$= \tau\tau' \cdot \exp\left[-2 j\hat{n}_s(\omega)\frac{\omega c}{l} \right] \cdot FP(\omega) \cdot E_0(\omega) \qquad (5)$$

де $FP(\omega)$ представляє ефект Фабрі – Перо як наслідок відбиття всередині зразка і подається як

$$FP(\omega) = \left\{ 1 + \rho'^2 \cdot \exp\left[-2 j\hat{n}_s(\omega) \right] + \rho'^4 \cdot \exp\left[-4 j\hat{n}_s(\omega) \right] + ... \right\} =$$
$$= \sum_{m=0}^{\infty} \left\{ \rho'^2 \cdot \exp\left[-2 j\hat{n}_s(\omega) \right] \right\}^m =$$
$$= \left\{ 1 - \rho'^2 \cdot \exp\left[-2 j\hat{n}_s(\omega) \right] \right\}^{-1} \qquad (6)$$

Для товстих зразків часові криві демонструють добре розділені відлуння (рис. 3). Основна ідея методу полягає у часовому вікні принаймні двох ехо-сигналів терагерцового імпульсу, викликаних багаторазовими відбиттями в зразку, і для здійснення процесу визначення для кожного з цих відлунь, тоді у нас буде більше рівнянь, ніж невідомих. Цей метод передбачає, що поглинання зразка досить низьке, щоб дозволити існування кількох спостережуваних відлунь [5, 6]. Крім того в цих публікаціях представлено метод, який покращує визначення оптичних констант шляхом одночасного з визначенням коефіцієнта заломлення визначення товщини зразка також.

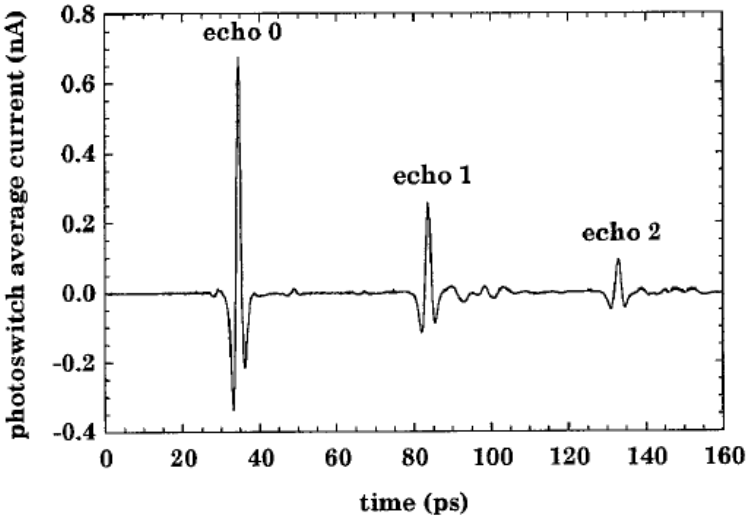


Рис. 3. Терагерцові імпульси, що передаються через пластину з LiNbO3 товщиною 1,1 мм з поляризацією, паралельною повільній оптичній осі [6]

На рис. 3 показані відлуння, на рис. 4 – відлуння, які відповідають інтерференційним членам, тобто з цього можна зробити важливий висновок, що відлуння об'єктивно існують, їх можна виміряти і в подальшому використовувати в визначенні параметрів.

Для оптично тонких зразків накладання між послідовними відлуннями не дозволяє розбити терагерцовий сигнал, що передається через зразок, на його послідовні ехо-сигнали. Однак ефективну товщину зразка можна визначити з частотної кривої. Дійсно, коли визначається комплексний показник заломлення зразка за умов помилкової товщини, і показники

заломлення, і криві поглинання представляють штучні коливання в залежності від частоти. Такі коливання можна побачити на рис. 4.

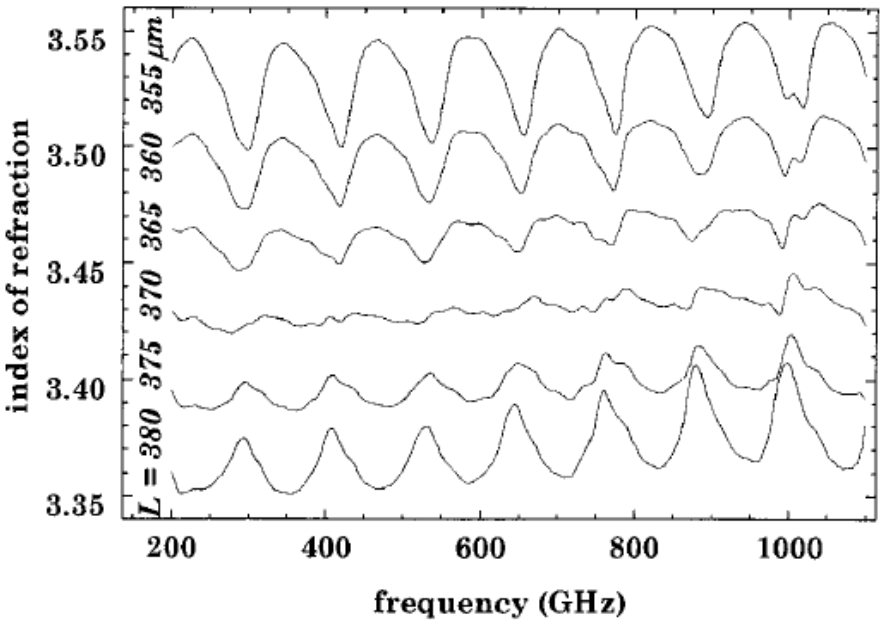


Рис. 4. Показник заломлення кремнію для різних розрахункових товщин зразка [6]

Оцінка похибки вимірювання коефіцієнта заломлення описується такими виразами:

$$\Delta n \cong (1-n_0)\frac{\Delta L}{L} - \frac{c}{\omega L}\theta,$$

$$\theta = \arg\left(\frac{1-N}{1-D}\right),$$

$$N = \left(\frac{n_0 - 1}{n_0 + 1 + 2\Delta L / L_0}\right)^2$$

$$\times \exp\left(-2in_0\frac{\omega L_0}{c}\right)\exp\left(-2i\frac{\omega \Delta L}{c}\right),$$

$$D = \left(\frac{n_0 - 1}{n_0 + 1}\right)^2 \exp\left(-2in_0\frac{\omega L_0}{c}\right), \qquad (7)$$

Перший доданок правої частини першого рядка відповідає за загальний зсув показника заломлення, вилученого зі зразка з помилковою товщиною. Штучні коливання кривих оптичних констант, побудовані в залежності від частоти рис. 4, обумовлені другим доданком першого рядка виразу (7). Проаналізуємо вплив другого доданка. Цей аналіз значно спрощується використанням представлення похибки на комплексній площині (рис. 5). Вектори OA і OB представляють 1-N і 1-D відповідно. Величина θ дорівнює arg(OA) –arg(OB) і, таким чином, представляє кут між векторами OA і OB. Якщо припустити, що $\Delta L << L$, тоді точки A і B обертаються навколо точки I. Оскільки $N \cong D$, θ коливається між екстремальними значеннями $\theta_{\min}$ і $\theta_{\max}$, як показано на рис. 5. Використовуючи елементарну тригонометрію в прямокутних трикутниках, можна показати, що

$$\min(\Delta n) = (1-n_0)\frac{\Delta L}{L} - \frac{c}{\omega L}\theta_{\max} \cong (1-n_0)\frac{\Delta L}{L}$$
$$-\frac{2c}{\omega L}\arctan\left[\frac{R\left|\sin\left(\omega\Delta L / c\right)\right|}{1-R}\right],$$
$$R = \frac{|N|+|D|}{2} = \left(\frac{n_0 - 1}{n_0 + 1 + \Delta L / L_0}\right)^2$$
$$\cong \left(\frac{n-1}{n+1+\Delta L / L}\right)^2, \qquad (8)$$

Кут, який є мірою невизначеності, утворений векторами OA та OB. Вектори не мають фіксованого положення, а обертаються у зв'язку з невизначеністю кута. Кут буде мінімальним у місці перетину відрізка OI та кола зліва. Перетин продовження відрізка OI справа так само може використовуватися для розрахунку невизначеності, але розрахунок аналогічний розрахунку для перетину зліва і розглядатися окремо не буде. Позначимо усереднений радіус кола – R, тоді прилягаючий до кута θ катет – 1-R, протилежний катет визначається шляхом опускання перпендикуляру на OI. В трикутнику, що знаходиться в межах кола, R виступає гіпотенузою. Кут, який знаходиться в центрі кола визначається аргументом експоненціальної функції в виразах (7), отже значення кута $\omega\Delta L / c$. Тоді, користуючись визначенням синуса, знаходимо протилежний спільний катет двох трикутників, того, що знаходиться в межах кола і того, що містить кут θ. Переходячи до трикутника з кутом θ і користуючись визначенням тангенса, отримуємо вирази (8).

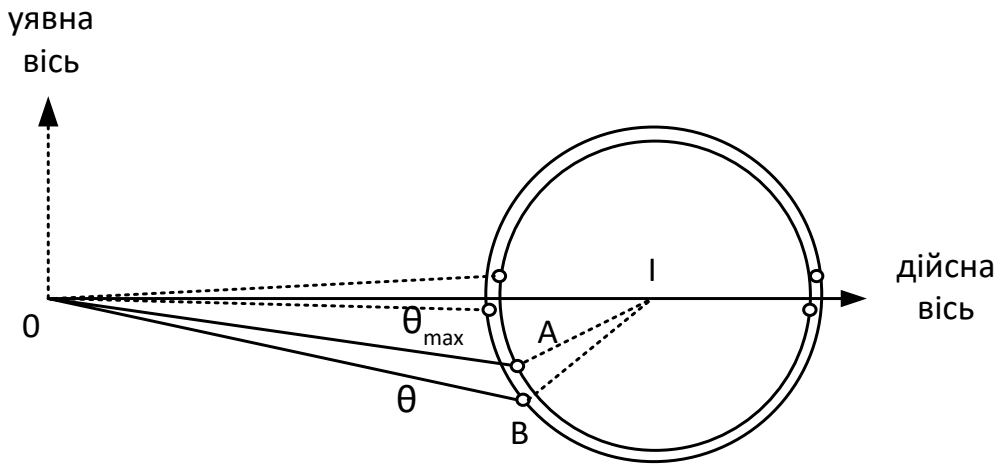

<antуявна вісь="" />
<antдійсна вісь="" />

Рис. 5. Представлення осцилюючого члена рівняння ефекту Фабрі – Перо, що відповідає за штучні коливання комплексного показника заломлення [6]

Нехай наступний рис. 6 буде зв'язуючим ланцюгом між терагерцовими та мікрохвильовими моделями, адже вони схожі тим що уособлюють похибки, представлені на комплексних площинах, використовують тригонометрію, звичайно з деякими розбіжностями.

Точність вимірювання дванадцятиполюсного рефлектометра і також багатозондового хвильового мультиметра найкраще виражається через радіус невизначеності δ (рис. 6). Це радіус кола невизначеності з центром у виміряному комплексному коефіцієнті відбиття на комплексній площині, всередині кола невизначеності з високою ймовірністю (наприклад, 99 %) знаходиться справжній коефіцієнт відбиття. Він може поєднувати як систематичні, так і випадкові помилки [16]. Типове значення похибки становить від 0,01 до 0,03, що для вимірювання низького коефіцієнта відбиття відповідає ефективній спрямованості від 40 до 30 дБ.

<antISSN="" 0485-8972="" radiotekhnika="" no.="" 209="" (2022)="" 221="" eissn="" 2786-5525="" />

Проте застосовувані в метрології рефлектометри досягають кращих значень δ від 10^{-3} до 10^{-4}.

На рис. 6 показана похибка визначення коефіцієнта відбиття навантаження, в даному випадку прямокутний трикутник в моделі використовується таким чином: кут відповідний за невизначеність Δф відбудовується від центра великого кола, вектор Г в напрямку радіуса великого кола є прилягаючим катетом прямокутного трикутника, протилежний катет є похибка, протилежний катет проходить через центр меншого кола, на відмінність від рис. 4, де прямокутний трикутник знаходиться в місті лівого перетину кола і відрізка, який з'єднує точки О та І, Г є модулем коефіцієнта відбиття навантаження багатозондового мікрохвильового мультиметра.

.

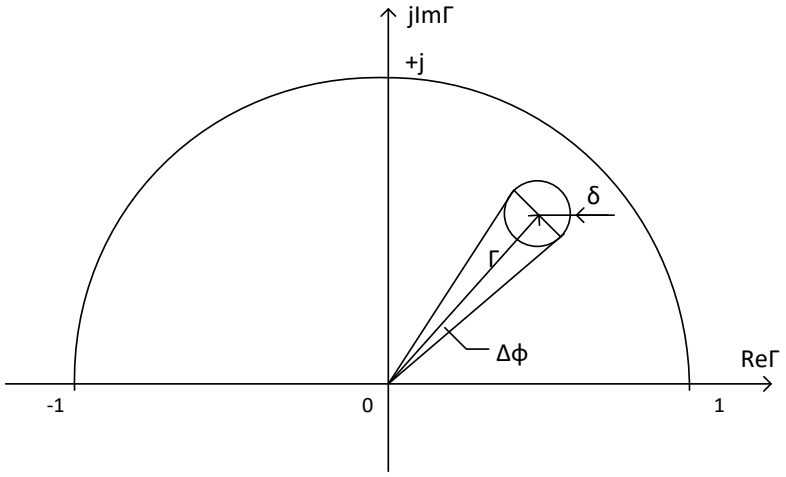


Рис. 6. Коло невизначеності вимірювання коефіцієнта відбиття навантаження [16]

Проведене порівняння метрологічних моделей доводить наявність спільних властивостей у мікрохвильових та терагерцових вимірювальних приладів.

Звернемося до графічних моделей рис. 2 та 7. Орієнтований граф багатозондового мікрохвильового мультиметра (рис. 7) складається з вузлів та гілок. Сигнал, що передається гілкою у вузол, до якого ця гілка підходить, дорівнює добутку вхідного сигналу, тобто сигналу відповідного вузла, з якого вона виходить, на її передачу. Під шляхом в теорії графів розуміють сукупність гілок, які проходять в прямому напрямку, та які не торкаються жодного з вузлів більш одного разу [9, 10].

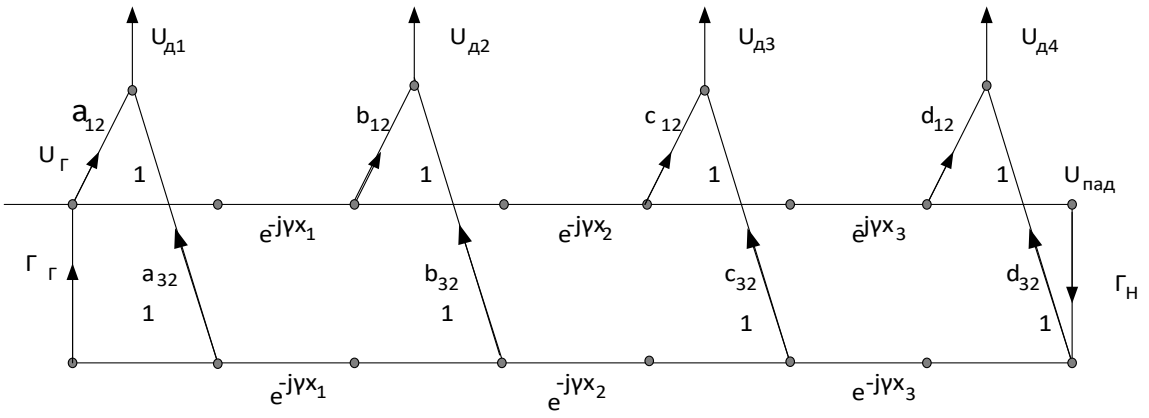


Рис. 7. Модель у вигляді орієнтованого графа в багатозондовому мікрохвильовому мультиметрі

Ефект Фабрі – Перо (рис. 2) одночасно схожий на парціальні хвилі у НВЧ передавальних трактах та на перевідбиття в багатозондовому мікрохвильовому мультиметрі. Парціальні хвилі, на перший погляд, краща фізична аналогія, але вони є моделлю дисперсійних властивостей хвилевода, тому ми змушені цю модель поки відкинути. Щодо моделі у вигляді орієнтованих графів спочатку відзначимо обмеження застосування та підкреслимо відмінності, які полягають в тому, що орієнтовані графи походять із каскадного з'єднання графічних еквівалентів матриць розсіювання [9], які описують датчики, а ефект Фабрі – Перо [4 – 6] фізично спостерігається у досліджуваному зразку. Тим не менш, аналогією точок 1, 2, 3 (рис. 2) є сигнали на датчиках (рис. 7). Привертає увагу подібність у тому, що сигнали є результатом накопичення коефіцієнтів передавання певних гілок. В орієнтовному графі більш складне математичне підґрунтя, тому що там за допомогою формули Мезона, яку ще називають формулою контурів, які не торкаються [9], розраховують сигнали на датчиках, і яка зайва для тегагерцової графічної моделі з рис. 2.

Нарешті, порівняємо аналітичні моделі. Чотирьохзондова секція в НВЧ блоці багатозондового мікрохвильового мультиметра описується рівняннями. З орієнтованого графу слідує система рівнянь [8]:

$$\begin{aligned}
&|U_{\partial 1}| = a_{12}^2 |U_{nа\partial}|^2 \left|1 + \Gamma_н e^{-2j\gamma(x_1+x_2+x_3)}\right|^2 \\
&|U_{\partial 2}| = a_{12}^2 |U_{nа\partial}|^2 \left|1 + \Gamma_н e^{-2j\gamma(x_2+x_3)}\right|^2 \\
&|U_{\partial 3}| = a_{12}^2 |U_{nа\partial}|^2 \left|1 + \Gamma_н e^{-2j\gamma x_3}\right|^2 \\
&|U_{\partial 4}| = a_{12}^2 |U_{nа\partial}|^2 |1 + \Gamma_н|^2 \\
&U_{nа\partial} = U_{ген} \Big/ \left(1 - \Gamma_н \Gamma_н e^{-2j\gamma(x_1+x_2+x_3)}\right)
\end{aligned} \tag{9}$$

де $\Gamma_н, \Gamma_г$ – модулі коефіцієнта відбиття навантаження та генератора відповідно, γ – коефіцієнт розповсюдження, $U_{nа\partial}$ – напруга падаючої хвилі, a_{12}^2 – коефіцієнт перетворення датчика, однакові коефіцієнти перетворення датчиків є ідеалізацією з метою спростити модель, $a_{12} = b_{12} = c_{12} = d_{12}$, x_i – відстань між сусідніми датчиками, $U_{\partial i}$ – напруга на *i*-му датчику.

Вирази (9) подібні до виразів (4) – (6), тому що в виразі (9) показники експонент є результатом накопичення коефіцієнтів передач гілок орієнтованого графа на шляху від початкового вузла через проміжні до кінцевого, так само як і вираз (4).

Вираз (9) можна спростити і зробити більш придатним для подальших розрахунків таким чином. Експоненти можна перетворити за допомогою формул Ейлера $\cos(x) = \left(e^{ix} + e^{-ix}\right)/2$ на тригонометричні функції, і тоді за умов спеціально обраного початку обліку фази можна отримати

$$\begin{cases}
\mathrm{P}_1 = \mathrm{P}_{\text{пад}}(1 + \Gamma^2 + 2\Gamma\cos(\phi - \theta)) \\
\mathrm{P}_2 = \mathrm{P}_{\text{пад}}(1 + \Gamma^2 + 2\Gamma\cos(\phi)) \\
\mathrm{P}_3 = \mathrm{P}_{\text{пад}}(1 + \Gamma^2 + 2\Gamma\cos(\phi + \theta)) \\
\mathrm{P}_4 = \mathrm{P}_{\text{пад}}(1 + \Gamma^2 + 2\Gamma\cos(\phi + 2\theta))
\end{cases} \tag{10}$$

де Γ, ϕ – модуль та фаза коефіцієнта відбиття навантаження, θ – фазова відстань між сусідніми датчиками $\theta = \frac{4\pi x}{\lambda_{хв}}$, $\lambda_{хв}$ – довжина хвилі в хвилеводі, $P_{пад} = U_{пад}^2$ – потужність падаючої хвилі, P_i – потужність на *i*-му датчику.

Третій доданок в дужках – інтерференційний член рівняння.

Нехай фазова відстань θ дорівнює $\pi/2$, тоді використовуючи тригонометричні формули приведення отримаємо з виразу (6).

$$\begin{cases} P_1 = P_{пад}(1+\Gamma^2+2\Gamma\sin(\phi)) \\ P_2 = P_{пад}(1+\Gamma^2+2\Gamma\cos\phi) \\ P_3 = P_{пад}(1+\Gamma^2-2\Gamma\sin(\phi)) \\ P_4 = P_{пад}(1+\Gamma^2-2\Gamma\cos(\phi)) \end{cases} \quad (11)$$

Додавання чотирьох рівнянь (9) за умов, що θ дорівнює $\pi/2$ призводить до компенсації інтерференційних членів, а саме однакових тригонометричних функцій з протилежними знаками. Запропоноване удосконалення у терагерцовому діапазоні полягає у підборі фазової відстані проходженя проміня за рахунок варіювання на стадії створення товщини зразка, таким чином, щоб проміні в точках 1, 2, 3, 4… на рис. 2 мали інтерференційні члени пропорційні $\sin\alpha$, $\cos\alpha$, $-\sin\alpha$, $-\cos\alpha$ та при додаванні компенсувалися. Умовою і обмеженням застосування є рівність амплітуд, але співвідношення амплітуд в точках 1, 2, 3, 4… на рис. 2 є предметом подальших досліджень.

Аналіз графічних, аналітичних та метрологічних моделей для терагерцових та мікрохвильових приладів показав їх подібність та довів можливість перенесення доробок з мікрохвильового діапазону в терагерцовий.

Висновки

Удосконалення методу терагерцової спектроскопії за рахунок обліку інтерференційних складових стало можливим завдяки доказу аналогій моделі в терагерцовому та мікрохвильовому (гігагерцовому) діапазоні і можливості опису явища системою лінеарізованих рівнянь, тим самим з'являється можливість використання відомих авторам статті методів рішення систем лінійних рівнянь, яких існує багато [11 – 15], наприклад методи лінійної алгебри, метод найменших квадратів, процедура Робінса – Монро, фільтр Калмана, що частково співпадає з відомими рішеннями [1].

Перспективний напрямок досліджень пов'язаний з оптимізацією товщини зразка, що дозволить удосконалити модель і метод вимірювання в терагерцовій спектроскопії. Запропонований підхід використовує аналогію з мультиметрами в мікрохвильовому діапазоні, а саме фазова відстань між датчиками в мікрохвильовому блоці багатозондового мікрохвильового мультиметра подібна до електричного шляху променя від однієї до іншої грані зразка матеріала у терагерцовому спектрометрі.

Список літератури:

1. Mohtashemi L., Westlun, P., Sahota D. G., Lea G. B., Bushfield I., Mousavi P., Dodge J. S. Maximum-likelihood parameter estimation in terahertz time-domain spectroscopy // Optics Express. 2021. Vol. 29, No. 4. P. 4912-4926.

2. Naftaly M., Savvides G., Alsharee, F., Flanigan P., Lui G., Florescu M. Mullen R. A. Non-Destructive Porosity Measurements of 3D Printed Polymer by Terahertz Time-Domain Spectroscopy// Applied Sciences. 2022. Vol.12, No. 2. P. 927-938.

3. Klokkou N., Gorecki J., Wilkinson J. S. Apostolopoulos V. Artificial neural networks for material parameter extraction in terahertz time-domain spectroscopy // Optics Express. 2022, Vol. 30, No. 9. P. 15583-15595.

4. Withayachumnankul W., Naftaly M. Fundamentals of measurement in terahertz time-domain spectroscopy // Journal of Infrared, Millimeter, and Terahertz Waves. 2014. Vol. 35, No.8. P. 610-637.

5. Dorney T. D., Baraniuk R. G., Mittleman D. M. Material parameter estimation with terahertz time-domain spectroscopy // JOSA A. 2001. Vol. 18, No. 7. P.1562-1571.

6. Duvillaret L., Garet F., Coutaz J. L. Highly precise determination of optical constants and sample thickness in terahertz time-domain spectroscopy // Applied optics. 1999. 199938(2). P.409-415.

7. Oberto L., Bisi M., Kazemipour A., Steiger A., Kleine-Ostmann T., Schrader T. Measurement comparison among time-domain, FTIR and VNA-based spectrometers in the THz frequency range // Metrologia. 2017. Vol.54, No.1. P. 77-84.

8. Билько М. И., Томашевский А. К. Измерение мощности СВЧ. Москва : Радио и связь, 1976. 168 с.

9. Силаев М. А., Брянцев С. Ф. Приложение матриц и графов к анализу СВЧ устройств. Москва : Сов. радио, 1970. 248 с.

10. Somlo P. I., Hunter J. D. Microwave impedance measurement. Peter Peregrinus Ltd. 1985 207 p.

11. Zaichenko O., Miroshnyk M., Galkin, P. Signal Flow Graph for Optimizing of Mutual Sensors Reflection in the Multiprobe Microwave Multimeter // 2019 IEEE 2nd Ukraine Conference on Electrical and Computer Engineering (UKRCON). 2019. P. 200-203.

12. Zaichenko O., Galkin P., Zaichenko N., Miroshnyk M. Six-port Reflectometer with Kalman Filter Processing of Sensor Signals Proceedings / 15th International Conference on Advanced Trends in Radioelectronics // Telecommunications and Computer Engineering, TCSET 2020. 2020. P. 55–58.

13. Zaichenko O., Miroshnyk M., Zaichenko N., Miroshnyk A. A. Multiprobe microwave multimeter signals iterative processing // 30th International Scientific Symposium Metrology and Metrology Assurance, MMA. 2020. 2020. P. 1-4.

14. Zaichenko O., Galkin P., Miroshnyk M., Zaichenko N., Miroshnyk A. Application of Six-Port for Distance Measurement // 2020 IEEE International Conference on Problems of Infocommunications Science and Technology, PICST 2020 Proceedings. 2020. P. 97-100.

15. Zaichenko O. B., Zaichenko, N. Y. Systematization of the Formulas of Resonant Ferrite Isolator Loss // Radio Electronics, Computer Science, Control. 2022. Vol. 1. P.20-29.

16. Bilik V. Six-port measurement technique: principles, impact, applications // Invited paper at the International Conference Radioelectronika. 2002. P. 1-32.

Надійшла до редколегії 20.05.2022

Відомості про авторів:

Хорошайло Юрій Євгенійович – канд. техн. наук, професор, завідуючий кафедрою проектування та експлуатації електронних апаратів, Харківський національний університет радіоелектроніки, Україна, e-mail: yurii.khoroshailo@nure.ua, ORCID: https://orcid.org/0000-0002-4239-4357

Зайченко Наталія Ярославівна – аспірант кафедри медіаінженерії та інформаційних радіоелектронних систем, Харківський національний університет радіоелектроніки, Україна, e-mail: nataliia.zaichenko@nure.ua, ORCID: https://orcid.org/0000-0001-9798-7136

Зайченко Ольга Борисівна – канд. техн. наук, доцент, доцент кафедри проектування та експлуатації електронних апаратів Харківський національний університет радіоелектроніки, Україна, e-mail: olha.zaichenko@nure.ua, ORCID: https://orcid.org/0000-0003-4936-2785

УДК 655.3.022 **DOI:10.30837/rt.2022.2.209.23**

О.В. ВОВК, канд. техн. наук, І.Б. ЧЕБОТАРЬОВА, Д.В. ПОЛЕНОК

ДОСЛІДЖЕННЯ ОСОБЛИВОСТЕЙ КОЛЬОРОВІДТВОРЕННЯ НА ПІДПРИЄМСТВІ ТОВ «НАРГУС»

Вступ

Технологія флексографічного друку набирає все більше замовників у сфері друку гнучкої рулонної упаковки. Завдяки точному відтворенні кольору, стійкому зносу флексографічних форм, гнучкому налаштуванні обладнання надає замовникам повну свободу керування процесу. Але з розвитком флексографії створюються нові стандарти, які більш жорсткіші від тих, що були. Насамперед це стосується відтворення кольору під час друку будь-якого накладу. Замовник бажає незмінність та стійкість кольору від накладу до накладу. Щоб заохочувати замовників і відповідати технологічним стандартам, вдосконалюється як саме друкарське обладнання, так і спосіб контролю кольору. За стандартом ISO 12647-2 від 2013 р., відхилення кольору за dE_{2000} повинно складати не більше 5. Виходячи з цього, підготовка фарби та її корекція – найважливіші процеси на друкарському підприємстві, оскільки саме на ці процеси припадає найбільше витраченого часу і матеріалів. Несерйозне ставлення до даної проблеми призводить до великої кількості браку, що, в свою чергу, веде до збитків і поганого іміджу підприємства перед замовниками.

Мета роботи – дослідження особливостей кольоровідтворення на ТОВ «Наргус» та виявлення факторів, які впливають на якість флексодруку. Дослідження основних етапів виробництва гнучкого пакування на різних матеріалах в умовах діючого підприємства дозволить виявити основні проблеми щодо кольоровідтворення. Використання апаратних та програмних засобів забезпечить повне дослідження відтворення кольору на друкарському виробництві. Детальне дослідження додрукарської підготовки продукції та технологій виготовлення флексоформ дозволить виявити основні фактори, які впливають на кінцеву якість продукції.

Для досягнення поставленої мети необхідно вирішити наступні задачі:

- ознайомлення з найважливішими технологічними процесами відтворення кольору на флексографічному підприємстві;
- дослідження властивостей фарби на надрукованому матеріалі;
- аналіз браку на підприємстві «Наргус» та пропозиції щодо його усунення;
- ознайомлення з нормативно-технічною документацією на флексографічному виробництві, етапами і стадіями розробки друкованої продукції;
- дослідження особливостей додрукарської підготовки і виготовлення флексоформ, та визначення факторів, які впливають на якість друку;
- розробка методики вибору флексографських форм для друкування на невбираючих матеріалах;
- дослідження особливостей відтворення кольору в умовах діючого поліграфічного підприємства ТОВ «Наргус»;
- розробка методики підвищення швидкості підбору фарби та рекомендації щодо її застосування.

1. Аналіз процесу контролю якості на підприємстві

Під час аналізу світового ринку поліграфічної продукції друкування пакувань залишається єдиною галуззю, де спостерігається деяке зростання (на 3,3 % на рік), в цей сегмент входять коробки, етикетки, гнучкі пакування [1, 2]. Пандемія вплинула на обсяги виробництва упаковки в набагато меншому ступені, ніж на випуск книжково-журнальної продукції, рекламної продукції та оперативної поліграфії.

Згідно з даними дослідження «Майбутнє друку упаковки до 2025 р.», проведеного агентством Smithers, ринок друку упаковок та етикеток на кінець 2020 р. досяг 431,6 млрд дол. Не дивлячись на карантин, світовий ринок друкування упаковок буде в середньому зростати на 2,6 % і до 2025 р досягне обсягу 491,1 млрд [3].

Харківська фабрика флексографського друку «Наргус» – це сучасне високотехнологічне підприємство з виробництва гнучкої упаковки для харчової, фармацевтичної, хімічної та інших галузей промисловості, один з провідних на українському ринку виробників упаковки [4]. Підприємство намагається максимально контролювати якість продукції. Згідно з цим, для підприємства були поставлені такі цілі:

– постійно удосконалювати технологію виробництва, виконувати вимоги замовників та перевершувати їхні сподівання;

– проводити оптимізацію виробничих процесів і зниження витрат;

– вдосконалювати компетентність персоналу, проводити аудити з підвищення кваліфікації.

Контроль готової продукції здійснюється відповідно до нормативно-технічної документації з оформленням паспортів якості. Лабораторія з контролю якості володіє такими приладами: прилад для тестування плівок на розрив; тестер для підбору оптимальних режимів пайки; термошафа; електронні ваги; мікрометри, цифрові мікроскопи, спектрофотометр, тощо. На підприємстві проводиться контроль напівфабрикатів на кожній стадії виробничого процесу:

– додрукарської підготовки оригінал-макетів;

– плівок для виготовлення фотополімерних друкарських форм;

– фотополімерних друкарських форм;

– виготовлення напівфабрикатів.

Завдяки жорсткому контролю продукції підприємство намагається якнайбільше уникати браку продукції, але повністю уникнути браку неможливо. Це пов’язано з великою кількістю параметрів. Дефекти, що призводять до браку продукції, існують як на готовій продукції, так і на напівфабрикатах. Тому було проведено дослідження статистики відділу з контролю якості для збору інформації щодо дефектів, які викликають брак продукції.

Найбільш часто при флексографічному друці зустрічаються такі проблеми [5]:

а) проблеми взаємодії фарби з підложкою. Фарби в цьому виді друку мають відносно низьку в'язкість, що призводить до високого вбирання до висихання, отже, втрати насиченості друку. Тому найкращою для флексографічного друкування стає УФ-фарба. Її переваги пов'язані з миттєвим затвердінням і відсутністю органічних розчинників;

б) втрата контрастності на відбитку. Це найбільш важлива проблема, яка пов’язана з тим, що флексографські друкарські форми будучи еластичними, сприяють появі ефекту «розтискування» і, як наслідок, відбиток втрачає контрастність.

Необхідними умовами якості стає застосування друкарських форм, що забезпечують мінімальне збільшення тону. Актуальною задачею є обґрунтування методології вибору форм флексографічного друку, а також вибір оптимального обладнання для їх виробництва.

2. Основні дефекти, виявлені на виробництві

На формування градаційних характеристик у флексографському друкарському процесі впливає ряд факторів:

– параметри друкарської форми (тип матеріалу, товщина, жорсткість);

– кріплення друкарських форм на формні вали друкарської машини за допомогою двосторонньої липкої демпфуючої стрічки додатково усереднює тиск в друкарській парі;

– характеристики друкарського процесу (тиск, швидкість, температура сушильного пристрою);

– характеристики анілоксових валів (передана кількість фарби);

– фізико-хімічні та технологічні властивості друкарських фарб;

– тип і властивості процесу задруковування матеріалу (адгезійно-когезійна взаємодія з друкарською фарбою, активація поверхні для полімерних плівок, коронація поверхні тощо) [5].

Якість кінцевої флексографічної продукції визначається підготовкою до друку – особливостями додрукарської підготовки та правильним вибором фотополімерної форми.

За даними проведених досліджень на підприємстві ТОВ «Наргус» виявлено основні чинники, які приводять до браку продукції (рис. 1).

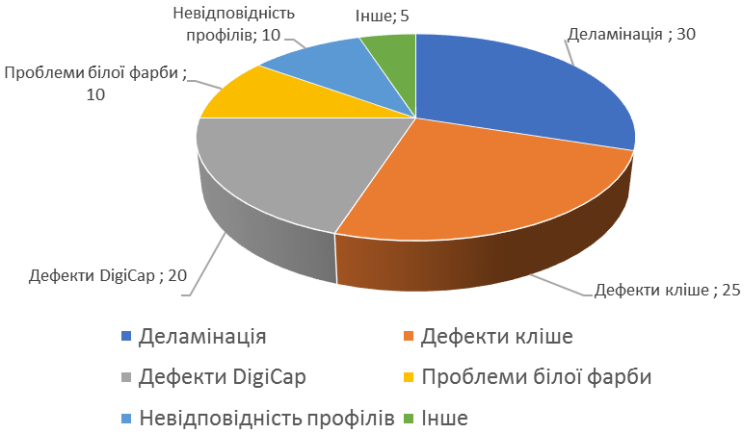


Рис. 1. Статистика браку на підприємстві «Наргус»

Найбільший відсоток (30 %) – це проблеми деламінації (розшарування через фарбу, клей, матеріал тощо). На другому місці (25 %) – дефект кліше (бульбашки на кліше, погане засвічування, побиття озоном). Ще 20 % – проблеми технології DigiCap (наявність смуг мікрорастрування, збільшення наносу, невідповідність кліше під окремі види робіт). Останні 25 % – проблеми з кольоровідтворення, пов'язані з різними причинами, наприклад перенесення білої фарби (різний склад білої фарби від партії до партії; при друкуванні на темних фонах наявність «вікон» білої задруківки) – 10 %, та невідповідність профілю теж 10 %, а ще 5 % – це помилки кольороподілу, матеріалу, фарби, порушення вимог технолога тощо. Це показна статистика, яка відповідає реальному виробництву.

Аналіз наведених даних показує, що 45 % браку пов'язані з друкарськими формами (технологіями їх виготовлення, растрування та обраними фотополімерами). Правильний вибір додрукарських технологій та матеріалів для виготовлення друкарських форм значно знизить процент браку кінцевої продукції. Тому цей етап потребує детального дослідження.

Брак продукції може з'явитися в результаті виникнення різноманітних дефектів фотополімерних флексоформ (кліше). Більшість браку, який виникає у зв'язку з дефектами кліше, це недостатнє експонування друкарських елементів та неправильний вибір технології виготовлення флексоформ.

Щоб зменшити кількість цього виду браку на підприємстві «Наргус», пропонується дослідити різні технології виготовлення фотополімерних форм для флексодруку на невбираючих матеріалах.

Розглянемо непопадання кольору в рамки відхилення dE_{2000} у процесі підготовки друкарського обладнання (приладки) до друку тиражу. Для контролю правильності кольоровідтворення після отримання першого друкованого відбитка на приладці робиться порівняння отриманого кольору з еталоном за допомогою спектрофотометра. Вимірюється відхилення кольору dE_{2000} і відхилення координат кольору ΔL, ΔC, ΔH. Результат вважається задовільним за наступними допустимим відхилення кольору, які наведені в табл. 1.

Таблиця 1

Колориметричні допуски для тріадних та спеціальних фарб

Параметр	Чорний	Блакитний	Пурпурний	Жовтий	Pantone
Допустиме відхилення	L<5, C<3	H<6	H<6	H<6	H<8
Зміна відхилень	E_{2000}<2	E_{2000}<2	E_{2000}<2	E_{2000}<2	E_{2000}<2

Проблеми з відтворенням кольору на відбитку можуть бути вирішені завдяки стандартизації виробництва, що і підтверджено під час виконання досліджень на підприємстві ТОВ «Наргус».

Будь-який етап підготовки макету до друку та відповідно сам процес друку на підприємстві підпорядковується внутрішнім розробленим правилам згідно досвіду та зовнішнім стандартам з друку. Тому розроблені рекомендації щодо покращання процесу кольоровідтворення можуть бути впроваджені на цьому виробництві.

У роботі розглянуто усі етапи відтворення кольору:

– розробка оригінал-макету поліграфічної продукції;

– відтворення особливостей дизайну;

– кольороподіл;

– кольоропроба;

– відтворення необхідного кольорового охоплення завдяки правильному використанню відповідної технології растрування;

– вибір правильних параметрів флексографічних фотополімерних форм та анілоксових валів;

– підготовка фарби до друку.

Для вирішення задач, поставлених в роботі, необхідна наступна експериментальна база: тиражі з наявністю декількох пантонів; різноманітні невбираючі матеріали, на яких відбуватиметься тиражний друк на підприємстві; пігментні фарби, які використовуються для друкування накладу; прободрукарський станок для прокатки фарб; спектрофотометр, цифровий мікроскоп; програмне забезпечення для обчислення оптичних властивостей фарб; пантонне віяло; комплект тестових флексоформ.

3. Аналіз технологічного процесу на ТОВ «НАРГУС»

3.1. Технологічні інструкції з процесу флексодруку

Для того щоб розглянути в повній мірі кольоровідтворення на підприємстві ТОВ «Наргус», проаналізовано особливості технічної документації з процесу флексографічного друку [6].

За годину до початку приладки тиражу старший друкар отримує у начальника зміни наступну документацію: технічне завдання на друк тиражу (ТЗ); технологічну карту (ТК); зразки на приладку, завірені технологом (менеджером) або оригінал-макет (кольоропробу), завірений замовником (менеджером), зразки кольорів.

На ТК має бути присутній підпис особи, яка перевірила правильність монтажу друкарських форм на формних валах. Друкар вивчає в ТЗ і ТК інформацію, що стосується монтажу кліше, фарб і добавок до них, процесу друку, а також всі примітки і рекомендації менеджера, дизайнера, технолога. У разі, якщо друкар виявляє помилку в ТК, чи вважає, що можна зробити зміни в технології друку, що дозволяють поліпшити якість друку, він погоджує пропоновані зміни з технологом з друку (з повідомленням начальника зміни). Будь-які зміни в технічному завданні повинні бути відображені в самому ТЗ і обов'язково узгоджені з представником технічного відділу.

На друкарські секції встановлюються анілоксові і формні вали в порядку, зазначеному в технологічній карті технічного завдання. Формні вали встановлюються відповідно до напряму друку, зазначеним у технологічній карті. Перед установкою анілоксових валів необхідно попередньо переконатися в їх чистоті. Старший друкар контролює результат роботи

колориста щодо підготовки до друку. Під час контролю перевіряються: серії фарб, лаків, праймерів; розташування фарб по секціях; правильність підключення розчинників до секцій з різними фарбами; наявність зазначених в ТК добавок в фарбах або їх відсутність; в'язкість фарб, лаків, праймерів; різні рівні визначення оптичної щільності.

Також у процесі пробного друку перевіряється адгезія фарби. Адгезія характеризує якість зчеплення фарби з поверхнею матеріалу і залежить від поверхневого натягу (активації) поверхні матеріалу і властивостей фарби. Якість адгезії визначається завдяки «скотч-тесту». У процесі друку треба витримувати 100 % адгезію.

Процес підготовки друкарського обладнання та друк гнучкої продукції виконується за детально описаними стандартами і рекомендаціями в повній мірі.

3.2. Технологічні інструкції з використанням фарб в процесі флексодруку

В процесі флексографічного друку на підприємстві «Наргус» використовуються два види фарб: готова фарба і виготовлена на «Станції змішання фарб». Фарби створені на основі сольвентно-водних фарб. На «Станції змішання фарб» базову тріадну фарбу (без освітлювача) необхідно готувати заздалегідь і складувати біля станції. На «Станції змішання фарб» пантонна фарба виготовляється безпосередньо перед тиражем, при відсутності її на складі зворотних фарб. Якщо на новий тираж необхідний пантон, формули якого немає в «базі даних формул Inkmaker», то необхідно виготовити приблизний пантон, керуючись «пантонним віялом». Під час приладки на друкованому відбитку вимірюються оптичні щільності $D_{опт}$ тріадних фарб: C, M, Y, K. Отримані значення порівнюються зі значеннями еталонного зразка або з зазначеними в довідковій таблиці значеннями. Якщо $D_{опт}$ відрізняються в більшу або меншу сторону від табличних значень на величину, яка перевищує ± 0,05, фарба корегується додаванням освітлювача або більш пігментованої фарби.

3.3. Засоби вимірювальної техніки

На всіх етапах виробництва має бути використаний єдиний стандарт освітлення D50 (5000 К). Відбитки необхідно переглядати на спеціальних переглядових пристроях, що забезпечують рівномірне підсвічування знизу розсіяним світлом. Навколишнє освітлення повинно бути рівномірним і вдвічі менш інтенсивним, ніж освітлення в області перегляду.

На підприємстві «Наргус» біля кожної друкарської машини та в дизайн-відділі стоїть переглядовий стіл, завдяки якому можна переглядати кольоропроби за однаковими умовами освітлення в кімнаті. Переглядовий стіл Etman Color view system володіє перемикачами режиму світла, що дозволяє порівняти макет дизайну при різноманітних умовах освітлення.

Для обчислення dE використовується спектрофотометр Standard eXact. Standard eXact був спеціально розроблений для друку упаковки і є провідним на ринку спектрофотометром для перевірки кольору CMYK та спеціальних кольорових фарб.

Контроль в'язкості для флексографічного друку надзвичайно важливий, тому що від в'язкості в значній мірі залежить швидкість висихання фарби, гарне сприйняття її задрукованою поверхнею, чіткість друку, відсутність забивання пробільних елементів друкарської форми. На підприємстві «Наргус» використовуються ручні віскозиметри типу ВЗП-4, призначені для визначення умовної в'язкості лакофарбувальних матеріалів та відносних до них продуктів – ньютонівських або наближених до них рідин через зміну швидкості спливання рідини і поступової конвертації часу за спеціальними таблицями або за допомогою допоміжних засобів у абсолютних одиницях виміру в'язкості. Крім того, на підприємстві існує автоматичний віскозиметр, який встановлено на друкарському обладнанні. Під час друку обов’язково підтримується в’язкість фарби в певних рамках, оскільки можуть виникнути проблеми з просиханням фарби, або її налипанню на задрукованому матеріалі.

Одним з основних недоліків друкарського процесу у флексографії є високий приріст колірного тону. На збільшення тону під час друку впливають і властивості формного матеріалу. Більш точні вимірювання можна отримати з використанням спеціальних спектрофотометрів та цифрових мікроскопів. Для вимірювання параметрів друкарських форм використову-

ється прилад FAG FLEXi PRO, який дозволяє оцінити форму точки в тривимірному вимірюванні і визначити площу растрових точок на друкарській флексоформі.

4. Контроль кольоровідтворення на різних етапах виробництва

4.1. Відділ додрукарської підготовки

На підприємстві «Наргус» існує власний відділ додрукарської підготовки, де дизайнер і препрес-інженер виконують підготовку макетів до друку. Виходячи з можливостей флексографічного друку, дизайнер повинен надати концепцію дизайну, яка дозволить друкарському обладнанню видати всі очікування замовнику. У відділі розроблено рекомендації для створення макету з метою запобігання можливого браку. При бажанні замовника отримувати стабільний відтінок кольору використовують систему пантонних кольорів. Потрібно використовувати власні профілі, оскільки на підприємстві існує як друкарське обладнання так і інші ланки (наприклад монітор препрес-інженера) завдяки яким настає змога стандартизувати кольоровідтворення. Використання власних профілів для кольороподілу і кольоропроби на етапах додрукарського і друкарського процесах – невід'ємна умова стандартизованого поліграфічного технічного процесу. Переваги використання власних профілей на кольоропробі – прискорена приладка і скорочення рекламацій.

Для компенсації невідповідностей кольорових охоплень оригіналу та надрукованого відбитку на підприємстві використовується система семифарбувального друку Opaltone Matching System (OMS). Вона дозволяє розширити колірне охоплення відбитків за рахунок відтворення яскравих синіх, зелених і помаранчевих кольорів, які не можна отримати при тріадному друці, а також дає можливість мінімізувати застосування сумішевих фарб. Саме при введені у макет пантонних кольорів принтер, що друкує кольоропробу, використовує не тільки тріаду фарб, а ще й додаткові фарби для яскравості та точності відтворення пантонних кольорів. На підприємстві для кольоропроб використовують кольоропробний папір EFI Proof Paper, спеціально розроблений для імітації тиражного друку. Він відповідає друкарським паперам з Міжнародного стандарту ISO 12647-2, сертифікованого інститутом FOGRA.

4.2. Особливості виготовлення кліше

Підприємство «Наргус» має свій репроцентр, на якому виготовляються флексоформи, а також іноді замовляє кліше для виконання окремих робіт в ТОВ «Лазерфлекс».

Для виготовлення флексографічної форми використовується технологія «Flexcel NX». Технологія застосовується для фотоформ з термочутливою багатошаровою плівкою, які розроблені компанією KODAK – Flexcel NX 830 Thermal Imaging Layer [7]. На цих фотоформах записується негативне зображення. Після запису зображень, плівку прикочують до звичайної аналогової форми за допомогою ламінатору.

Технологія «KODAK Flexcel NX» вирішує проблему окислення. Вона повністю виключає вплив кислоти на фотополімерний шар у процесі експонування. Сформоване в результаті прямого експонування зображення на фотополімері в точності повторює зображення, сформоване на плівці KODAK TIL, при цьому поверхня растрових точок має абсолютно плоску форму.

Для збільшення оптичної щільності, вимкнення «сивини» на плашках та растрах у системі «Flexcel NX» застосована інноваційна технологія растрування «Kodak DigiCap NX». Програмно-апаратна функція «DigiCap NX» формує на всій поверхні друкарської форми зернистого мікрорельєфу (5x10 мкм), підвищуючи фарбоперенос та якість друку у всіх тональних зонах, включаючи плашки. Застосування даної функції не лише забезпечує відсутність ефекту «сивини» на плашках, але і суттєво збільшує кольорове охоплення, забезпечує якісне відтворення деталей у контрастних кольорах. На підприємстві використовують дві технології растрування DigiCap (рис. 2): standart, advanced. Завдяки технології standart, растрові елементи кліше відтворюються з особливою формою конуса, що дозволяє відтворювати найсклад-

ніші растрові «розтяжки». В свою чергу, технологія advanced відтворює якнайкраще плашкові елементи, завдяки своїй особливій формі зрубленого конуса [7, 8].

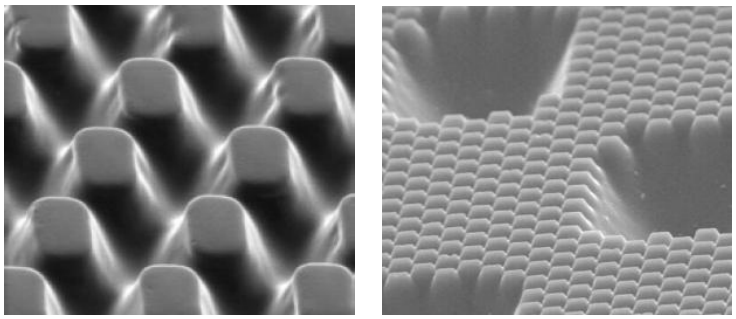


Рис. 2. Технології растрування advanced (зліва) та standart (справа)

4.3. Методика вибору формних пластин

Для аналізу характеристик пластин була розроблена відповідна методика оптимального вибору за репродукційно-графічними і друкарсько-технологічними характеристиками з використанням методу аналізу ієрархії (MAI). В якості критеріїв відбору пластин були визначені параметри, які найбільш пріоритетні для поліграфічних підприємств [5, 9].

Визначення асортименту досліджуваних пластин

Асортимент пластин був звужений на підготовчому етапі. Було проведене опитування групи експертів – фахівців цього підприємства, які обрали найбільш популярні пластини за їх думкою. Під час опитування були враховані критерії: популярність у виробників; ціна; час виготовлення. Для попереднього уточнення найбільш популярних пластин віддалася перевага методу рангу. Експерт повинен оцінити популярність за шкалою відносної значущості в діапазоні від 1 до 11 (оцінюються пластини, які можуть бути застосовані для друкування на невбираючих матеріалах).

Визначення критеріїв порівняння пластин та побудова ієрархії

Основні критерії для порівняння: фарбоперенос; еластичність (модуль пружності, МПа) або жорсткість (ShA); профіль крапки; технологія виготовлення ФПФ; тоновий охват (%); час виготовлення (години); ціна за 1 м^2.

Основні альтернативи: ACE 114D, CtP; FTF 114D, CtP; ACE 114D, NexT C25 MC WSI_P04_P+; Kodak Flexcel NXH.

Всі пластини представлені з різними значеннями товщини. Для уточнення поставленої задачі обираємо фіксовану товщину – 1,14 мм. Вона найбільш застосовувана для виготовлення гнучких пакувань, тобто для друку на тонких плівках. Відповідно, ціна та час виготовлення буде вказана саме для пластин цієї товщини.

Були також оцінені пріоритети для поліграфічних підприємств, наприклад еластичність важливіша для споживачів, ніж набухання форми, тому що тиражі все частіше стають не об'ємними, результат еластичності видно відразу, в той час, як форма набухає від розчинників не так швидко. Фактор ціни так само важливий для споживачів, як фарбоперенос форми, тому що він оцінюється безпосередньо кінцевим замовником і впливає на привабливість кінцевої продукції. Внаслідок цього можна оцінити частку того чи іншого параметра форм в частковому співвідношенні від єдиного цілого поняття пріоритетності.

За допомогою методу MAI здійснюється вибір формної пластини для виготовлення фотополімерної форми, призначеної для друку на тонких невбираючих матеріалах.

Побудова матриць попарних порівнянь та їх аналіз

Розглянемо процедуру побудови матриці попарних порівнянь критеріїв.

Кількість порівнянь, які здійснював експерт на рівні 2 становить $K_{порівн} = \frac{n(n-1)}{2}$.

$K_{порівн.} = 7(7-1)/2 = 21$. Матриця порівнянь наведена в табл. 2.

Таблиця 2

Матриця та результати парних порівнянь для критеріїв

Номер рядка (i)	Критерії	Номер стовпця (j)							Вага в долях	Вага, %	Ранг
		1	2	3	4	5	6	7			
1	Фарбоперенос	1	1/3	1/5	1/3	1	9	1/5	0,103	10,27%	6
2	Жорсткість	3	1	1/5	3	1	7	1/3	0,137	13,68%	4
3	Профіль крапки	5	5	1	1	3	1/5	1	0,218	21,77%	1
4	Технологія	3	1/3	1	1	1/5	1/3	1/7	0,062	6,18%	7
5	Тоновий охват	1	1	1/3	5	1	3	1	0,131	13,11%	5
6	Час виготовлення	1/9	1/7	5	3	1/3	1	1	0,149	14,91%	3
7	Ціна	5	3	1	7	1	1	1	0,201	20,08%	2

За результатами експертних оцінювань критеріїв визначаємо їх важливість (рис. 3).

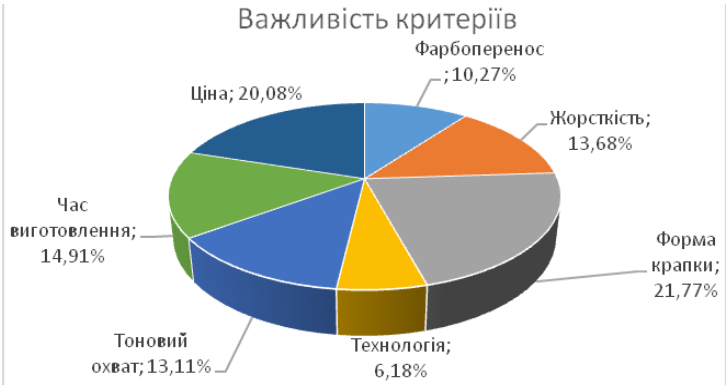


Рис. 3. Аналіз критеріїв вибору полімерних флексоформ

З точки зору задоволення нашої мети найбільш вагомим є критерій «Форма крапки» (21,77 %). Це пояснюється підвищеними вимогами до якості флексодруку на невбираючих матеріалах. Це зазвичай пакування, які вимагають точності відтворення кольорів, напівтонів та насиченості плашки (особливо для пантонних фарб). Це дозволяє тільки пласка точка. Далі слідує ціна (20,08 %). Що теж відповідає вимогам замовника. Фотополімерні кліше мають досить високу ціну. Замовники згодні платити таку ціну за якісну продукцію, але виробники повинні розглянути можливість зниження цього показника за рахунок технологічних інновацій для збільшення попиту у замовників. Досить вагомий, але значно менший за попередні, критерій «Час виготовлення фотополімерних форм» (14,91 %). Це пов'язано з тим, що для неперервного технологічного процесу кожна затримка у часі досить проблемна й тягне за собою простоювання обладнання і, відповідно, матеріальні витрати. Майже на такому ж рівні критерії «Жорсткість пластини» (13,68 %) та «Тоновий охват» (13,11 %). Вони впливають на властивості форм відтворювати необхідну якість зображень під час друку. Для всіх пластин це нормовані і стабільні значення, тому вони майже внизу рейтингу. Потім слідує «Фарбоперенос» (10,27 %). І на останньому місці технології виготовлення – всі вони показують дуже високі показники якості.

За результатами проведених розрахунків перше місце посідають ACE 114D, NexT C25. Технологія nyloflex Next дозволяє сформувати стійку структуру растрових точок на формі, які не випадають у процесі друкування тиражу, що забезпечує стабільне та плавне відтворення градієнтів аж до значення 0 % та широкий тоновий діапазон. Сформовані мікроструктури дозволяють підвищити оптичну густину плашок.

Для отримання відбитків високої якості з розширеним діапазоном градацій також рекомендується використовувати комбінацію гібридного растру HD Flexo C25 MCWSI P+ з технологією плоскої точки nyloflex Next. Не зважаючи на різницю у ціні між ACE 114D, NexT C25 та ACE 114D приблизно в півтора рази, можна рекомендувати ці пластини на ті поліграфічні

фічні підприємства, які на перший план становлять якість продукції. Ці пластини допомагають зменшити кількість браку і забезпечити високу якість.

На другому місці пластини Kodak Flexcel NXH. Вони мають вищу оптичну щільність. Програмно-апаратна функція «DigiCap NX», яка є безкоштовною, формує на всій поверхні друкарської форми зернистий мікрорельєф, що помітно підвищує фарбоперенесення та якість друку у всьому тональному діапазоні, включаючи плашки. Застосування цієї функції не тільки усуває ефект «сивини» на плашках, але й суттєво збільшує колірне охоплення, а також забезпечує якісне відтворення деталей у високих кольорах. Але ці пластини дорожче та потребують більше часу на їх виготовлення. Друкарські форми за технологією Flexcell NX можна рекомендувати виробникам поліграфічної продукції для підвищення якості друкованої продукції, але на тих тиражах, які не дуже термінові.

4.4. Виробничий цех

Коли макет дизайну створено, кліше експоноване – машина готується до друку тиражу. Друкарське обладнання провідних світових виробників «Fischer & Krecke» серії BOBST (F&K 20SIX) дозволяє друкувати на всіх видах полімерних матеріалів шириною до 1250 мм, десятьма фарбами, з діапазоном довжини відбитка від 300 до 670 мм. Машина оснащена системами комп'ютерного контролю і управління процесом друку, системою GPS, комп'ютерними відео-системами контролю кольору, що дозволяє постійно підтримувати високу якість відбитка.

Встановлення відеосистеми контролю якості відбитків допоможе підтримувати контроль кольору, та відстеження дефектів під час швидкісного друку. Будь-які дефекти легше виявити та виправити завдяки постійному контролю. Покращена реєстрація кольорів та моніторинг, масштаб, що збільшує зображення у 10 разів дозволяє дуже точно реєструвати «плями» та «бруд», а також здійснювати перевірку тексту та інших друкарських знаків. Відходи зменшуються, оскільки оператор машини може негайно вносити виправлення, поки машина друкує. Отже, друк займає менше часу і використовується менше матеріалу.

До початку друку друкар згідно з технологічною картою підбирає анілоксові вали, які різняться за такими параметрами: виробник; тип гравірування; лініатура аніліоксу; належність до певної друкарської машини. Для задруковування плашкових елементів використовуються анілоксові вали від 80 лін./дюйм до 240 лін./дюйм, для растрових елементів від 280 лін./дюйм до 500 лін./дюйм. Оскільки пантони в більшості використовуються в плашкових елементах, технолог обирає переважно низьколініатурні вали [6].

4.5. Станція змішування фарби

Основна функція, яку виконує станція змішування фарби, це – відтворення нової фарби та її зберігання. Доставка, транспортування і зберігання фарб. Термін зберігання фарб – не більше року. Після закінчення цього терміну, так само як і при недотриманні умов зберігання і транспортування, фарба може бути використана тільки після попереднього тестування на друкарські та колористичні властивості. З часом фарба пігментується, що позначається на друці продукції – виникають дефекти. Тріадна фарба зберігається у великих бочках, з яких дозують фарбу на тираж, в той час коли пантонна фарба зберігається у невеликих відрах, з певним номером на ній та вифарбовкою.

Оскільки підприємство має автоматизовану систему управління «1С: Поліграфічне підприємство 8», знаходити певне відро з пантоном дуже просто та швидко. Всі дані з вифарбовок зберігаються в АСУ, тому, при необхідності вибору конкретного пантону, треба лише вказати координати фарби. Формули пантонів формуються по суб’єктивним характеристикам L (світлота) C (насиченість) H (тон). Завдяки колу Іттена колорист змішує відповідні пігменти фарби для отримання певного номеру пантону.

4.6. Кольороподіл та профілювання

Процес відтворення кольору починається на стадії розробки дизайну – в дизайн-студії. Дизайн-відділ виконує функцію перевірки кольорів в макеті та кольороподілу. Дизайн розбивається на тріаду (CMYK), при необхідності, додаються пантони. Дизайнери узгоджують дизайн з менеджерами, а вони насамперед домовляються з замовниками. Якщо замовників все задовольняє, ТЗ рухається до технічного відділу, де вже прописується ТЗ з параметрами, які будуть використовуватися для друку. Оскільки ТОВ «Наргус» має власні друкарські машини та поєднаний з цим дизайн-відділ, воно має можливість друкувати тестові шкали для створення профілей під різноманітні матеріали.

Підприємство має широкий спектр матеріалів, які воно пропонує для друку продукції, але кожний матеріал має свої оптичні властивості та фізико-хімічні властивості, які впливають на оптичні властивості фарб. Для компенсації цих властивостей матеріалу використовують профілі. Щоб створити такий профайл, створюють технічне завдання в якому будуть друкуватися спеціальні тестові шкали на різноманітних матеріалах. Після чого, ці тести відносять до менеджера з кольоропроби [6]. Завдяки програмному забезпеченню та спектрофотометру від компанії X-Rite, за певними налаштуваннями будується профіль матеріалу, який буде передано до дизайн відділу у вигляді електронного формату .icc.

4.7. Особливості кольоропроби на підприємстві

Після того, як дизайнер отримує технічне завдання від менеджера з продажів, в якому вказаний певний матеріал, дизайнер обирає необхідний профіль і виконує кольороподіл згідно з профілем: тобто на його екрані буде відображено зображення, як би воно вийшло, якщо друкувалося на флексографічному обладнанні в підприємстві «Наргус». Профілі робляться лише під обладнання підприємства. Після того, як дизайнер зробив певний дизайн, друкується кольоропроба, яка максимально точно передає зображення, якби воно друкувалося на друкарській машині підприємства.

Щоб в дійсності кольоропроба відповідала зображенню на екрані, дизайнерські монітори калібрують за допомогою калібратора X-Rite. Наступний етап – друкування кольоропроби та її оптимізація. Здійснюється перевірка точності імітації кольору системою для кольоропроби і при необхідності проводиться оптимізація.

Друкування кольоропроби виконується на професійному принтері від компанії Epson. Використовуються спеціальний папір для кольоропроби EFI Proofing Paper, який практично позбавлений оптичних відбілювачів і забезпечує відмінні умови для друку кольоропроби з ефективним управлінням кольору. Після того, як замовник побачить кольоропробу вже на певному матеріалу та з урахуванням друкарського обладнання, на якому буде виконаний друк тиражу (враховується на кольоропробі), підписується акт договору про друк тиражу.

4.8. Обґрунтування підготовки пантонів до друку тиражу

Замовник встановлює, чи хоче він використовувати у друці дизайну пантони. Найскладнішим етапом при підготовці фарб на новий тираж є підготовка пантонних кольорів. Головною перевагою пантонних кольорів в тому, що існує паперове та електронне віяло. Завдяки ним колорист за допомогою спектрофотометру від компанії X-Rite може замірювати відхилення віяла від того, що вийшло при друці пантону на друкарському обладнанні. Але є й недоліки такої системи: паперове віяло дуже швидко стирається, віяла мають відхилення між собою (у деяких кольорах відхилення, за стандартом CIE2000, dE>4), формули створення пантонних кольорів не відповідають фарбам, які використовуються на підприємстві.

Перше питання – це стандартизація пантонних кольорів для друку на флексографічному підприємстві «Наргус». Не зважаючи на те, що формули не відповідають фарбам на підприємстві, існує ще більш значна проблема – різноманітна кількість матеріалів, які використовуються для друку. Наприклад: якщо пантон або тріадні фарби будуть друкуватися на матовій плівці, в порівнянні з прозорою плівкою – ці фарби будуть менш «світліші» (Lightness),

більш «брудніші» (Chromasity), та буде змінений кут тону фарби (Hue). Ці параметри допомагають описати оптичні властивості будь-якої фарби на виробництві, завдяки цим параметрам описується відхилення від еталонного кольору.

Для вирішення такої суттєвої проблеми компанією було вирішено купити австрійське програмне забезпечення, яке б передбачало, яку формулу потрібно створити (змішування пігментів основних фарб) для відтворення пантону. Оскільки таке передбачення не однозначне, для його перевірки треба зробити «прокатку» фарби на прободрукарському станку.

Було обрано декілька технічних завдань, в яких використано декілька різних пантонів, з різними матеріалами, на яких вони будуть друкуватися. Завдяки великій базі підприємства, обираються схожі пантони, з мінімальними відхиленнями. Щоб перевірити, чи підходить цей пантон, – з іншої бази (з формулами пантонів) змішуються основні фарби згідно з формулою у спеціальному мірному стаканчику. Фарба добре розмішується та завдяки піпетці береться близько 5 грамів фарби і наноситься на друкарський станок біля матеріалу. Робиться прокатка на потрібному матеріалі та порівнюється з електронним віялом. Якщо дельта Е фарби менше 5, її можна вже заносити в базу та віддавати у друк, але, якщо дельта більше, треба коригувати формулу або розробляти нову.

Після того, як формули було розроблено та видано на приладку тиражу, робиться перший викат фарби та порівняння з еталонною кольоропробою – пантони звіряють з електронним віялом завдяки спектрофотометру від компанії X-Rite eXact.

Для дослідження пантонів на різноманітних матеріалах було зроблено таблицю відхилень значень пантонних кольорів від теоретичних значень (табл. 3).

Таблиця 3

Відхилення пантонів від теоретичних значень

Матеріал	Теоретичний пантон	Фактичний пантон	Дельта			
			L	C	H	De2000
ПЭТпр 12 + Пленка пр 50	2144	2119	26,21	-2	-50,21	36,95
ПЭТпр 12 + Пленка пр 50	2747	2746	-3,61	-3,53	0,56	2,72
ПЭТпр 12 + Пленка пр 40	2347	2347	0,11	-1,23	-2,69	2,19
ПЭТмат 12 + БОППмет 20	1915	198	0,25	-2,37	5,02	2,9
ПЭТмат 12 + БОППмет 20	7481	3522	2,87	-3,12	-6,39	4,31
ПЭТмат 12 + БОППмет 20	3515	3515	-2,39	-1,43	-0,25	1,82
ПЭТмат 12 + БОППмет 20	7427	187	-2,09	-7,26	-7,44	4,9
ПЭТпр 12 + ПЭВДбел 70	2322	469	-1,81	-7,04	10,32	5,5
ПЭТпр 12 + ПЭВДбел 70	7726	356	4,66	10,02	10,9	7,27
ПЭТпр 12 + ПЭВДбел 80	390	384	2,08	5,33	-6,95	5,5
ПЭТпр 12 + ПЭВДбел 80	186	1795	-0,83	-10,12	-5,16	4,45
ПЭТмат 12 + ПЭВДбел 140	7438	2066	-0,01	-7,62	-2,17	2,85
ПЭТпр 12 + БОППмет 20	320	320	1,66	-0,56	0,46	1,69

Завдяки цій таблиці бачимо, що з 13 підготовлених пантонів 9 відповідають стандарту дельта Е2000. У стовбці «Теоретичний пантон» – це той пантон, що готувався на станції фарб, заміряний на тому ж самому матеріалі, та прокатаний на прокатному станку. У стовбці «Фактичний пантон» – заміряний пантон, що був використаний під час друку тиражу.

Чим вища лініатура анілоксового валу, тим «світлішим» вийде пантон, чим нижча – тим «темнішим». Ми можемо прослідкувати цю залежність в першому замірі пантону 2144. Планувалося розробити більш світліший пантон для високолініатурного валу, але він кардинально змінився внаслідок того, що друкар ввів низьколініатурний вал. Про що кажуть і заміри дельта Е, які більше ніж 30.

Дані таблиці показують, що чистота (С) кольору завжди виходить більша, по світлості (L) майже не має змін, а по тону (H) все залежить від самого кольору фарби.

4.9. Рекомендації щодо підбору фарб для точного кольоровідтворення

Завдяки аналізу, проведеному в роботі, були розроблені рекомендації щодо автоматизації підбору фарб пантонів для будь-якого матеріалу з необхідною точністю:

– аналізувати макет дизайну та його кольороподіл щоб: підібрати теоретичний анілоксовий вал, яким буде друкуватися тираж згідно з лініатурою, наявністю плашкових елементів чи растрових; чи друкується пантон в один прохід без підкладки іншого кольору;

– перевірити матеріал, на якому буде друкуватися тираж: при наявності матового матеріалу слід урахувати, що dC повинна бути значно більша за підбираючий пантон (приблизно на сім одиниць); для прозорого матеріалу dC повинна >2, а dL <2; для друку на прозорому матеріалі без білої фарби (другий шар білий матеріал), слід врахувати, що білий поліпропілен – не чистий білий, а жовтить за кутом «Н» на три одиниці;

– при наявності АСУ: слід шукати схожі пантони в базі даних. Звертати увагу на dH – не перевищувати >5, відносно підбираючого пантону;

– при відсутності АСУ: на станції виготовлення фарби, підбирати за мінімальною dE пантони, відносно підбираючого пантону;

– після підбору схожого пантону розробити формулу пантону на тираж (використання спеціальних програм змішення фарб); намагатися не використовувати більше ніж три пігменти у фарбі;

– завжди робити прокатку фарби на прободрукарському станку з тим матеріалом, на якому буде друкуватися основний тираж;

– завжди заміряти прокатки на фотопапері (кольоропробний папір);

– при наявності другого шару, для більш точного підбору – імітувати ламінування завдяки невеликої кількості води, накрапаною на другий шар;

– враховувати, що при зміні лініатури анілоксового валу буде змінено відтінок, насиченість та світлота фарби.

Для швидкісного і точного підбору фарб потрібно мати програмне та апаратне забезпечення; знати основні процеси флексодруку; мати уявлення, як змішується фарба (за колом Іттена) та які параметри зміняться при змішуванні певних пігментів. При наявності всіх складових, підприємство буде забезпечено швидкісним підбором пантонів на тираж та мінімальними затратами на приладку друкарського обладнання.

Висновки

Проведено аналіз процесу контролю якості на підприємстві ТОВ «Наргус», проаналізовано статистику браку на виробництві та причини його виникнення; розглянуто особливості використання фарб в процесі флексодруку. Розглянуто всі етапи, які включали в себе відтворення кольору та його стандартизацію. Описано етапи підготовки фарби до друку. Розглянуто додрукарські процеси, які відтворюють колір: препрес, кольоровий менеджмент, колористика. Описано технологічний процес підготовки фарби та надано рекомендації щодо коригування та стандартизації кольору на підприємстві.

Проаналізовано процес підготовки пантоних кольорів до друку тиражу; створено таблицю залежності відхилень пантонів на різноманітних матеріалах; розроблено методику підвищення швидкості підбору фарби та рекомендації щодо її застосування.

Встановлено, що виникаючий брак на підприємстві «Наргус», спричинений дефектом «Перевищення норм за dE_{2000}», може бути усунений повністю або частково. Проблему можна вирішити стандартизацією підбору фарби до початку друку, що зменшить час приладки та витрати матеріалів.

Виявлено, що на якість продукції впливає якість додрукарської підготовки та процес виготовлення флексоформ. Методом аналізу ієрархій виявлені чинники, які мають найбільший вплив на якість флексографічної форми під час друку на невбираючих матеріалах, та розроблена методика оптимального вибору формних пластин для невбираючих матеріалів.

Отримані результати говорять про те, що підготовка пантонів на прокатному станку впливає на приладку, також, якщо проаналізувати, який анілоксовий вал буде на тиражі, – можна з високою точністю припустити реальний пантон, який вийде в процесі друку. Відповідно, налагодження останнього етапу стандартизування кольору на підприємстві дозволяє підвищити ефективність приладки тиражу та зменшити витрати.

Список літератури:

1. Цифровая эра упаковки. http://machouse.ua/press-center/s3/news/ tsifrovaja-era-upakovki.html.
2. Рынок цифровой печати Украины: предчувствие изменений. https://printus.com.ua/article/read/3778.
3. Статистика. Исследование Smithers про будущее упаковки в период пандемии COVID-19. https://www.publish.ru/news/202011_20093065.
4. Сайт «Наргус». http://nargus.com.ua/ru.
5. Разработка и апробации методики комплексной оценки уровня качества флексопечати экструзионной упаковки / Манаков В.П., Чеботарева И.Б., Чеботарев Р.И., Муравьева А.В. // Traektoriâ Nauki = Path of Science. 2016. №4. https://cyberleninka.ru/article/n/razrabotka-i-aprobatsii-metodiki-kompleksnoy-otsenki-urovnya-kachestva-fleksopechati-ekstruzionnoy-upakovki.
6. Поленок Д.В., Чеботарьова І.Б. Основні етапи виготовлення гнучкої рулонної упаковки на підприємстві "Наргус": PRINT, MULTIMEDIA & WEB // Матеріали молодіжної школи-семінару V Міжнародної науково-технічної конференції (3 листопада 2020, м. Харків). 2020. С. 84-86.
7. Микрорастирование Kodak Digicap NX. http://es-print.info/catalog/oborudovanie/kodak-flexcel-nx/mikrorastirovanie-kodak-digicap-nx.html.
8. Технология Flat Top Dots в изготовлении флексографских печатных форм / М.П. Кулинченко, М.Г. Зубченко, М.А. Чабан, И.Б. Чеботарева // Бионика интеллекта. 2016. №1 (86). С. 149-154.
9. Саати Т. Принятие решений. Метод анализа иерархий. https://pqm-online.com/assets/files/lib/books/saaty.pdf.

Надійшла до редколегії 11.05.2022

Відомості про авторів:

Вовк Олександр Володимирович – канд. техн. наук, доцент, доцент кафедри медіасистем і технологій, Харківський національний університет радіоелектроніки; Україна; e-mail: oleksandr.vovk@nure.ua; ORCID: https://orcid.org/0000-0001-9072-1634

Чеботарьова Ірина Борисівна – ст. викладач кафедри медіасистем і технологій, Харківський національний університет радіоелектроніки; Україна; e-mail: iryna.chebotarova@nure.ua; ORCID: https://orcid.org/0000-0003-0105-4484

Поленок Денис Віталійович – магістр кафедри медіасистем і технологій; Харківський національний університет радіоелектроніки; Україна; e-mail: denys.polenok@nure.ua

УДК 621.391:519.246.8 **DOI:10.30837/rt.2022.2.209.24**

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

МОДЕЛЬ ОЦІНЮВАННЯ СТАТИСТИЧНИХ ХАРАКТЕРИСТИК ДОВГОСТРОКОВОЇ СКЛАДОВОЇ ВИПАДКОВОГО ПРОЦЕСУ НА ПРИКЛАДІ АНАЛІЗУ СЕРЕДНЬОМІСЯЧНИХ ТЕМПЕРАТУР

Вступ

Оцінювання статистичних характеристик складових випадкових процесів, що спостерігаються в різних галузях людської діяльності протягом досить тривалих проміжків часу, є актуальним завданням. Актуальною є проблема виділення довготривалих корельованих складових акустичного сигналу БПЛА, що формують спектральний пік в низькочастотної області спектра [1 – 3]. Виділення спектру сигналу БПЛА в області низьких частот з використанням відповідних математичних моделей дозволяє ефективно виділяти БПЛА на фоні шумів та перешкод, що формуються іншими джерелами звуку [4 – 6].

Використання моделі авторегресії дозволяє також оцінювати параметри та розпізнавати сигнали [7, 8] на фоні перешкод, розпізнавати людину за голосом [9]. Актуальна, зокрема, проблема оцінки довготривалої зміни клімату Землі під дією природних та антропогенних факторів, яка цікавить не лише кліматологів, а й економістів, політиків, а також фахівців інших галузей [10].

З'ясувалося, що на температуру атмосфери впливає багато чинників: склад атмосфери; промислові викиди у повітря; активність Сонця; періодичні похолодання на Землі, що призводять до льодовикових періодів; зіткнення Землі з астероїдами та метеоритами; викиди у повітря великих вулканів; зміни у нерівномірному нагріванні земної поверхні та ін.

Особливий інтерес викликає вплив людини у вигляді викидів промислових підприємств на склад атмосфери Землі, отже, і температуру Землі. На думку ряду експертів, подолання кліматичних аномалій коштуватиме трильйони доларів на рік протягом 30 років. Тому актуальним є облік впливу людини на температуру атмосфери Землі та запобігання льодовиковим періодам [10, 11]. Для цього необхідно зокрема удосконалення методів аналізу змін температури, що фіксуються метеостанціями в різних точках Землі.

Метою дослідження був аналіз методу та моделі для оцінювання статистичних характеристик довгострокової складової випадкового процесу на прикладі аналізу середньомісячних температур. Отримані результати можуть використовуватися для аналізу середньострокових та довгострокових змін атмосферних явищ, уточнення результатів, отриманих традиційними методами математичної статистики, а також в інших сферах діяльності, наприклад для розпізнавання різних типів БПЛА.

Постановка задачі

У статті розглядається можливість знаходження параметрів слабких довгострокових змін випадкового процесу за наявності потужних короткострокових сезонних періодичних збурень. Для аналізу довгострокової зміни температури використовувалися дані середньомісячних значень температури атмосфери (3108 відліків) (рис. 1), отримані Пулковською обсерваторією за 259 років – з 1752 по 2010 р.

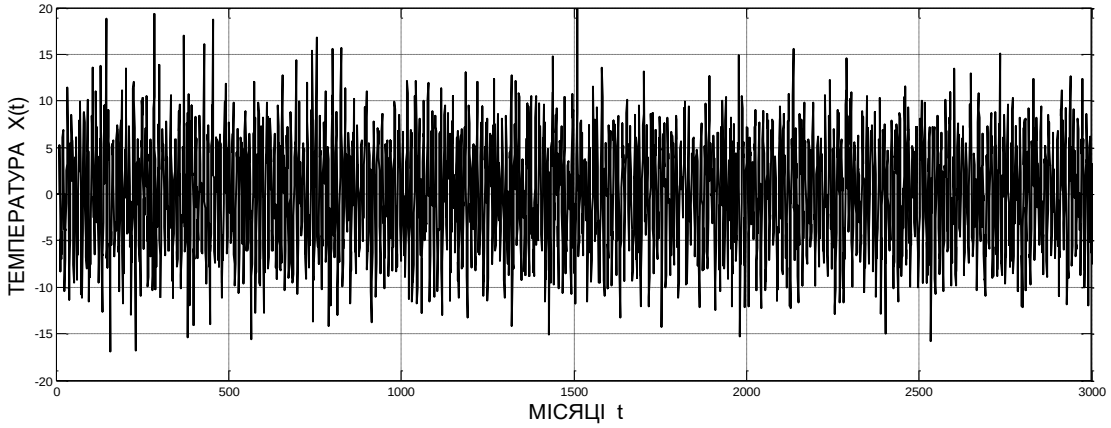


Рис. 1. Дані середньомісячних значень температури, зафіксованих у метеообсерваторії міста Пулкове (Санкт-Петербург)

На рис. 2 представлені дані середньомісячних температур, зафіксованих метеообсерваторією міста Сент-Луїс, шт. Міссурі [11] з 1845 по 1978 р. Подані на рис. 1, 2 дані містять слабкий тренд, пов'язаний із довготривалою зміною температури, сезонні коливання з періодом 12 місяців та стаціонарний процес змін середньомісячних температур.

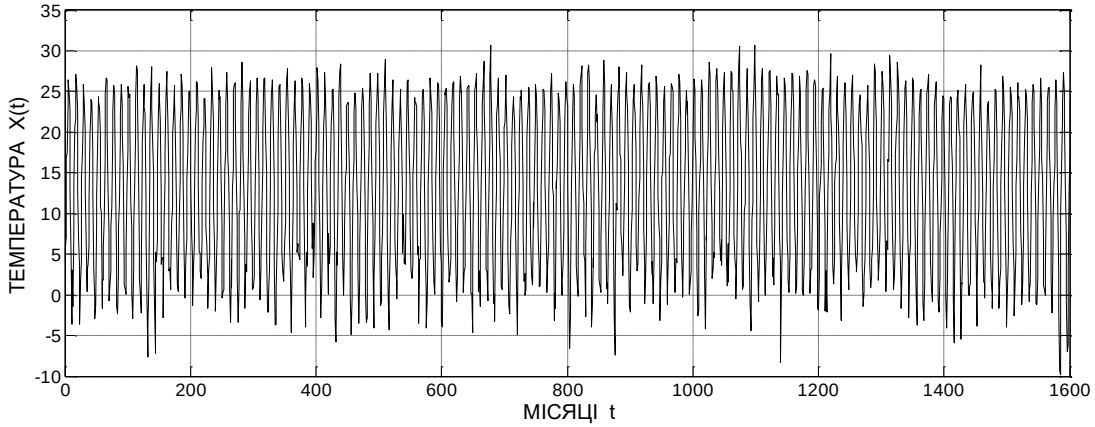


Рис. 2. Дані середньомісячних значень температури, зафіксованих у метеообсерваторії міста Сент-Луїс, штат Міссурі

Модель АРПКС сезонної складової та тренду температур

В основу математичної моделі для оцінювання статистичних характеристик довгострокової складової випадкового процесу покладемо модель авторегресії та проінтегрованого ковзного середнього (АРПКС) [12]. Нехай процес $x[t]$ містить тренд, сезонну складову та стаціонарний процес, який описуватимемо в загальному випадку моделлю авторегресії ковзного середнього (АРСС). Це класична модель декомпозиції нестаціонарного процесу [13].

Мультиплікативний процес $\omega[t]$ без сезонної складової і тренду можна записати у вигляді [12]

$$\omega[t]=\nabla^d\nabla_s x[t]=(1-z)^d\,(1-z_s)\,x[t]=\nabla^d\omega_1[t] \tag{1}$$

Розглянемо оператори, що входять до (1). Для виключення сезонної складової застосовується оператор різниці $\nabla_s=1-z^{-s}$, де z^{-s} – оператор зсуву, дія якого визначається виразом

$z^{-s}x[t]=x[t-s]$. Тоді процес без сезонної складової, з трендом та стаціонарної складовими, записується у вигляді

$$\omega_1[t]=\nabla_s x[t]=(1-z_s)x[t].$$

Щоб виключити тренд з часового ряду $\omega_1[t]$, необхідно впливати на нього оператором $\nabla^d=(1-z)^d$, тобто [5]

$$\omega[t]=(1-z)^d\,\omega_1[t]. \tag{2}$$

Для лінійного тренду зазвичай вважають $d=1$, а для квадратичного тренду необхідно використовувати $d=2$ і так далі. Для лінійного тренду з (2) отримуємо, при $d=1$

$$\omega[t]=\nabla\omega_1[t]=\omega_1[t]-\omega_1[t-1]. \tag{3}$$

Для квадратичного тренду отримуємо вираз (2), при $d=2$. Тоді, з користуванням (3), маємо вираз для процесів без сезонної складової та квадратичного тренду

$$\omega[t]=\nabla^2\omega_1[t]=\nabla(\omega_1[t]-\omega_1[t-1])=(\omega_1[t]-2\omega_1[t-1]+\omega_1[t-2]).$$

Зауважимо, що оператори, що усувають сезонні коливання, діють не тільки на сезонність процесу, а й на інші складові нестаціонарного процесу [14, 15]. Як показали експерименти, видалення сезонної складової сильно впливає на тренд і слабко впливає на стаціонарну складову процесу АРПКС. Операція видалення тренду слабко впливає на властивості сезонної складової і на стаціонарну складову процесу.

На рис. 3, 4 показано вибірки даних середньомісячних температур після видалення сезонної складової. Порівняння із графіками на рис. 1, 2 показує, що видалення сезонної складової в часових рядах середньомісячних температур не призводить до виявлення слабкого тренду. За графіками на рис. 3, 4 складно визначити наявність довготривалих змін температури та виявити форму їхнього тренду.

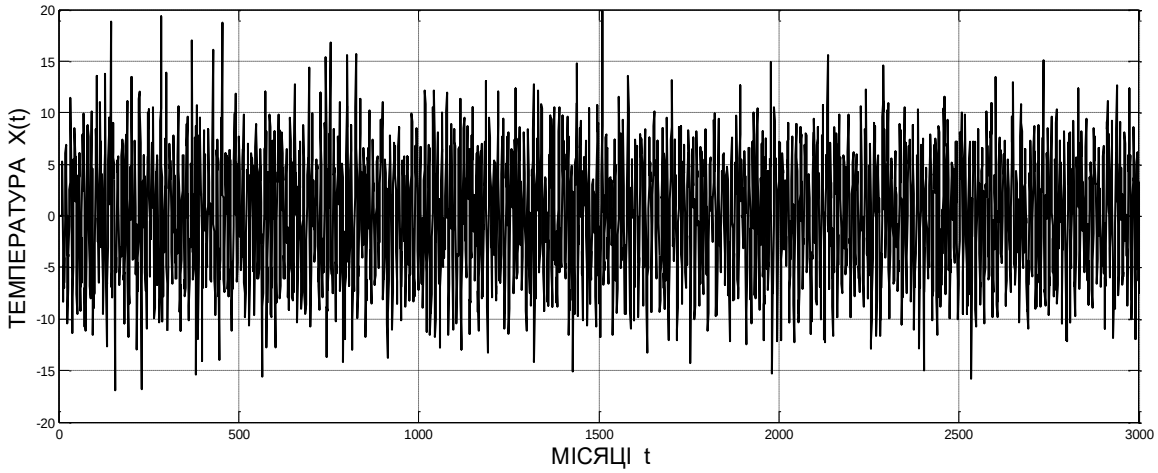


Рис. 3. Часовий ряд даних середньомісячних температур, зафіксованих у метеообсерваторії міста Пулкове, після видалення сезонної складової

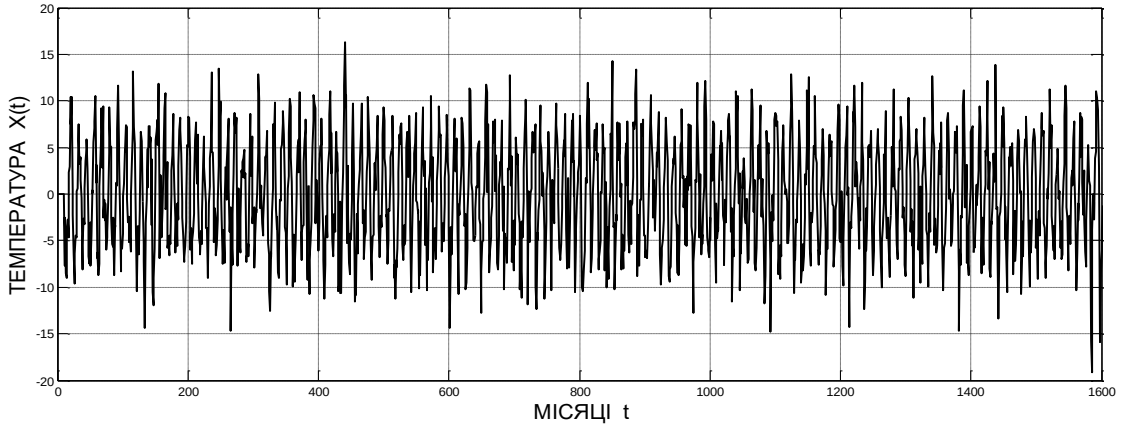


Рис. 4. Часовий ряд даних середньомісячних температур, зафіксованих у метеообсерваторії міста Сент-Луїс, після видалення сезонної складової

Виділення тренду температур

За даними миттєвих значень середньомісячних температур показаних на рис. 1, 2, важко визначити, чи є тренд температур. Видалення сезонної складової з використанням моделі АРПКС не дозволяє виділити довготривалий тренд температур.

Для оцінки тренду, знайдемо спочатку часовий ряд ковзним усередненням по кожному з відрізків, що складається з 12 місяців:

$$\omega_1[t^{'}] = \frac{1}{n}\sum_{i=1}^{n} x[i + t^{'} - 1], \;\; n = 12, \tag{4}$$

де $t^{'} = 1,...,m,$ а $m-$ кількість років спостережень середньомісячних температур. На рис. 5 представлено дані середньорічних змін температури, показані на рис. 1.

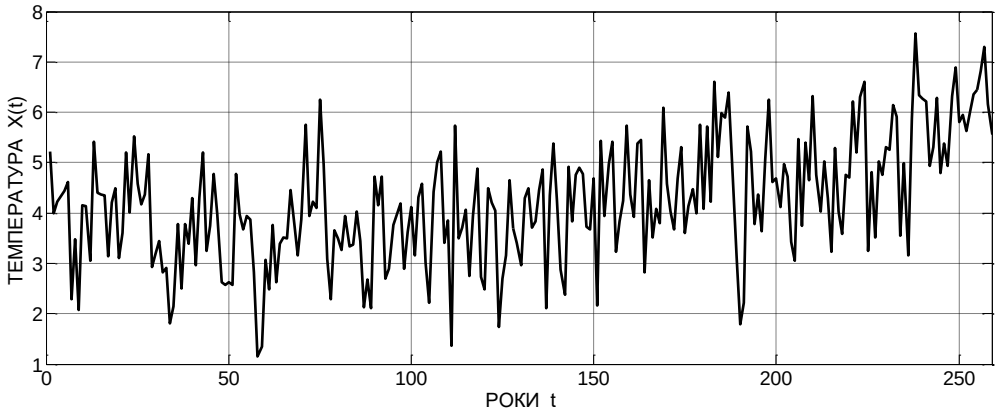


Рис. 5. Зміни середньорічних температур у м. Пулкове

На рис. 6 представлено дані середньорічних змін температури, показаних на рис. 2, знайдені за допомогою (4). Як показує аналіз даних, представлений на графіках (рис. 5, 6), спостерігається тренд середньорічних температур.

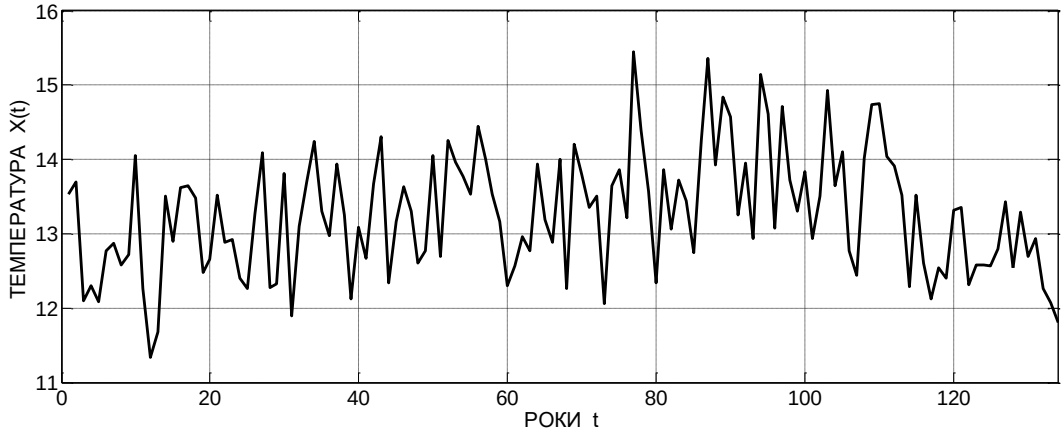


Рис. 6. Зміни середньорічних температур у місті Сент-Луїс

Чисельна оцінка тренду температур

Щоб отримати тренд довготривалої зміни температур протягом всього періоду спостереження, згладимо середньорічні значення, показані рис. 5, 6 за допомогою низькочастотного фільтра. Для зручності представлення даних продовжимо кожне значення тренду на 12 відліків. Тоді отримаємо часові ряди первісної довжини.

Аналіз тренду рис. 7 показує, що з 1752 до 1803 р. температура падала з 4,045 °С до 3,446 °С. Спад температури становив 0,599 °С. З 1804 р. спостерігалося зростання температури з 3,446 °С до 5,961 °С у 2010 р. Приріст температури за цей період становив 2,515 °С.

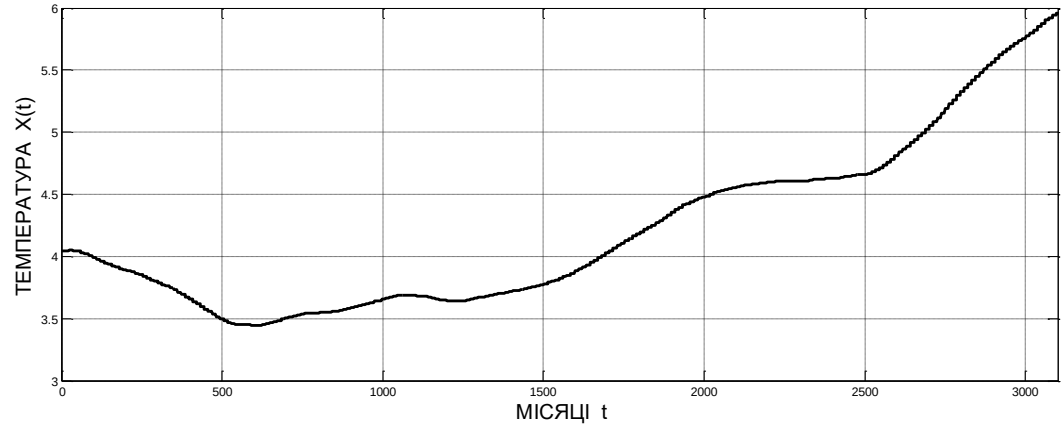


Рис. 7. Тренд температур у м. Пулкове, отриманий ковзним середнім
від зміни середньорічних температур

Аналіз тренду на рис. 8 показує, що з 1845 до 1935 р. температура зросла з 12,82 °С до 13,76 °С. Зростання температури склало 0,947 °С. Але з 1936 спостерігалося падіння температури з 13,76 ° С до 12,79 ° С в 1978 р. Падіння температури за цей термін становило 0,974 °С. Таким чином зростання температури у цій місцевості спостерігався лише з 1845 р. до 1935 р., а потім, до кінця спостережень у 1978 р., температура падала. Це вказує на те, що останнім часом температура повітря не для всіх місць Землі має тенденцію до зростання.

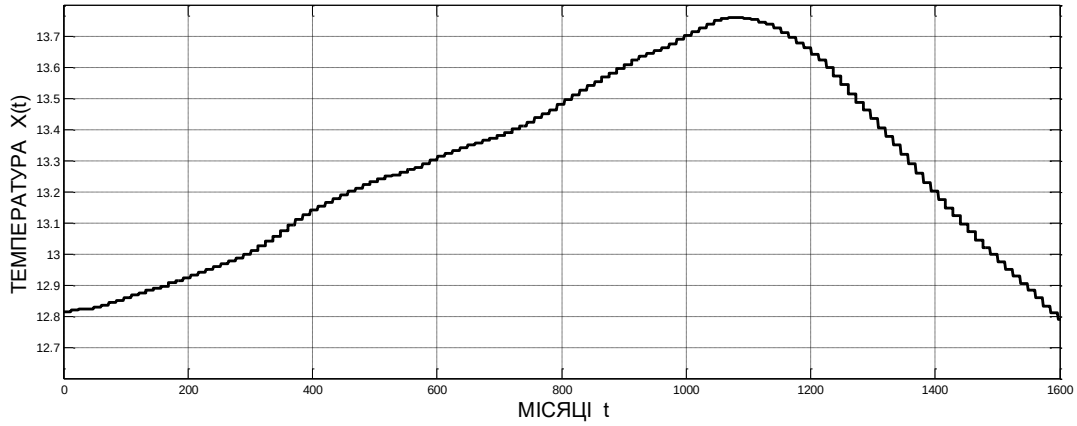


Рис. 8. Тренд температур у м. Сент-Луїс, отриманий ковзним середнім
від зміни середньорічних температур

За даними фахівців, протягом останніх 140 років середньорічна температура Землі підвищилася приблизно на 1°С. У заяві вчених також зазначається, що глобальні середні температури у 2019 р. були на 1,1 °С вищими порівняно з доіндустріальним періодом (1850 – 1900 рр.).

Висновки

Для використовуваних у процесі аналізу даних температури неможливо з використанням моделі АРПКС визначити форму і величину тренду досліджуваного параметра. Для оцінки тренду попередньо було отримано середньорічні значення температур. З отриманих середньорічних значень температури ковзним усередненням отримано тренд процесу.

Як показали результати прикладних досліджень, в деякі інтервали часу тренд температур, що спостерігаються, не зростав, а й знижувався. За даними метеообсерваторії у м. Пулкове з 1804 до 2010 р. спостерігалося загальне зростання. Приріст температури за цей термін становив 2,515 °С. За даними вимірювання температури в місті Сент-Луїс, з 1936 по 1978 р., спостерігалося падіння температури. Падіння температури за цей період становило 0,974 °С.

Запропонована модель може бути використана для дослідження процесів у різних галузях людської діяльності: аналізу траєкторій руху літальних апаратів, що спостерігаються, зокрема безпілотних літальних апаратів, метеорологічних процесів, що відображають стан атмосфери.

Список літератури:

1. Кошкин Р.П. Беспилотные авиационные системы. Москва : Стратегические приоритеты, 2016. 676 с.

2. Макаренко С. И., Тимошенко А. В., Васильченко А. С. Анализ средств и способов противодействия беспилотным летательным аппаратам. Ч. 1. Беспилотный летательный аппарат как объект обнаружения и поражения // Системы управления, связи и безопасности. 2020. № 1. С. 109-146. DOI: 10.24411/2410-9916-2020-10105.

3. Kartashov V.M., Oleynikov V.N, Sheyko S.A., Koryttsev I.V., Babkin S.I., Zubkov O.V. Peculiarities of small unmanned aerial vehicles detection and recognition // Telecommunications and Radio Engineering. 2019. Vol. 78, Issue 9. P. 771-781.

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

5. Тихонов В.А., Карташов В.М., Олейников В.М., Леонидов В.И., Тимошенко Л.П., Селезнев И.С., Рыбников Н.В.. Обнаружение-распознавание беспилотных летательных аппаратов с использованием составной модели авторегрессии их акустического излучения // Вісник НТУУ «КПІ». Радіотехніка. Радіоапаратобудування. Вип. №81, 2020; С. 38–46. DOI: https://doi.org/10.20535/RADAP.2020.81.38-46.

6. Ситнік О.В., Карташов В.М. Радіотехнічні системи : навч. посібник. Харків : Сміт, 2009. 448 с.

7. Омельченко В.А., Безрук В.М., Коваленко Н.П. Распознавание заданных радиосигналов при наличии неизвестных сигналов на авторегрессионной основе // Радиотехника. 2001. № 123. С. 195–199.

8. Дробахин О.О. Автоматизация процесса распознавания сигналов дефектоскопа на основе модели линейного предсказания // Дефектоскопия. 1985. № 10. С. 64–67.
9. Рамишвили Г.С. Автоматическое распознавание говорящего по голосу. Москва : Радио и связь, 1981. 224 с.
10. Калистратова М.А., Кон А.И. Радиоакустическое зондирование атмосферы. Москва : Наука, 1985. 200 с.
11. Карташов В.М., Тихонов В.А., Олейников В.Н. Обработка сигналов в радиоэлектронных системах дистанционного мониторинга атмосферы. Харьков : ХНУРЭ, 2014. 312 с.
12. Марпл.-мл. С. Л. Цифровой спектральный анализ и его приложения. Москва : Мир, 1990. 584 с.
13. Бокс Дж., Дженкинс Г. Анализ временных рядов : пер. с. англ. Москва : Мир, 1974. Вып.1. 406 с.
14. Brockwell P.J., Davis R.A. Introduction to Time Series and Forecasting. Springer, 2002. P. 434.
15. Кармалита В.А. Цифровая обработка случайных колебаний. Москва : Машиностроение, 1986. 80 с.

Надійшла до редколегії 04.06.2022

Відомості про авторів:

Тихонов В'ячеслав Анатолійович – д-р фіз-мат. наук, професор, професор кафедри інформаційно-мережної інженерії; Харківський національний університет радіоелектроніки, Україна; e-mail: vyacheslav.tykhonov@nure.ua; ORCID: https://orcid.org/0000-0002-4618-4787

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

Карташов Олександр Володимирович – здобувач кафедри медіаінженерії та інформаційних радіоелектронних систем; Харківський національний університет радіоелектроніки,Україна; e-mail: mservicekh1@gmail.com

ABSTRACTS РЕФЕРАТИ РЕФЕРАТЫ

METHODS, ALGORITHMS AND TOOLS FOR CRYPTOGRAPHIC PROTECTION OF INFORMATION

МЕТОДИ, АЛГОРИТМИ ТА ЗАСОБИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

МЕТОДЫ, АЛГОРИТМЫ И СРЕДСТВА КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

UDC 004.056.55

Risk estimation methodology in the post-quantum period / *M.V. Yesina, O.V. Potii, Yu.I. Gorbenko, V.A. Ponomar* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2022. №209. P. 7 – 15.

The world is in the process of intensive creation and application of quantum technologies. On May 4, 2022, the President of the United States signed the «National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems». Therefore, advancing leadership is an important challenge in quantum computing in general, while reducing risks to vulnerable cryptographic systems. Accordingly, standardized scientific and methodological support for risk assessment should be justified, accepted and applied at the international and national levels when quantum computing is used in general and especially when quantum computing is used in cryptology. The purpose of the work is to substantiate and develop a risk assessment methodology for quantum computing used in cryptology in the so-called "post-quantum period". With this aim in view the following components were taken into account: the use of methods that have not yet arisen to combat cybersecurity threats; determination of the essence of the quantum risk assessment methodology; identification and documentation of information assets and their current cryptographic protection; research on the state of quantum computers and quantum-safe cryptography. Quantum risk assessment is considered, an ideal approach for identifying and prioritizing threats and vulnerabilities, as well as laying the foundation for the reliable and cost-effective development of systems so that they are resistant to quantum attacks. Quantum risk assessment provides organizations with the knowledge necessary to understand the extent of their quantum cyber risk and the terms in which quantum threats can arise. This will provide the organization with a basis for proactively addressing quantum risks, building a path to a quantum safe state, and implementing and validating quantum safe solutions.

Key words: quantum computer; qubit; methodology; evaluation; risk; post-quantum period.

Ref: 13 items.

УДК 004.056.55

Методологія оцінки ризику в постквантовий період / *М.В. Єсіна, О.В. Потій, Ю.І. Горбенко, В.А. Пономар* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2022. Вип. 209. С. 7 – 15.

У світі відбувається процес інтенсивного створення та застосування квантових технологій. Президент США підписав 4 травня 2022 р. «Меморандум про національну безпеку з просування лідерства в галузі квантових обчислень при одночасному зниженні ризиків для вразливих криптографічних систем, що свідчить про надзвичайну важливість квантових обчислень та їх застосування в криптології». Тому, наразі просування лідерства в галузі квантових обчислень взагалі, при одночасному зниженні ризиків для вразливих криптографічних систем, є важливою проблемою. Відповідно на міжнародному та національному рівнях повинне бути обґрунтовано, прийняте та застосовуватись стандартизоване науково-методичне забезпечення оцінки ризиків взагалі для квантових обчислень та надзвичайно важливим для квантових обчислень при його застосуванні в криптології. Метою цієї роботи є обґрунтування та розробка методології оцінки ризиків для квантових обчислень при його застосуванні в криптології у так званий «постквантовий період» з урахуванням таких складових вирішення цієї проблеми: використання способів боротьби із загрозами кібербезпеці, яка ще не виникла; визначення сутності методології квантової оцінки ризику; ідентифікація та документування інформаційних активів та їх поточний криптографічний захист; дослідження стану квантових комп'ютерів та квантово-безпечної криптографії. Розглядається квантова оцінка ризику – ідеальний підхід для виявлення та визначення пріоритетів загроз і вразливостей, а також закладання основи для надійного та економічно ефективного розвитку систем, щоб вони були стійкими до квантових атак. Квантова оцінка ризику дає організації знання, необхідні для розуміння ступеня їх квантового кіберризику та термінів, за які можуть виникнути квантові загрози. Це забезпечить організацію основою для проактивного вирішення квантових ризиків, побудови шляху до квантово безпечного стану, а також для впровадження та підтвердження квантово-безпечних рішень.

Ключові слова: квантовий комп'ютер; кубіт; методологія; оцінка; ризик; постквантовий період.

Бібліогр.: 13 назв.

УДК 004.056.55

Методология оценки риска в постквантовый период / *М.В. Есина, А.В. Потий, Ю.И. Горбенко, В.А. Пономарь* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2022. Вып. 209. С. 7 – 15.

В мире происходит процесс интенсивного создания и применения квантовых технологий. Президент США подписал 4 мая 2022 г. «Меморандум о национальной безопасности по продвижению лидерства в области кван-

товых вычислений при одновременном снижении рисков для уязвимых криптографических систем, что свидетельствует о чрезвычайной важности квантовых вычислений и их применении в криптологии». Поэтому, продвижение лидерства в области квантовых вычислений вообще, при одновременном снижении рисков для уязвимых криптографических систем, является важной проблемой. Соответственно, на международном и национальном уровнях должно быть обосновано, принято и применяться стандартизированное научно-методическое обеспечение оценки рисков вообще для квантовых вычислений и чрезвычайно важным для квантовых вычислений при его применении в криптологии. Цель работы – обоснование и разработка методологии оценки рисков для квантовых вычислений при его применении в криптологии в так называемый «постквантовый период» с учетом таких составляющих решения этой проблемы: использование еще не возникших способов борьбы с угрозами кибербезопасности; определение сущности методологии квантовой оценки риска; идентификация и документирование информационных активов и их текущая криптографическая защита; исследование состояния квантовых компьютеров и квантово-безопасной криптографии. Рассматривается квантовая оценка риска – идеальный подход для выявления и определения приоритетов угроз и уязвимостей, а также закладки основы для надежного и экономически эффективного развития систем, чтобы они были устойчивы к квантовым атакам. Квантовая оценка риска дает организации знания, необходимые для понимания степени их квантового киберриска и терминов, при которых могут возникнуть квантовые угрозы. Это обеспечит организацию основой для проактивного решения квантовых рисков, построения пути к квантово-безопасному состоянию, а также для внедрения и подтверждения квантово-безопасных решений.

Ключевые слова: квантовый компьютер; кубит; методология; оценка; риск; постквантовый период.

Библиогр.: 13 назв.

UDC 004.056.5

Properties of the cost function in the iterative algorithm for generating nonlinear substitutions / *O.O. Kuznetsov, Yu.I. Горбенко, M.O. Poluyanenko, S.O. Kandiy, E.D. Matveeva* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2022. №209. P. 16 – 28.

To ensure the security of information technology, cryptographic information protection tools are used, in particular block and stream encryption algorithms with a symmetric key. Reliability and cryptographic strength of cryptoalgorithms is provided by the properties of the applied primitives. For example, non-linear substitutions (S-boxes) are used as the main component of modern symmetric ciphers. Therefore, generation of substitutions is an important scientific task directly related to the security of information technology and improvement of modern symmetric ciphers. The paper investigates the properties of iterative algorithms for generating non-linear substitutions and special cost functions, which play a decisive role in the heuristic search for S-boxes with the required properties. We consider the cost function of the WCF (Cost Function of the content of the Walsh-Hadamard spectrum) and optimize its parameters. The obtained optimization results in combination with the Hill Climbing iterative search algorithm can reduce significantly the number of iterations. In particular, we show that for a substitution search with a non-linearity of 104, on average, we reduce the computational complexity of generation by more than 20%. In addition, it is possible to increase the success rate of the heuristic search. In particular, for the selected settings, in 100% of cases, a beaktive S-box with a non-linearity of 104 was found.

Key words: symmetric cryptography; cost function; generation methods; nonlinearity; Walsh – Hadamard transform; S-box.

1 tab. 16 fig. Ref: 24 items.

УДК 004.056.5

Властивості функції вартості в ітеративному алгоритмі генерації нелінійних підстановок / *О.О. Кузнецов, Ю.І. Горбенко, М.О. Полуяненко, С.О. Кандій, Є.Д. Матвєєва* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2022. Вип. 209. С. 16 – 28.

Для забезпечення безпеки інформаційних технологій застосовують засоби криптографічного захисту інформації, зокрема алгоритми блочного та поточного шифрування із симетричним ключем. Надійність та криптографічна стійкість криптоалгоритмів забезпечується властивостями застосованих примітивів. Наприклад, у якості основного компоненту сучасних симетричних шифрів є нелінійні підстановки (S-блоки). Отже генерація підстановок є надзвичайно важливим науковим завданням, безпосередньо пов'язаним із забезпеченням безпеки інформаційних технологій та вдосконаленням сучасних симетричних шифрів. В цій роботі досліджуються властивості ітеративних алгоритмів генерації нелінійних підстановок та спеціальних функцій вартості, які відіграють вирішальну роль в евристичному пошуку S-блоків із необхідними властивостями. Ми розглядаємо функцію вартості WCF (Cost Function of the content of the Walsh-Hadamard spectrum) та оптимізуємо її параметри. Отримані результати оптимізації у поєднанні із ітеративним алгоритмом пошуку Hill Climbing дозволяють значно скоротити кількість ітерацій. Зокрема ми показуємо, що для пошуку підстановки із нелінійністю 104 в середньому ми скорочуємо обчислювальну складність генерації понад на 20 %. Крім того, вдається підвищити частоту успіху евристичного пошуку. Для обраних налаштувань у 100 % випадках було знайдено бієктивний S-блок з нелінійністю 104.

Ключові слова: симетрична криптографія; функція вартості; методи генерації; нелінійність; перетворення Уолша – Адамара; S-блок

Табл. 1. Іл. 16. Бібліогр.: 24 назв.

УДК 004.056.5

Свойства функции стоимости в итеративном алгоритме генерации нелинейных подстановок / *А.А. Кузнецов, Ю.И. Горбенко, Н.А. Полуяненко, С.А. Кандий, Е.Д. Матвеева* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2022. Вып. 209. С. 16 – 28.

Для обеспечения безопасности информационных технологий применяют средства криптографической защиты информации, в частности алгоритмы блочного и поточного шифрования с симметричным ключом. Надежность и криптографическая стойкость криптоалгоритмов обеспечивается свойствами применяемых примитивов. Например, в качестве основного компонента современных симметричных шифров используются нелинейные подстановки (S-блоки). Следовательно, генерация подстановок является важной научной задачей, непосредственно связанной с обеспечением безопасности информационных технологий и совершенствованием современных симметричных шифров. Исследуются свойства итеративных алгоритмов генерации нелинейных подстановок и специальных функций стоимости, играющих решающую роль в эвристическом поиске S-блоков с необходимыми свойствами. Мы рассматриваем функцию стоимости WCF (Cost Function of the content of the Walsh-Hadamard spectrum) и оптимизируем ее параметры. Полученные результаты оптимизации в сочетании с итеративным алгоритмом поиска Hill Climbing позволяют значительно сократить количество итераций. В частности, мы показываем, что для поиска подстановки с нелинейностью 104 в среднем мы сокращаем вычислительную сложность генерации более чем на 20 %. Кроме того, удается повысить частоту успеха эвристического поиска. Для выбранных настроек в 100 % случаях был найден биективный S-блок с нелинейностью 104.

Ключевые слова: симметричная криптография; функция стоимости; методы генерации; нелинейность; преобразование Уолша – Адамара; S-блок.

Табл. 1. Ил. 16. Библиогр.: 24 назв.

UDC 004.056.5

Comparison of the quality of sampling algorithms from discrete normal distribution on NTRU lattices / *I.D. Gorbenko, C.O. Kandiy, Ye.V. Ostrianska* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2022. №209. P. 29 – 37.

Post-quantum cryptography is a field of research that studies cryptographic transformations protected against attacks using quantum computers. For many years, lattice-based cryptography has become one of the most promising solutions to protect against the threat of quantum computing. An important feature of the post-quantum period in cryptography is the significant uncertainty about the source data for cryptanalysis and countermeasures in the capabilities of quantum computers, their mathematical support and software, as well as the application of quantum cryptanalysis to existing cryptocurrencies and cryptoprotocol. The main methods are mathematical methods of electronic signature, which have undergone significant analysis and justification in the process of extensive research by cryptologists and mathematicians at the highest level. The security of signature schemes depends strongly on the standard deviation of the discrete Gaussian distribution, which has a sampling algorithm. In this paper, the most common variants of sampling algorithms were considered and analyzed, because the quality of all algorithms depends significantly on the structure of the lattice for which sampling takes place. A comparison of the quality of lattice sampling algorithms is highlighted. In particular, the paper considers Klein's algorithms (its modification is the Thomas Prest and Dukas algorithm), Peikert's algorithm and the floating-point sampling algorithm. Klein's sampling algorithm, in particular its modification, namely, the Dukas-Prest algorithm, gives the smallest vectors. Theoretically, it is much better than Klein's algorithm on NTRU lattices, but it requires the use of floating-point arithmetic, which complicates greatly the analysis of its security and tocreation of software or hardware implementation.

Key words: electronic signature; post-quantum cryptography; sampling algorithm; NTRU lattice.

1 tab. 5 fig. Ref: 15 items.

УДК 004.056.5

Порівняння якості алгоритмів семплування з дискретного нормального розподілу на NTRU решітках / *І.Д. Горбенко, С.О. Кандій, Є.В. Острянська* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2022. Вип. 209. С. 29 – 37.

Постквантова криптографія є напрямом досліджень, що вивчає криптографічні перетворення, які захищені від атак з використанням квантових комп'ютерів. Протягом багатьох років криптографія на основі решіток стала одним з найбільш перспективних рішень для захисту від загрози квантових обчислень. Важливою особливістю постквантового періоду у криптографії є суттєва невизначеність щодо вихідних даних для криптоаналізу та протидії в частині можливостей квантових комп'ютерів, їх математичного та програмного забезпечення, а також застосування квантового криптоаналізу до існуючих криптоперетворень та криптопротоколів. В якості основних методів обрано математичні методи електронного підпису, що пройшли суттєвий аналіз та обґрунтування в процесі широких досліджень криптологами та математиками на найвищому рівні. Безпека схем підпису сильно залежить від стандартного відхилення дискретного гаусівського розподілу, який має алгоритм семплування. В роботі розглянуто та проаналізовано найбільш розповсюджені варіанти алгоритмів семплування, адже якість всіх алгоритмів значно залежить від структури решітки, для якої відбувається семплування. Висвітлено порівняння якості алгоритмів семплування на решітках. Зокрема, розглянуто алгоритми Клейна (його модифікацію – алгоритм Преста та Дукаса), алгоритм Пейкерта та алгоритм семплування без використання арифмети-

ки з плаваючою крапкою. Алгоритм семплування Клейна, зокрема його модифікація – алгоритм Дукаса – Преста, дає найменші вектори. З теоретичної точки зору він набагато кращий за алгоритм Клейна на NTRU решітках, проте він вимагає використання арифметики з плаваючою крапкою, що значно ускладнює аналіз його безпеки та створення програмної чи апаратної реалізації.

Ключові слова: електронний підпис; постквантова криптографія; алгоритм семплування; NTRU решітки.

Табл. 1. Іл. 5. Бібліогр.: 15 назв.

УДК 004.056.5

Сравнение качества алгоритмов сэмплирования с дискретного нормального распределения на NTRU решетках / *И.Д. Горбенко, С.О. Кандий, Е.В. Острянская* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2022. Вып. 209. С. 29 – 37.

Постквантовая криптография – направление исследований, изучающее криптографические преобразования, защищенные от атак с использованием квантовых компьютеров. В течение многих лет криптография на основе решеток стала одним из наиболее перспективных решений для защиты от угрозы квантовых вычислений. Важной особенностью постквантового периода в криптографии является существенная неопределенность относительно исходных данных для криптоанализа и противодействия части возможностей квантовых компьютеров, их математического и программного обеспечения, а также применение квантового криптоанализа к существующим криптопреобразованиям и криптопротоколам. В качестве основных методов выбраны математические методы электронной подписи, прошедшие существенный анализ и обоснование в процессе широких исследований криптологами и математиками на самом высоком уровне. Безопасность схем подписи сильно зависит от стандартного отклонения дискретного гаусовского распределения, имеющего алгоритм сэмплирования. В работе рассмотрены и проанализированы наиболее распространенные варианты алгоритмов сэмплирования, ведь качество всех алгоритмов значительно зависит от структуры решетки, для которой происходит сэмплирование. Отражено сравнение качества алгоритмов сэмплирования на решетках. В частности, рассмотрены алгоритмы Клейна (его модификация – алгоритм Преста и Дукаса), алгоритм Пейкерта и алгоритм сэмплирования без использования арифметики с плавающей точкой. Алгоритм сэмплирования Клейна, в частности его модификация – алгоритм Дукаса – Преста, дает самые маленькие векторы. С теоретической точки зрения он гораздо лучше алгоритма Клейна на NTRU решетках, однако требует использования арифметики с плавающей точкой, что значительно усложняет анализ его безопасности и создание программной или аппаратной реализации.

Ключевые слова: электронная подпись; постквантовая криптография; алгоритм сэмплирования; NTRU решетки.

Табл. 1. Ил. 5. Библиогр.: 15 назв.

UDC 004.056.5

Factorial number system for nonlinear substitutions generation / *Ya.A. Derevianko, Yu.I. Gorbenko, O.O. Kuznetsov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2022. №209. P. 38 – 58.

Modern cryptographic applications use cryptographic algorithms with a symmetric key. They provide high conversion rates and resistance to crypto-graphic attacks. To complicate the plaintext – cipher-text ratio, symmetric ciphers usually use nonlinear substitutions (S-boxes). S-boxes cryptographic metrics play a crucial role in ensuring resilience to most known attacks (differential, linear, algebraic, and other cryptanalysis methods). However, generating efficient s-boxes is a challenge. Even for small input/output sizes, there are an extremely large number of possible solutions. Usually, the substitution is represented as a set of Boolean functions. This allows you to apply discrete transformations, for example, Walsh-Hadamard, to evaluate cryptographic indicators. However, methods for generating s-boxes by selecting suitable Boolean functions are extremely complex. Therefore, it is necessary to study new mathematical methods for representing nonlinear substitutions, studying their cryptographic properties, and developing generation algorithms. In this paper, we propose applying factorial number systems to represent nonlinear substitutions. Each substitution can be represented in a unique way through a set of inversions, which, in turn, can be transformed into a factorial number. That is, we can naturally arrange all substitutions by numbering them in the factorial number system. We give examples of such numbering and investigate the cryptographic characteristics of S-boxes with their initial numbers. In particular, we show how the variable functions used in heuristic algorithms for generating non-linear substitutions change. The results obtained can be used to simplify heuristic methods in order to speed up the generation of non-linear substitutions.

Key words: substitution; factorial number system; S-box; cryptographic indicators; cost functions; heuristic search methods.

10 tab. 11 fig. Ref: 6 items.

УДК 004.056.5

Факторіальна система числення для генерації нелінійних підстановок / *Я.А. Дерев'янко, Ю.І. Горбенко, О.О. Кузнецов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2022. Вип. 209. С. 38 – 58.

В сучасних криптографічних застосунках використовують криптографічні алгоритми із симетричним ключем. Вони забезпечують високу швидкість перетворення та стійкість до криптографічних атак. Для ускладнення співвідношення відкритий текст – шифр-текст в симетричних шифрах зазвичай застосовують нелінійні підстановки (S-boxes). Криптографічні показники S-boxes відіграють вирішальну роль у забезпеченні стійкості проти більшості відомих атак (диференційного, лінійного, алгебраїчного та інших методів криптоаналізу).

Однак генерація ефективних S-boxes є складною задачею. Навіть для невеликих розмірів входу-виходу існує надзвичайно велика кількість можливих рішень. Зазвичай підстановку подають у вигляді сукупності булевих функцій. Це дозволяє застосувати дискретні перетворення, наприклад, Уолша – Адамара, для оцінки криптографічних показників. Однак методи генерації S-boxes через підбір підходящих булевих функцій є надзвичайно складними. Отже необхідно досліджувати нові математичні методи для подання нелінійних підстановок, вивчення їх криптографічних властивостей та розробки алгоритмів генерації. В роботі ми пропонуємо застосовувати факторіальні системи числення для подання нелінійних підстановок. Кожна підстановка унікальним чином може бути подана через множину інверсій, яка, у свою чергу, може бути трансформована у факторіальне число. Тобто ми маємо можливість природнім чином впорядкувати всі підстановки через їх нумерацію у факторіальній системі числення. Ми наводимо приклади такої нумерації та досліджуємо криптографічні показники S-boxes із сусідніми номерами. Зокрема, ми показуємо, як змінюються функції вартості, що використовуються в евристичних алгоритмах генерації нелінійних підстановок. Отримані результати можна застосовувати для удосконалення евристичних методів з метою прискорення генерації нелінійних підстановок.

Ключові слова: підстановка; факторіальна система числення; S-box; криптографічні показники; функції вартості; евристичні методи пошуку.

Табл. 10. Іл. 11. Бібліогр.: 6 назв.

УДК 004.056.5

Факториальная система счисления для генерации нелинейных подстановок / *Я.А. Деревянко, Ю.И. Горбенко, А.А. Кузнецов* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2022. Вып. 209. С. 38 – 58.

В современных криптографических приложениях используются криптографические алгоритмы с симметричным ключом. Они обеспечивают высокую скорость преобразования и устойчивость к криптографическим атакам. Для усложнения соотношения открытый текст – шифр-текст в симметричных шифрах обычно применяют нелинейные подстановки (S-boxes). Криптографические показатели S-boxes играют решающую роль в обеспечении устойчивости против большинства известных атак (дифференциального, линейного, алгебраического и других методов криптоанализа). Однако генерация эффективных S-boxes является сложной задачей. Даже для небольших размеров входа-выхода существует очень большое количество возможных решений. Обычно подстановку подают в виде совокупности булевых функций. Это позволяет применить дискретные преобразования, например, Уолша – Адамара, для оценки криптографических показателей. Однако методы генерации S-boxes путём подбора подходящих булевых функций чрезвычайно сложны. Таким образом, необходимо исследовать новые математические методы для представления нелинейных подстановок, изучения их криптографических свойств и разработки алгоритмов генерации. В данной работе мы предлагаем использовать факториальные системы счисления для представления нелинейных подстановок. Каждая подстановка уникальным образом может быть представлена через множество инверсий, которое, в свою очередь, может быть трансформировано в факторное число. То есть мы имеем возможность естественным образом упорядочить все подстановки путём их нумерации в факториальной системе счисления. Мы приводим примеры такой нумерации и исследуем криптографические показатели S-boxes с соседними номерами. В частности, мы показываем, как изменяются функции стоимости, используемые в эвристических алгоритмах генерации нелинейных подстановок. Полученные результаты можно применять для усовершенствования эвристических методов с целью ускорения генерации нелинейных подстановок.

Ключевые слова: подстановка; факториальная система счисления; S-box; криптографические показатели; функции стоимости; эвристические методы поиска.

Табл. 10. Ил. 11. Библиогр.: 6 назв.

UDC 003.026:004.056

RAINBOW algorithm and its ability to resist RBS attacks and third party channels / *D.V. Harmash* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2022. №209. P. 59 – 63.

The essence and possibilities of protecting the Rainbow post-quantum cryptographic algorithm are considered. The main properties of algorithms based on multidimensional quadratic transformations are studied. An assessment is given of what resources and computational energy are needed for the successful use of algorithms based on multidimensional quadratic transformations. The ability to protect the algorithm against attacks by third-party channels is analyzed. It is studied how successfully a cryptographic algorithm based on Rainbow multivariate quadratic transformations can withstand RBS attacks. A detailed description of the steps used to build an attack on a cryptographic algorithm based on Rainbow multivariate quadratic transforms is given. A structural analysis of the Rainbow algorithm is performed. Detailed conclusions are made regarding the performed analyzes. An assessment of the stability and complexity of the cryptographic encryption algorithm and electronic signature based on multivariate quadratic transformations is given.

Key words: Rainbow; cryptanalysis; vulnerability; minrank; scheme; algorithm.

Ref: 8 items.

УДК 003.026:004.056

Алгоритм RAINBOW та його здатність протидіяти атакам RBS та сторонніми каналами / *Д.В. Гармаш* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2022. Вип. 209. С. 59 – 63.

Розглядається сутність та можливістьзахисту постквантового криптографічного алгоритму Rainbow. Розглядаються основні властивості алгоритмів на основі багатовимірних квадратичних перетворень. Дається оцінка того, які ресурси та обчислювальна енергія необхідна для вдалого використання алгоритмів на основі багатовимірніх квадратичніх перетворень. Наведено аналізи стосовно здатності захисту алгоритму від атаки сторонніми каналами. Проаналізоано, з яким успіхом криптографічний алгоритм на основі мультиваріативних квадратичних перетворень Rainbow може вистояти проти RBS атаки. Наведено детальний опис кроків, з яких побудована атака на криптографічний алгоритм на основі мультиваріативних квадратичних перетворень Rainbow. Проведено структурний аналіз алгоритму Rainbow. Надано детальні висновки стосовно виконаних аналізів.

Наведено оцінку стійкості та складності криптографічного алгоритму шифрування та електронного підпису на основі мультиваріативних квадратичних перетворень.

Ключові слова: Rainbow; криптоаналіз; вразливість; мінранк; схема; алгоритм.

Бібліогр.: 8 назв.

УДК 003.026:004.056

Алгоритм RAINBOW и его способность противодействовать атакам RBS и сторонними каналами / *Д.В. Гармаш* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2022. Вып. 209. С. 59 – 63.

Рассматривается сущность и возможности защиты постквантового криптографического алгоритма Rainbow. Рассматриваются главные характеристики алгоритмов на базе многомерных квадратических преобразований. Дается оценка того, какие ресурсы и вычислительная энергия необходима для удачного использования алгоритмов на основе многомерных квадратических преобразований. Проанализирована способность защиты алгоритма от атаки посторонними каналами. Проанализировано насколько успешно криптографический алгоритм на основе мультивариативных квадратических преобразований Rainbow может выстоять против RBS атаки. Приведено подробное описание шагов, из которых построена атака на криптографический алгоритм на основе мультивариативных квадратических преобразований Rainbow. Проведен структурный анализ алгоритма Rainbow. Представлены подробные выводы по выполненным анализам. Дана оценка устойчивости и сложности криптографического алгоритма шифрования и электронной подписи на основе мультивариативных квадратических преобразований.

Ключевые слова: Rainbow; криптоанализ; уязвимость; минранк; схема; алгоритм.

Библиогр.: 8 назв.

UDC 003.026:004.056

Analysis of partial key recovery attack on multivariate cryptographic transformations using rank systems / *G. Maleeva* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2022. №209. P. 64 – 70.

The Rainbow signature scheme, proposed by Ding and Schmidt in 2005, is one of the oldest and most studied signature schemes in multidimensional cryptography. The Rainbow, based on the unbalanced Oil and Vinegar signature scheme, has the necessary cryptocurrency since 1999 with the right parameters. Interest in multivariate cryptography has increased in the last decade, as it is considered to be quantum-stable.

Cryptanalysis of the Rainbow and its predecessors was actively developed in the early 2000s. Attacks from this era include the MinRank attack, the HighRank attack, the Bill-Gilbert attack, the UOV agreement attack, and the Rainbow bandwidth attack. After 2008, cryptanalysis seemed to have stopped, until the Rainbow's participation in the NIST PQC project, which motivated the continuation of cryptanalysis. During the second round of NIST, Bardett and others proposed a new algorithm for solving the MinRank problem. This dramatically increased the effectiveness of MinRank's attack, although not enough to threaten the parameters provided to NIST. A less memory-intensive version of this algorithm was suggested by Baena et al. Perlner and Smith-Tone analyzed the Rainbow bandwidth attack in depth, which showed that the attack was more effective than previously thought. This prompted the Rainbow team to increase slightly the parameters for the third round. During the third round, Bellens introduced a new attack that reduced the Rainbow's security by 2^{20} times for SL 1. The Rainbow team claimed that despite the new attacks, the Rainbow's parameters still met NIST requirement.

The purpose of this article is to present two new (partial) key recovery attacks on multivariate cryptographic transformations using rank systems.

Key words: cryptosecurity; cryptanalysis; rank experiments; attack analysis; postquantum period.

4 tab. Ref: 17 items.

УДК 003.026:004.056

Аналіз атаки часткового відновлення ключа на мультиваріативні криптографічні перетворення з використанням рангових систем / *Г.А. Малєєва* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2022. Вип. 209. С. 64 – 70.

Схема підпису Rainbow, запропонована Дінгом і Шмідтом у 2005 році, є однією з найстаріших і найбільш вивчених схем підпису в багатовимірній криптографії. Rainbow заснована на схемі підпису (unbalanced) Oil and Vinegar, яка за правильно обраних параметрів мала необхідну криптостійкість починаючи з 1999 року. В остан-

нє десятиліття збільшився інтерес до багатоваріантної криптографії, оскільки вважається, що вона є квантово-стійкою.

Криптоаналіз Rainbow та його попередників активно розвивався на початку 2000-х років. Атаки з цієї епохи включають атаку MinRank, атаку HighRank, атаку Білле – Гілберта, атака погодження UOV та атака розподілу смуги Rainbow. Після 2008 року криптоаналіз, здавалося, припинився, аж до участі Rainbow у проєкті NIST PQC, що стало мотиватором до продовження криптоаналізу. Під час другого раунду NIST, Бардет та інші запропонували новий алгоритм для розв'язування задачі MinRank. Це різко підвищило ефективність атаки MinRank хоча й недостатньо, щоб загрожувати параметрам, поданим до NIST. Менш витратну, з точки зору пам'яті, версію цього алгоритму запропонувала Баена та інш. Перлнер і Сміт-Тон глибше проаналізували атаку розподілення смуги Rainbow, що показала, що атака була ефективнішою, ніж до цього вважалося. Це спонукало команду Rainbow дещо збільшити параметри для третього туру. Під час третього раунду Белленс представив нову атаку, яка знизила рівень безпеки Rainbow у 2^{20} разів для параметрів SL 1. Команда Rainbow стверджувала, що, незважаючи на нові атаки, параметри Rainbow все ще відповідають вимогам NIST.

Мета статті – представити дві нові атаки (часткового) відновлення ключа на мультиваріативні криптографічні перетворення з використанням рангових систем.

Ключові слова: криптостійкість; криптоаналіз; рангові експерименти; аналіз атак; постквантовий період.

Табл. 4. Бібліогр.: 17 назв.

УДК 003.026:004.056

Анализ атаки частичного восстановления ключа на мультивариативные криптографические преобразования с использованием ранговых систем / *А.А. Малеева* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2022. Вып. 209. С. 64 – 70.

Схема подписи Rainbow, предложенная Дингом и Шмидтом в 2005 году, является одной из старейших и изученных схем подписи в многомерной криптографии. Rainbow основана на схеме подписи (unbalanced) Oil and Vinegar, которая при правильно выбранных параметрах обладала необходимой криптостойкостью начиная с 1999 года. В последнее десятилетие увеличился интерес к многовариантной криптографии, поскольку считается, что она квантово устойчива.

Криптоанализ Rainbow и его предшественников активно развивался в начале 2000-х годов. Атаки из этой эпохи включают атаку MinRank, атаку HighRank, атаку Билле – Гилберта, атаку согласования UOV и атаку распределения полосы Rainbow. После 2008 года криптоанализ, казалось, прекратился, вплоть до участия Rainbow в проекте NIST PQC, что послужило мотиватором для продолжения криптоанализа. Во время второго раунда NIST, Бардет и другие предложили новый алгоритм для решения задачи MinRank. Это резко повысило эффективность атаки MinRank хотя и недостаточно, чтобы угрожать параметрам, представленным в NIST. Менее затратную, с точки зрения памяти, версию этого алгоритма предложила Баэна и т.д. Перлнер и Смит – Тон глубже проанализировали атаку распределения полосы Rainbow, что показало, что атака была более эффективной, чем до этого считалось. Это подвигло команду Rainbow несколько увеличить параметры для третьего тура. Во время третьего раунда Белленс представил новую атаку, снизившую уровень безопасности Rainbow в 2^{20} раз для параметров SL 1. Команда Rainbow утверждала, что, несмотря на новые атаки, параметры Rainbow все еще отвечают требованиям NIST.

Цель статьи – представить две новые атаки (частичного) восстановления ключа на мультивариативные криптографические преобразования с использованием ранговых систем.

Ключевые слова: криптостойкость; криптоанализ; ранговые эксперименты; анализ атак; постквантовый период.

Табл. 4. Библиогр.: 17 назв.

UDC 004.056.5

Study of a new cost function for generating random substitutions of symmetric ciphers / *O.O. Kuznetsov, , M.O. Poluyanenko, S.O. Kandiy, O.I. Peliukh* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2022. №209. P. 71 – 82.

Cryptographic transformations with a secret key play an essential role in providing information and cyber security. Block and stream symmetric ciphers are used in various applications both as a separate cryptographic protection mechanism and as part of other applications (pseudo-random sequence generators, hashing algorithms, electronic signature protocols, etc.). Therefore, the design and study of individual components of symmetric ciphers is a relevant and important scientific task. In this paper we consider and investigates iterative algorithms for generating non-linear substitutions (substitutions, S-boxes), which are used in modern block and stream encryption algorithms with a symmetric key. Cryptographic resistance of symmetric ciphers to statistical, differential, linear and other methods of cryptanalysis is provided by the properties of substitutions. In addition, S-boxes must be random from the point of view of the possibility to use algebraic cryptanalysis. Therefore, the task of quickly generating random S-boxes with the desired cryptographic properties is an urgent, but extremely difficult task. For example, the best known generation algorithm requires more than 65 thousand iterations to find a random bijective 8-bit substitution with a non-linearity of 104. In this paper, we study an iterative algorithm for generating substitutions for hill climbing with different cost functions and propose a

new cost function, the use of which can significantly reduce the number of search iterations. In particular, the search for a bijective S-box with nonlinearity 104 requires less than 50 thousand iterations.

Key words: symmetric cryptography; cost function; generation methods; nonlinearity; Walsh – Hadamard transform; S-box.

6 tab. 4 fig. Ref: 31 items.

УДК 004.056.5

Дослідження нової функції вартості для генерації випадкових підстановок симетричних шифрів / *О.О. Кузнецов, М.О. Полуяненко, С.О. Кандій, О.І. Пелюх* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2022. Вип. 209. С. 71 – 82.

Криптографічні перетворення із секретним ключем відграють суттєву роль у забезпеченні інформаційної та кібербезпеки. Блокові та потокові симетричні шифри застосовуються в різних додатках як окремий механізм криптографічного захисту, так і у складі інших додатків (генератори псевдовипадкових послідовностей, алгоритми гешування, протоколи електронного підпису і т.д.). Отже проєктування та дослідження окремих компонентів симетричних шифрів є актуальною та важливою науковою задачею. В роботі розглядаються та досліджуються ітеративні алгоритми генерації нелінійних підстановок (substitutions, S-boxes), які застосовуються в сучасних алгоритмах блокового та потокового шифрування із симетричним ключем. Криптографічна стійкість симетричних шифрів до статистичного, диференціального, лінійного та інших методів криптоаналізу забезпечується властивостями підстановок. Крім того, з погляду на можливість застосування алгебраїчного криптоаналізу, S-boxes повинні бути також випадковими. Отже швидка генерація випадкових S-boxes із потрібними криптографічними властивостями є актуальним але надзвичайно складним завданням. Наприклад, найкращий відомий алгоритм генерації потребує понад 65 тисяч ітерацій для пошуку випадкової бієктивної 8-бітної підстановки із нелінійністю 104. В роботі досліджується ітеративний алгоритм генерації підстановок сходження на пагорб (Hill climbing) із різними функціями вартості та пропонується нова функція вартості, застосування якої дозволяє значно скоротити кількість ітерацій пошуку. Зокрема для пошуку бієктивного S-box із нелінійністю 104 необхідно менше 50 тисяч ітерацій.

Ключові слова: симетрична криптографія; функція вартості; методи генерації; нелінійність; перетворення Уолша – Адамара; S-блок.

Табл. 6. Іл. 4. Бібліогр.: 31 назв.

УДК 004.056.5

Исследование новой функции стоимости для генерации случайных подстановок симметричных шифров / *А.А. Кузнецов, Н.А. Полуяненко, С.А. Кандий, А.И. Пелюх* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2022. Вып. 209. С. 71 – 82.

Криптографические преобразования с секретным ключом играют существенную роль в обеспечении информационной и кибербезопасности. Блочные и поточные симметричные шифры применяются в различных приложениях как отдельный механизм криптографической защиты, так и в составе других приложений (генераторы псевдослучайных последовательностей, алгоритмы хеширования, протоколы электронной подписи и т.д.). Следовательно, проектирование и исследование отдельных компонентов симметричных шифров является актуальной и важной научной задачей. В работе рассматриваются и исследуются итеративные алгоритмы генерации нелинейных подстановок (substitutions, S-boxes), которые применяются в современных алгоритмах блочного и потокового шифрования с симметричным ключом. Криптографическая устойчивость симметричных шифров к статистическому, дифференциальному, линейному и другим методам криптоанализа обеспечивается свойствами подстановок. Кроме того, с точки зрения возможности применения алгебраического криптоанализа, S-boxes должны быть случайными. Следовательно, быстрая генерация случайных S-boxes с нужными криптографическими свойствами является актуальной, но чрезвычайно сложной задачей. Например, наилучший известный алгоритм генерации требует более 65 тысяч итераций для поиска случайной биективной 8-битной подстановки с нелинейностью 104. В работе исследуется итеративный алгоритм генерации подстановок восхождения на холм (Hill climbing) с разными функциями стоимости и предлагается новая функция стоимости, применение которой позволяет значительно сократить количество итераций поиска. В частности, для поиска биективного S-box с нелинейностью 104 необходимо менее 50 тысяч итераций.

Ключевые слова: симметричная криптография; функция стоимости; методы генерации; нелинейность; преобразование Уолша – Адамара; S-блок.

Табл. 6. Ил. 4. Библиогр.: 31 назв.

UDC 004.056.55

Analysis of methods and algorithms for generating key data for FALCON-like electronic signature algorithms / *O.G. Kachko, M.V. Yesina, K.O. Kuznetsova* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2022. №209. P. 83 – 86.

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 being 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. This work is devoted to the analysis of methods and algorithms for generating key data for Falcon-like algorithms of electronic signature. Some of the basic algorithms for Falcon-shaped algorithms of electronic signature are considered, namely the algorithm of key data generation and algorithm of random polynomials *f, g* generation, which satisfy the Gauss distribution. The Falcon algorithm itself is the finalist of the post-quantum electronic signature contest due to the satisfactory value of the public key and signature lengths, but the key data generation algorithm uses many methods and difficult to implement. The Falcon authors use this algorithm for polynomials n=512, 1024. To increase the sixth level of cryptostability, this algorithm can be expanded for n=2048. This work is devoted to study the Falcon algorithm, taking into account its expansion for n=512, 1024, 2048 in terms of generating key data. Also, the paper considers the results of justifying the choice of a mathematical apparatus for implementing a software package for generating a key pair of a cryptographic algorithm for an electronic signature in order to create reliable electronic signatures.

Key words: post-quantum cryptography; electronic signature algorithm; lattice theory; Falcon algorithm; key pair generation.

3 tab. Ref: 3 items.

УДК 004.056.55

Аналіз методів та алгоритмів генерації ключових даних для FALCON подібних алгоритмів електронного підпису / *О.Г. Качко, М.В. Єсіна, К.О. Кузнецова* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2022. Вип. 209. С. 83 – 86.

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 в 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. Роботу присвячено аналізу методів та алгоритмів генерації ключових даних для Falcon-подібних алгоритмів електронного підпису. Розглядаються одні з основних алгоритмів Falcon-подібних алгоритмів електронного підпису, а саме алгоритм генерації ключових даних та алгоритм генерація випадкових поліномів *f, g*, які задовольняють розподілу Гауса. Сам алгоритм Falcon є фіналістом конкурсу постквантових алгоритмів електронного підпису завдяки задовільному значенню суми довжин відкритого ключа та підпису, але алгоритм генерації ключових даних застосовує багато методів та важкий для реалізації. Автори Falcon застосовують цей алгоритм для поліномів розміром n=512, 1024. Для збільшення шостого рівня криптостійкості цей алгоритм може бути розширено для n=2048. Саме дослідженню алгоритму Falcon з урахуванням його розширення для n=512, 1024, 2048 в частині генерації ключових даних присвячена ця робота. Також розглянуто результати обґрунтування вибору математичного апарату для впровадження програмного комплексу з генерації ключової пари криптографічного алгоритму електронного підпису з метою створення надійних електронних підписів.

Ключові слова: постквантова криптографія; алгоритм електронного підпису; теорія решіток; алгоритм Falcon; генерація ключової пари.

Табл. 3. Бібліогр.: 3 назв.

УДК 004.056.55

Анализ методов и алгоритмов генерации ключевых данных для FALCON подобных алгоритмов электронной подписи / *Е.Г. Качко, М.В. Есина, Е.А. Кузнецова* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2022. Вып. 209. С. 83 – 86.

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. Работа посвящена анализу методов и алгоритмов для генерации ключевых данных для Falcon-подобных алгоритмов. Рассматриваются одни из основных алгоритмов Falcon-подобных алгоритмов, а именно алгоритм генерации ключевых данных и алгоритм генерации случайных полиномов *f, g*, которые удовлетворяют распределению Гауса. Сам алгоритм Falcon является финалистом конкурса постквантовых электронных подписей из-за удовлетворительного значения суммы открытого ключа и длины подписи, но алгоритм генерации ключевых данных использует много методов и его трудно реализовать. Авторы Falcon используют этот алгоритм для полиномов n=512, 1024. Чтобы увеличить шестой уровень криптостойкости, этот алгоритм может быть расши-

рен для *n*=2048. Именно изучению алгоритма Falcon с учетом его расширения для *n*=512, 1024, 2048, с точки зрения генерации ключевых данных, посвящена эта работа. Также рассмотрены результаты обоснования выбора математического аппарата для внедрения программного комплекса по генерации ключевой пары криптографического алгоритма электронной подписи с целью создания надежных электронных подписей.

Ключевые слова: постквантовая криптография; алгоритм электронной подписи; теория решеток; алгоритм Falcon; генерация ключевой пары.

Табл. 3. Библиогр.: 3 назв.

UDC 003.026:004.056

Analysis of the RAINBOW post-quantum electronic signature algorithm state and attacks on it for the period of the NIST PQC third round completion / Ye.*Yu. Kaptiol* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2022. №209. P. 87– 92.

The paper identifies and analyzes attacks aimed at cryptanalysis of the Rainbow post-quantum electronic signature algorithm and the state of this electronic signature within the framework of the NIST PQC competition and as a whole. The Rainbow electronic signature as a candidate in the third round of the NIST PQC was examined in detail for the possibility of cryptanalysis. The possibility to use this quantitative attack on the Rainbow electronic signature and the complexity of such an attack depends on the possibility to use this electronic signature in the post-quantum period. Also during the NIST PQC report on the peculiarities of the adoption of the first post-quantum standards, which took place on March 8-11, 2022, some concerns about the Rainbow's security were mentioned due to the implementation of an attack on one of the parameter sets (although the parameter set of the second round). Some details of this attack were discussed in the paper to understand better the state of the Rainbow's electronic signature at the end of the third round of the NIST PQC.

Key words: electronic signature; cryptographic stability; cryptanalysis; quantum cryptanalysis.

7 tab. Ref: 11 items.

УДК 003.026:004.056

Аналіз стану постквантового алгоритму електронного підпису RAINBOW та атак на нього на період завершення третього раунду NIST PQC / *Є.Ю. Каптьол* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2022. Вип. 209. С. 87– 92.

Визначаються та аналізуються атаки, спрямовані на здійснення криптоаналізу постквантового алгоритму електронного підпису Rainbow та стан цього електронного підпису в рамках конкурсу NIST PQC та в цілому. Як кандидат в третьому раунді NIST PQC електронний підпис Rainbow було детально досліджено на предмет можливості здійснення криптоаналізу. Від наявності можливості реалізації квантової атаки стосовно електронного підпису Rainbow та складності здійснення такої атаки залежить можливість використання цього електронного підпису в постквантовий період. Також в ході доповіді в рамках NIST PQC щодо особливостей прийняття перших постквантових стандартів, що відбулася 8 – 11 березня 2022 р., було згадано про деяке занепокоєння щодо безпеки Rainbow з огляду на реалізацію атаки на один з наборів параметрів (хоча й набір параметрів версії другого раунду). Деякі деталі цієї атаки розглянуто в роботі для кращого розуміння стану електронного підпису Rainbow на час завершення третього раунду NIST PQC.

Ключові слова: електронний підпис; криптографічна стійкість; криптоаналіз; квантовий криптоаналіз.

Табл. 7. Бібліогр.: 11 назв.

УДК 003.026:004.056

Анализ состояния постквантового алгоритма электронной подписи RAINBOW и атак на него на период завершения третьего раунда NIST PQC / *Е.Ю. Каптел* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2022. Вып. 209. С. 87– 92.

Определяются и анализируются атаки, направленные на проведение криптоанализа постквантового алгоритма электронной подписи Rainbow и состояние этой электронной подписи в рамках конкурса NIST PQC и в целом. Как кандидат в третьем раунде NIST PQC электронная подпись Rainbow была подробно исследована на предмет возможности осуществления криптоанализа. От возможности реализации квантовой атаки относительно электронной подписи Rainbow и сложности осуществления такой атаки зависит возможность использования этой электронной подписи в постквантовый период. Также в ходе доклада в рамках NIST PQC относительно особенностей принятия первых постквантовых стандартов, состоявшегося 8 – 11 марта 2022 г., было упомянуто о некотором беспокойстве по поводу безопасности Rainbow с учетом реализации атаки на один из наборов параметров (хотя и набор параметров версии второго раунда). Некоторые детали этой атаки были рассмотрены в работе для лучшего понимания состояния электронной подписи Rainbow на завершение третьего раунда NIST PQC.

Ключевые слова: электронная подпись; криптографическая стойкость; криптоанализ; квантовый криптоанализ.

Табл. 7. Библиогр.: 11 назв.

UDC 004.056.5

Substantiation of the parameters of the annealing simulation algorithm for searching non-linear substitutions of symmetric ciphers / *O.O. Kuznetsov, M.O. Poluyanenko, S.O. Kandiy, Y.O. Lohachova* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2022. №209. P. 93 – 109.

Cryptographic protection in information and information and communication systems is an important component of cybersecurity. Therefore, the development, research and improvement of means of cryptographic information protection is an urgent and important task. In this paper, we study evolutionary methods for generating non-linear substitutions (S-boxes). These are cryptographic primitives that are an important component of many modern block and stream ciphers with a secret key. However, the problem of generating random highly non-linear substitutions is extremely difficult. In this paper, we study the annealing simulation method. This is an iterative algorithm, the essence of which is the gradual improvement of the current solution (substitution). Special cost functions are used as an improvement criterion. The initial state is formed randomly, and then, at each iteration the current solution is gradually changed. Approaching the target solution means minimizing the cost function. The paper investigates a simple and computationally efficient cost function based on the Walsh-Hadamard transform. Through exploratory research and numerous tests, it was possible to optimize the operation of the annealing simulation algorithm. Optimized algorithm for several parameters (initial temperature, "cooling factor", cost function) allows you to quickly generate highly non-linear bijective substitutions for cryptographic applications. Compared to other well-known implementations of the annealing simulation algorithm, the use of the recommended parameters can significantly reduce the generation time of nonlinear substitutions.

Key words: simulated annealing; symmetric cryptography; cost function; generation methods; non-linearity; Walsh-Hadamard transform; S-box.

2 tab. 21 fig. Ref: 22 items.

УДК 004.056.5

Обґрунтування параметрів алгоритму імітації відпалу для пошуку нелінійних підстановок симетричних шифрів / *О.О. Кузнецов, М.О. Полуяненко, С.О. Кандій, Є.О. Логачова* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2022. Вип. 209. С. 93 – 109.

Криптографічний захист в інформаційних та інформаційно-комунікаційних системах є важливою складовою кібербезпеки. Отже розробка, дослідження та вдосконалення засобів криптографічного захисту інформації є актуальним та важливим завданням. В роботі досліджуються еволюційні алгоритми генерації нелінійних підстановок (S-boxes). Це криптографічні примітиви, які є важливою складовою багатьох сучасних блокових та потокових шифрів із секретним ключем. Однак завдання генерації випадкових високонелінійних підстановок надзвичайно складне. В роботі досліджується алгоритм імітації відпалу. Це ітераційний алгоритм, сутність якого полягає в поступовому покращенні поточного рішення (підстановки). У якості критерію покращення застосовуються спеціальні функції вартості. Початковий стан формується випадково, потім, крок за кроком, на кожній ітерації поточне рішення поступово змінюється. Наближення до цільового рішення означає мінімізацію функції вартості. В роботі досліджується проста та обчислювально ефективна функція вартості, яка заснована на перетворенні Уолша – Адамара. За допомогою проведених пошукових досліджень та чисельних тестувань вдалося оптимізувати роботу алгоритму імітації відпалу. Оптимізований алгоритм за декількома параметрами (початкова температура, «cooling factor», функція вартості) дозволяє швидко генерувати високонелінійні бієктивні підстановки для криптографічних застосувань. В порівнянні із іншими відомими реалізаціями алгоритму імітації відпалу застосування обґрунтованих параметрів дозволяє значно скоротити час генерації нелінійних підстановок.

Ключові слова: імітація відпалу; симетрична криптографія; функція вартості; методи генерації; нелінійність; перетворення Уолша-Адамара; S-блок.

Табл. 2. Іл. 21. Бібліогр.: 22 назв.

УДК 004.056.5

Обоснование параметров алгоритма имитации отжига для поиска нелинейных подстановок симметричных шифров / *А.А. Кузнецов, Н.А. Полуяненко, С.А. Кандий, Е.О. Логачова* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2022. Вып. 209. С. 93 – 109.

Криптографическая защита в информационных и информационно-коммуникационных системах является важной составляющей кибербезопасности. Следовательно, разработка, исследование и совершенствование средств криптографической защиты информации является актуальной и важной задачей. В работе исследуются эволюционные методы генерации нелинейных подстановок (S-boxes). Это криптографические примитивы, являющиеся важной составляющей многих современных блочных и поточных шифров с секретным ключом. Однако задача генерации случайных высоконелинейных подстановок чрезвычайно сложна. В работе исследуется метод имитации отжига. Это итерационный алгоритм, суть которого заключается в постепенном улучшении текущего решения (подстановки). В качестве критерия улучшения используются особые функции стоимости. Начальное состояние формируется случайно, затем шаг за шагом на каждой итерации текущее решение постепенно меняется. Приближение к целевому решению означает минимизацию функции стоимости. В работе исследуется простая и вычислительно эффективная функция стоимости, основанная на преобразовании Уолша – Адамара. Посредством проведенных поисковых исследований и многочисленных тестирований удалось опти-

мизировать работу алгоритма имитации отжига. Оптимизированный алгоритм по нескольким параметрам (начальная температура, «cooling factor», функция стоимости) позволяет быстро генерировать высоконелинейные биективные подстановки для криптографических применений. По сравнению с другими известными реализациями алгоритма имитации отжига применение рекомендованных параметров позволяет значительно сократить время генерации нелинейных подстановок.

Ключевые слова: имитация отжига; симметричная криптография; функция стоимости; методы генерации; нелинейность; преобразование Уолша-Адамара; S-блок.

Табл. 2. Ил. 21. Библиогр.: 22 назв.

INFORMATION PROTECTION METHODS IN TELECOMMUNICATION SYSTEMS

МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ В ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ В ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ

UDC 004.056.52

Object-oriented model of a formal description of an information and communication system / *V.O. Poddubnyi, R.Y. Gvozdov, O.V. Sievierinov, V.M. Fedorchenko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2022. №209. P. 110 – 117.

The purpose of the article is to study algorithms for the formal description of information and communication systems. The article discusses the main provisions on the formal representation of objects of information and communication systems. It is noted that the main environments of the information and communication system that are subject to a formal description are: physical environment, computing system environment, user environment, information environment. These components of the information and communication system are considered in detail, analyzed and documented in an informal form (in the form of text). There is a need for a mechanism for a unified description of a system that includes all environments. Such a description will be unambiguously formalized with well-defined mathematical concepts. The mechanism of a single formal description or the technique of a formal description will be unambiguous in understanding and serve as a control description when developing an information security policy in an information and communication system. An algorithm for the formal description of the information and communication system is proposed. In this algorithm, it is proposed to focus on the types and interaction of objects with each other. In such a scheme, attention is focused on such concepts as the object, the characteristics of the object, and the type of interaction with the object. Further consideration of the created block diagrams (graphs) is proposed to explore the possibilities of using this model to simulate cyber-attacks. Since each element contains fields that connect it to other elements, and each attack has an "entry point" using graph theory, it is possible to traverse the graph to determine the possible horizontal propagation paths of a cyber-attack.

Key words: information and communication system; formal description technique; UML; communication networks.

1 tab. 2 fig. Ref: 6 items.

УДК 004.056.52

Об'єктно-орієнтована модель формального опису інформаційно-комунікаційної системи / *В.О. Поддубний, Р.Ю. Гвоздьов, О.В. Сєвєрінов, В.М. Федорченко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2022. Вип. 209. С. 110 – 117.

Мета статті – дослідження алгоритмів формального опису інформаційно-комунікаційних систем. Розглядаються основні положення щодо формального представлення об'єктів інформаційно-комунікаційних систем. Зазначено, що основними середовищами інформаційно-комунікаційної системи, що підлягають формальному опису, є: фізичне середовище, середовище обчислювальної системи, середовище користувачів, інформаційне середовище. Дані компоненти інформаційно-комунікаційної системи детально розглядаються, аналізуються та документуються в неформальному вигляді (у вигляді тексту). Виникає необхідність у механізмі єдиного опису системи, що буде включати в себе всі середовища. Такий опис буде однозначно формалізований з чітко визначеними математичними поняттями. Механізм єдиного формального опису або методика формального опису буде однозначна в розумінні та слугуватиме керуючим описом при розробці політики безпеки інформації в інформаційно-комунікаційній системі. Запропоновано алгоритм формального опису інформаційно-комунікаційної системи. В даному алгоритмі пропонується зосередитися на типах об'єктів та взаємодії об'єктів один з іншим. В такій схемі відбувається зосередження уваги на таких поняттях, як об'єкт, характеристики об'єкту та тип взаємодії з об'єктом. Пропонується подальший розгляд створених блок-схем (графів) для дослідження можливостей використання даної моделі для симуляції кібератак. Оскільки кожний елемент містить поля, що зв'язують його з іншими елементами, а кожна атака має «точку входу» за допомогою теорії графів можливо здійснювати обхід графу для визначення можливих шляхів горизонтального розповсюдження кібератаки.

Ключові слова: інформаційно-комунікаційна система; методика формального опису; UML; комунікаційні мережі.

Табл. 1. Іл. 2. Бібліогр.: 6 назв.

УДК 004.056.52

Объектно-ориентированная модель формального описания информационно-коммуникационной системы / *В.А. Поддубный*, *Р.Ю. Гвоздёв, А.В. Северинов, В.Н. Федорченко,* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2022. Вып. 209. С. 110 – 117.

Цель статьи – исследование алгоритмов формального описания информационно-коммуникационных систем. Рассматриваются основные положения по формальному представлению объектов информационно-коммуникационных систем. Отмечено, что основными средами информационно-коммуникационной системы, подлежащих формальному описанию, являются: физическая среда, среда вычислительной системы, среда пользователей, информационная среда. Данные компоненты информационно-коммуникационной системы подробно рассматриваются, анализируются и документируются неформальном виде (в виде текста). Возникает необходимость в механизме единого описания системы, включающей в себя все среды. Такое описание будет однозначно формализовано с четко определенными математическими понятиями. Механизм единого формального описания или методика формального описания будет однозначна в понимании и служит управляющим описанием при разработке политики безопасности информации в информационно-коммуникационной системе. Предложен алгоритм формального описания информационно-коммуникационной системы. В данном алгоритме предлагается сосредоточиться на типах и взаимодействии объектов друг с другом. В такой схеме происходит сосредоточение внимания на таких понятиях, как объект, характеристики объекта и тип взаимодействия с объектом. Предлагается дальнейшее рассмотрение созданных блок-схем (графов) для исследования возможностей использования данной модели для симуляции кибератак. Поскольку каждый элемент содержит поля, связывающие его с другими элементами, а каждая атака имеет «точку входа» с помощью теории графов, можно осуществлять обход графа для определения возможных путей горизонтального распространения кибератаки.

Ключевые слова: информационно-коммуникационная система; методика формального описания; UML; коммуникационные сети.

Табл. 1. Ил. 2. Библиогр.: 6 назв.

UDC 681.3.06

The concept of assessing the risks of cybersecurity of the information system of the critical infrastructure object / *I. Gorbenko*, O. Zamula, *Yu. Osipenko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2022. №209. P. 118 – 129.

Ensuring cyber and information security for critical infrastructure is achieved through the implementation of an appropriate set of information security management measures, which can be provided in the form of software policies, methods, procedures, organizational structures and functions. Information security requirements are determined, in particular, by systematic risk assessment of information security, which can be one of the elements of the predicted approach to identifying hazards in the provision of services to service participants in the information interaction of the information system. The paper presents conceptual provisions for assessing and managing cybersecurity risks of the critical infrastructure information system. The proposed concept involves the definition of: areas of security threats to the information system; involved information assets and calculation of their value; assessment of the probability of attacks on the information system; assessment of the probability of success of attacks on the information system and more. Risk assessment methods are proposed that take into account the probability of success of an attack and the probability of an attack occurring, which makes it possible to eliminate the shortcomings inherent in known approaches and provide more accurate identification of attack methods associated with the attacker's behavior. The concept of cybersecurity risk assessment and the methodology for analyzing and assessing security threats that are presented in the work correspond to approaches to building risk-oriented information security management systems and can become the basis for developing an information security system in the information system of a critical infrastructure object.

Key words: cybersecurity; informational security; information system; critical infrastructure object; risk assessment; asset value; the likelihood of attacks.

10 tab. 8 fig. Ref: 12 items.

УДК 681.3.06

Концепція оцінки ризиків кібербезпеки інформаційної системи об’єкта критичної інфраструктури / *І.Д. Горбенко, О.А. Замула, Ю.С. Осипенко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2022. Вип. 209. С. 118 – 129.

Забезпечення кібер- і інформаційної безпеки для критично важливих об’єктів інфраструктури досягається шляхом реалізації комплексу заходів з управління інформаційною безпекою, які можуть бути надані у формі політик, методів, процедур, організаційних структур і функцій програмного забезпечення. Вимоги до інформаційної безпеки визначаються, зокрема, за допомогою систематичної оцінки ризиків інформаційної безпеки, яка може бути однією з елементів прогнозованого підходу виявлення небезпечних факторів при наданні послуг з обслуговування учасників інформаційної взаємодії інформаційної системи. Представлено концептуальні положення щодо оцінки і управління ризиками кібербезпеки інформаційної системи об’єкта критичної інфраструк-

тури. Запропонована концепція припускає визначення: областей загроз безпеки інформаційної системи; задіяних інформаційних активів та розрахунок їхньої вартості; оцінку ймовірності виникнення атак на інформаційну систему; оцінку ймовірності успіху атак на інформаційну систему та інше. Запропоновано методи оцінки ризику, які враховують ймовірності успіху атаки та ймовірності виникнення атаки, що дозволяє усунути недоліки, які притаманні відомим підходам та забезпечити більш точну ідентифікацію методів атаки, пов'язаних із поведінкою зловмисника. Концепція оцінки ризиків кібербезпеки і методика аналізу та оцінки загроз безпеки, які надані у роботі, відповідають підходам до побудови ризикоорієнтованих систем управління інформаційною безпекою і можуть стати основою для розробки системи безпеки інформації в інформаційній системі об'єкта критичної інфраструктури.

Ключові слова: кібербезпека; інформаційна безпека; інформаційна система; об'єкт критичної інфраструктури; оцінка ризику; вартість активів; ймовірність виникнення атак.

Табл. 10. Іл.8. Бібліогр.: 12 назв.

УДК 681.3.06

Концепция оценки рисков кибербезопасности информационной системы объекта критической инфраструктуры / *И.Д. Горбенко, А.А. Замула, Ю.С. Осипенко* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2022. Вып. 209. С. 118 – 129.

Обеспечение кибер- и информационной безопасности для критически важных объектов инфраструктуры достигается за сет реализации комплекса мер по управлению информационной безопасностью, которые могут быть предоставлены в форме политик, методов, процедур, организационных структур и функций программного обеспечения. Требования к информационной безопасности определяются, в частности, посредством систематической оценки рисков информационной безопасности, которая может быть одним из элементов прогнозируемого подхода выявления опасных факторов при предоставлении услуг по обслуживанию участников информационного взаимодействия информационной системы. Представлены концептуальные положения по оценке и управлению рисками кибербезопасности информационной системы объекта критической инфраструктуры. Предложенная концепция предполагает определение: областей угроз безопасности информационной системы; задействованных информационных активов и расчет их стоимости; оценку вероятности возникновения атак на информационную систему; оценку вероятности успеха атак на информационную систему и прочее. Предложены методы оценки риска, учитывающие вероятности успеха атаки и вероятности возникновения атаки, что позволяет устранить недостатки, которые присущи известным подходам и обеспечить более точную идентификацию методов атаки, связанных с поведением злоумышленника. Концепция оценки рисков кибербезопасности и методика анализа и оценки угроз безопасности, которые представлены в работе, отвечают подходам к построению рискоориентированных систем управления информационной безопасностью и могут стать основой для разработки системы безопасности информации в информационной системе объекта критической инфраструктуры.

Ключевые слова: кибербезопасность; информационная безопасность; информационная система; объект критической инфраструктуры; оценка риска; стоимость активов; вероятность возникновения атак.

Табл. 10. Ил.8. Библиогр.: 12 назв.

UDC 004.056

Scaling analysis of the Telegram Open Network blockchain project / *V.I. Yukhymenko, O.I. Fediushyn* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2022. №209. P. 130 – 137.

Blockchain systems are always distributed but differ greatly in resolutions, sizes, roles, transparency, types of participants, and the way transactions are handled. The decentralized structure offers inalienable security benefits, but with a large number of participants faces the problem of limited scaling. Sharding is suggested to solve this problem. Sharding is a way to divide consensual workload and transactions into several nodes. Effective application of sharding requires a lot of detail and work in terms of architecture and system implementation. As was found in the process of the work, in order to achieve significant results in scaling the blockchain system through sharding, it is necessary that the blockchain project is based on several blockchains simultaneously (i.e. had a multi-blockchain architecture) and provides infrastructure for fast and reliable messaging between them (i.e. strongly interconnected). The Telegram Open Network (TON) and its component TON Blockchain are considered an example of such a project.

This work provides a comparative analysis of the most popular blockchain platforms (Bitcoin and Ethereum) with the implementations of TON Blockchain ideas (The Open Network and Everscale) on three parameters: system bandwidth (measured at transactions per second, abbreviated TPS), the average time of a new block's appearance in the network and projected bandwidth in TPS.

Key words: Telegram Open Network; scaling; blockchain; sharding

2 tab. 6 fig. Ref: 15 items.

УДК 004.056

Аналіз масштабування блокчейн проєкту Telegram Open Network / *В.І. Юхименко, О.І. Федюшин* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2022. Вип. 209. С. 130 – 137.

Блокчейн системи завжди розподілені, але сильно відрізняються за дозволами, розмірами, ролями, прозорістю, типами учасників та способом обробки транзакцій. Децентралізована структура пропонує невід'ємні

переваги безпеки, оскільки усуває єдину точку відмови, але при великій кількості учасників стикається з проблемою обмеженої продуктивності. Для вирішення проблеми продуктивності пропонується використання шардингу. Шардинг – це спосіб розділити консенсусне робоче навантаження та транзакції на кілька вузлів. Ефективне застосування шардингу потребує багато деталей та роботи з точки зору архітектури та реалізації системи. Як було виявлено у ході роботи, щоб досягнути значних результатів в масштабуванні системи за допомогою шардингу, потрібно щоб блокчейн проєкт базувався на декількох блокчейнах одночасно (тобто мав multi blockchain архітектуру) та надавав інфраструктуру для швидкого та надійного обміну повідомленнями між ними (тобто щоб ці блокчейни були сильно зв'язані поміж собою). Як приклад такого проєкту розглянуто Telegram Open Network (TON), і його складову TON Blockchain.

Проведений порівняльний аналіз найпопулярніших блокчейн платформ з реалізаціями TON Blockchain (The Open Network та Everscale) за трьома показниками: пропускна здатність системи (transactions per second, скорочено TPS), середній час появи нового блоку в мережі (average block time) та прогнозована пропускна здатність у TPS показав, що загальна архітектура TON унікальна і дуже орієнтована на підтримку масштабування.

Ключові слова: Telegram Open Network; масштабування; блокчейн; шардинг.

Табл. 2. Іл. 6. Бібліогр.: 15 назв.

УДК 004.056

Анализ масштабирования блокчейн проекта Telegram Open Network / *В.И. Юхименко, А.И. Федюшин* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2022. Вып. 209. С. 130 – 137.

Блокчейн системы всегда распределены, но сильно отличаются по правам, размерам, ролям, прозрачности, типам участников и способу обработки транзакций. Децентрализованная структура предлагает неотъемлемые преимущества безопасности, поскольку устраняет единую точку отказа, но при большом количестве участников сталкивается с проблемой ограниченной производительности. Для решения проблемы производительности предлагается использовать шардинг. Шардинг – это способ разделить консенсусную рабочую нагрузку и транзакции на несколько узлов. Эффективное применение шардинга требует многих деталей и работы с точки зрения архитектуры и реализации системы. Как было установлено в ходе работы, чтобы достичь значительных результатов в масштабировании системы с помощью шардинга, нужно чтобы блокчейн проект базировался на нескольких блокчейнах одновременно (т.е. имел multi blockchain архитектуру) и предоставлял инфраструктуру для быстрого и надежного обмена сообщениями между ними (т.е. чтобы эти блокчейны были сильно связаны между собой). В качестве примера такого проекта рассмотрен Telegram Open Network (TON) и его составляющая TON Blockchain.

Сравнительный анализ популярнейших блокчейн платформ с реализациями TON Blockchain (The Open Network и Everscale) по трем показателям: пропускная способность системы (transactions per second, сокращенно TPS), среднее время появления нового блока в сети (average block time) и прогнозируемая пропускная способность в TPS показал, что общая архитектура TON уникальна и очень ориентирована на поддержку масштабирования.

Ключевые слова: Telegram Open Network; масштабирование; блокчейн; шардинг.

Табл. 2. Ил. 6. Библиогр.: 15 назв.

UDC 004.056: 004.056.5

Research on the main methods and schemes of encryption with search capability / *V.I. Yesin, V.V. Vilihura* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2022. №209. P. 138 – 155.

The growing popularity of data outsourcing to third-party cloud servers causes their owners to have serious concerns about their security due to possible data leakage. A well-known measure to solve this problem and ensure the confidentiality of data is to encrypt it. However, the use of traditional encryption techniques is faced with the problem of how to allow untrusted cloud servers to perform search operations, while the actual data transmitted must remain confidential. Searchable encryption is a powerful tool, a class of cryptographic techniques that attempts to solve this problem. Searchable encryption acts as a data management technique that allows data owners to store and manage their data on a third-party, untrusted cloud server, and allows the data user to delegate search functions to the cloud server to retrieve that data. Currently, there are a number of approaches to solving this problem, although there is still no dominant solution. Therefore, the paper presents an overview of current secure search solutions. The main searchable encryption techniques are considered, which allow you to perform search operations on encrypted data without disclosing any information about what is being searched. The strengths and weaknesses of the analyzed methods are highlighted. Models and architectures of existing secure search engines are analyzed, taking into account the peculiarities of their operation scenarios. The problem of confidentiality in searchable encryption schemes is discussed. A comparative analysis of the performance of several searchable symmetric encryption schemes is given. Various gaps in the area under consideration are identified, with indication of open research problems.

Key words: database; data warehouse; confidentiality; encryption; searchable encryption.

1 tab. 5 fig. Ref: 56 items.

УДК 004.056: 004.056.5

Дослідження основних методів і схем шифрування з можливістю пошуку / *В.І. Єсін, В.В. Вілігура* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2022. Вип. 209. С. 138 – 155.

Зростаюча популярність аутсорсингу даних на сторонні хмарні сервери викликає у їх власників серйозну стурбованість за їхню безпеку через можливий витік даних. Відомим заходом вирішення цієї проблеми та забезпечення конфіденційності даних є їх шифрування. Однак використання традиційних методів шифрування стикається з проблемою, як дозволити ненадійним хмарним серверам виконувати пошукові операції, в той час як дані, що фактично передаються, мають залишатися конфіденційними. Шифрування із можливістю пошуку – це потужний інструмент, клас криптографічних методів, який намагається вирішити цю проблему. Шифрування з можливістю пошуку діє як метод керування даними, який дозволяє власникам даних зберігати свої дані та керувати ними на сторонньому, ненадійному хмарному сервері, а також дозволяє користувачеві даних делегувати функції пошуку хмарному серверу для отримання цих даних. Нині існує низка підходів до вирішення цієї проблеми, хоча домінуючого рішення немає досі. Тому в роботі подано огляд поточних рішень захищеного пошуку. Розглядаються основні методи шифрування з можливістю пошуку, які дозволяють виконувати операції пошуку зашифрованих даних без розкриття будь-якої інформації про те, що шукається. Виділяються слабкі та сильні сторони аналізованих методів у сценаріях, де потрібна як конфіденційність, так і доступність відповідних даних. Аналізуються моделі та архітектури існуючих захищених пошукових систем з урахуванням особливостей сценаріїв їхнього функціонування. Обговорюється проблема конфіденційності у схемах шифрування з можливістю пошуку. Наводиться порівняльний аналіз продуктивності кількох схем симетричного шифрування з можливістю пошуку. Виявляються різні прогалини у аналізованої області із зазначенням відкритих дослідницьких проблем.

Ключові слова: база даних; сховище даних; конфіденційність; шифрування; шифрування з можливістю пошуку.

Табл. 1. Іл. 5. Бібліогр.: 56 назв.

УДК 004.056: 004.056.5

Исследование основных методов и схем шифрования с возможностью поиска / *В.И. Есин, В.В. Вилигура* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2022. Вып. 209. С. 138 – 155.

Растущая популярность аутсорсинга данных на сторонние облачные серверы вызывает у их владельцев серьезную озабоченность их безопасности, в виду возможной утечки данных. Известной мерой решения этой проблемы и обеспечения конфиденциальности данных является их шифрование. Однако использование традиционных методов шифрования сталкивается с проблемой, как разрешить ненадежным облачным серверам выполнять поисковые операции, в то время как фактически передаваемые данные должны оставаться конфиденциальными. Шифрование с возможностью поиска – это мощный инструмент, класс криптографических методов, который пытается решить эту проблему. Шифрование с возможностью поиска действует как метод управления данными, который позволяет владельцам данных хранить свои данные и управлять ими на стороннем, ненадежном облачном сервере, а также позволяет пользователю данных делегировать функции поиска облачному серверу для извлечения этих данных. В настоящее время существует ряд подходов к решению данной проблемы, хотя доминирующего решения нет до сих пор. Поэтому в работе представлен обзор текущих решений защищенного поиска. Рассматриваются основные методы шифрования с возможностью поиска, которые позволяют выполнять операции поиска зашифрованных данных без раскрытия какой-либо информации о том, что ищется. Выделяются слабые и сильные стороны анализируемых методов в сценариях, где требуется как конфиденциальность, так и доступность соответствующих данных. Анализируются модели и архитектуры существующих защищенных поисковых систем с учетом особенностей сценариев их функционирования. Обсуждается проблема конфиденциальности в схемах шифрования с возможностью поиска. Приводится сравнительный анализ производительности нескольких схем симметричного шифрования с возможностью поиска. Выявляются различные пробелы в рассматриваемой области с указанием открытых исследовательских проблем.

Ключевые слова: база данных; хранилище данных; конфиденциальность; шифрование; шифрование с возможностью поиска.

Табл. 1. Ил. 5. Библиогр.: 56 назв.

UDC 621.396:004.056

Improving the efficiency of methods and means for suppressing unauthorized speech recording / *A.N. Oleynikov, V.A. Pulavsky, I.N. Chigirev* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2022. №209. P. 156 – 161.

The article analyzes the effectiveness of suppressing an unauthorized recording using acoustic, electromagnetic and ultrasonic countermeasures. It is shown that acoustic, electromagnetic and ultrasonic counteraction without a priori knowledge of the type of voice recorder does not provide guaranteed suppression of unauthorized speech recording. To increase the suppression efficiency, it is proposed to adapt the acoustic method, taking into account the characteristics of the propagation of acoustic vibrations in the air, the psychophysical perception of sounds by the human ear, and the use of an electrostatic emitter. The technical parameters of an electrostatic acoustic system make it possible to bring the spectral characteristics of the interference as close as possible to the voices of the interlocutors, increase the power flux density of the interference signal and reduce the intensity of its impact on the hearing organs. The article presents comparative results of experimental studies of suppressors based on adapted acoustic, electromagnetic and ultrasonic methods. The proposed adapted acoustic method for counteracting unauthorized speech recording is equally effective for any

type of recording device, since the interference is generated along a functional acoustic channel, taking into account the propagation and perception of acoustic vibrations by a person.

Key words: speech; record; acoustic; electromagnetic; ultrasonic; method; means; suppression; efficiency.

4 tab. 2 fig. Ref: 4 items.

УДК 621.396:004.056

Підвищення ефективності методів та засобів подавлення несанкціонованого запису мовн / *А.М. Олейніков,, В.А. Пулавський, І.М. Чигірьов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2022. Вип. 209. С. 156 – 161.

Аналізується ефективність подавлення несанкціонованого запису мови з використанням акустичних, електромагнітних та ультразвукових засобів протидії. Показано, що акустична, електромагнітна та ультразвукова протидія без апріорного знання типу диктофона не забезпечує гарантованого подавлення несанкціонованого запису мови. Для підвищення ефективності подавлення пропонується адаптувати акустичний метод з урахуванням особливостей поширення у повітрі акустичних коливань, психофізичного сприйняття звуків людським вухом та використання електростатичного випромінювача. Технічні параметри електростатичної акустичної системи дозволяють максимально наблизити спектральні характеристики перешкоди до голосів співрозмовників, збільшити щільності потоку потужності перешкодного сигналу та знизити інтенсивність його впливу на органи слуху. У статті наведено порівняльні результати експериментальних досліджень подавлювачів на основі адаптованого акустичного, електромагнітного та ультразвукового методів. Запропонований адаптований акустичний метод протидії несанкціонованого запису мови однаково ефективний для будь-яких типів записуючих пристроїв, оскільки перешкода формується по функціональному каналу – акустичному з урахуванням особливостей поширення та сприйняття людиною акустичних коливань.

Ключові слова: мова; запис; акустичний; електромагнітний; ультразвуковий; метод; засіб; подавлення; ефективність.

Табл. 4. Іл. 2. Бібліогр.: 4 назв.

УДК 621.396:004.056

Повышение эффективности методов и средств подавления несанкционированной записи речи / *А.Н. Олейников, В.А. Пулавский, И.Н. Чигирев* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2022. Вып. 209. С. 156 – 161.

Анализируется эффективность подавления несанкционированной записи с использованием акустических, электромагнитных и ультразвуковых средств противодействия. Показано, что акустическое, электромагнитное и ультразвуковое противодействие без априорного знания типа диктофона не обеспечивает гарантированное подавление несанкционированной записи речи. Для повышения эффективности подавления предлагается адаптировать акустический метод с учетом особенностей распространения в воздухе акустических колебаний, психофизического восприятия звуков человеческим ухом и использования электростатического излучателя. Технические параметры электростатической акустической системы позволяют максимально приблизить спектральные характеристики помехи к голосам собеседников, увеличить плотность потока мощности помехового сигнала и снизить интенсивность его воздействия на органы слуха. В статье представлены сравнительные результаты экспериментальных исследований подавителей на основе адаптированного акустического, электромагнитного и ультразвукового методов. Предложенный адаптированный акустический метод противодействия несанкционированной записи речи одинаково эффективен для любых типов записывающих устройств, поскольку помеха формируется по функциональному акустическому каналу с учетом особенностей распространения и восприятия человеком акустических колебаний.

Ключевые слова: речь; запись; акустический; электромагнитный; ультразвуковой; метод; средство; подавление; эффективность.

Табл. 4. Ил. 2. Библиогр.: 4 назв.

RADIOLOCATION AND RADIONAVIGATION
РАДІОЛОКАЦІЯ І РАДІОНАВІГАЦІЯ
РАДИОЛОКАЦИЯ И РАДИОНАВИГАЦИЯ

UDC 621.396.967.2

Comparative analysis of methods for determining the air objects' coordinates using wide-area multilateration systems / *I.V. Svyd, V.V. Semenets, O.S. Maltsev, M.G. Tkach, S.V. Starokozhev, O.O. Datsenko, I.O. Shevtsov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2022. №209. P. 162 – 177.

The presented work considers the place and role of wide-area multi-position airspace surveillance in the information support of airspace control and air traffic control systems. Classification of methods for estimating the coordinates of air objects using various primary measurements of the parameters of received signals in multi-position observation is given. A quantitative assessment of the accuracy in determining the air objects' coordinates by the considered methods is also given. The capabilities of wide-area multi-position surveillance systems increase significantly when

using the principles of constructing a secondary surveillance radar as a non-synchronous network, and an aircraft responder as an open single-channel queuing system with servicing the first correctly received request signal. An unauthorized request from an aircraft responder makes it possible to switch from completely passive methods for detecting and determining the coordinates of an air object to active-passive ones, which provide an increase in the accuracy of solving a coordinate task by dozens of times while maintaining the energy secrecy of a wide-area multi-position observation system. It is shown that the use of active and passive methods for constructing wide-area multi-position observation systems makes it possible to implement goniometric, difference-range, goniometer-range, total-range and goniometer-total-range methods for determining the coordinates of an air object. This increases significantly the number of options for estimating the coordinates of an air object. As a result, it allows improving the quality of information support for users by choosing the optimal method for estimating the coordinates of the observed air objects using various primary measurements of the received signals parameters.

Key words: Wide Area MultiLateration (WAM); primary surveillance radar; secondary surveillance radar; air traffic control; MultiLateration (MLAT); air object; coordinates; aircraft responder..

7 fig. Ref: 54 items.

УДК 621.396.967.2

Порівняльний аналіз методів визначення координат повітряних об’єктів системами широкозонової мультилатерації / *І.В. Свид, В.В. Семенець, О.С. Мальцев, М.Г. Ткач, С.В. Старокожев, О.О. Даценко, І.О. Шевцов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2022. Вип. 209. С. 162 – 177.

Розглядається місце та роль широкозонового багатопозиційного спостереження повітряного простору в інформаційному забезпеченні систем контролю використання повітряного простору та управління повітряним рухом. Наводиться класифікація методів оцінки координат повітряних об'єктів при використанні різних первинних вимірювань параметрів приймаємих сигналів при багатопозиційному спостереженні. Також наводиться кількісна оцінка точності визначення координат повітряних об'єктів розглянутими методами. Можливості систем широкозонового багатопозиційного спостереження значно зростають при використанні принципів побудови вторинного оглядового радіолокатора, як несинхронної мережі, і літакового відповідача, як відкритої одноканальної системи масового обслуговування, з обслуговуванням першого правильно прийнятого сигналу запиту. Несанкціонований запит літакового відповідача дозволяє перейти від повністю пасивних методів виявлення та визначення координат повітряного об'єкта до активно-пасивних, що забезпечує збільшення точності вирішення координатного завдання у десятки разів із збереженням енергетичної скритності системи широкозонового багатопозиційного спостереження. Показано, що використання активного та пасивного методів побудови систем широкозонового багатопозиційного спостереження дозволяє реалізувати кутомірний, різницево-далекомірний, кутомірно-далекомірний, сумарно-далекомірний та кутомірно-сумарно-далекомірний методи визначення координат повітряного об'єкта. Це істотно збільшує кількість варіантів оцінки координат повітряного об'єкта. І, як наслідок, дозволяє підвищити якість інформаційного забезпечення користувачів шляхом вибору оптимального методу оцінки координат спостерігаються повітряних об'єктів при використанні різних первинних вимірів параметрів приймаємих сигналів.

Ключові слова: Wide Area MultiLateration; WAM; первинний оглядовий радіолокатор; вторинний оглядовий радіолокатор; управління повітряним рухом; MultiLateration; MLAT; повітряний об'єкт; координати; літаковий відповідач.

Іл. 7. Бібліогр.: 54 назв.

УДК 621.396.967.2

Сравнительный анализ методов определения координат воздушных объектов системами широкозоновой мультилатерации / *И.В. Свид, В.В. Семенец, А.С. Мальцев, М.Г. Ткач, С.В. Старокожев, А.А. Даценко, И.А. Шевцов* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2022. Вып. 209. С. 162 – 177.

Рассматривается место и роль широкозонового многопозиционного наблюдения воздушного пространства в информационном обеспечении систем контроля использования воздушного пространства и управления воздушным движением. Приводится классификация методов оценки координат воздушных объектов при использовании различных первичных измерений параметров принимаемых сигналов при многопозиционном наблюдении. Также приводится количественная оценка точности определения координат воздушных объектов рассмотренными методами. Возможности систем широкозонового многопозиционного наблюдения значительно возрастают при использовании принципов построения вторичного обзорного радиолокатора как несинхронной сети и самолетного ответчика как открытой одноканальной системы массового обслуживания с обслуживанием первого правильно принятого сигнала запроса. Несанкционированный запрос самолетного ответчика позволяет перейти от полностью пассивных методов обнаружения и определения координат воздушного объекта к активно-пассивным, обеспечивающим увеличение точности решения координатного задания в десятки раз с сохранением энергетической скрытности системы широкозонового многопозиционного наблюдения. Показано, что использование активного и пассивного методов построения систем широкозонового многопозиционного наблюдения позволяет реализовать угломерный, разностно-дальномерный, угломерно-дальномерный, суммарно-дальномерный и угломерно-суммарно-дальномерный методы определения координат воздушного объекта. Это существенно увеличивает количество вариантов оценки координат воздушного объекта. И, как следствие, позволяет повысить качество информационного обеспечения пользователей путем выбора оптимального мето-

да оценки координат наблюдаемых воздушных объектов при использовании различных первичных измерений параметров принимаемых сигналов.

Ключевые слова: Wide Area MultiLateration; WAM; первичный обзорный радиолокатор; вторичный обзорный радиолокатор; управление воздушным движением; MultiLateration; MLAT; воздушный объект; координаты; самолетный ответчик.

Ил. 7. Библиогр.: 54 назв.

ELECTRODYNAMICS, RADIO WAVES PROPAGATION
ЕЛЕКТРОДИНАМІКА, ПОШИРЕННЯ РАДІОХВИЛЬ
ЭЛЕКТРОДИНАМИКА, РАСПРОСТРАНЕНИЕ РАДИОВОЛОН

UDC 621.396.677.494

Estimation of requirements to signal parameters at V-shaped frequency distribution in mathematical model of multi-position transmitter system / *A.I. Kovalenko, S.V. Titov, E.V. Titova, O.S. Cherna* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2022. № 209. P. 178 – 184.

This paper is a brief review of methods for electromagnetic radiation focusing using a multi-position system of radiators based on mutually consistent spatial-amplitude-phase-frequency control of radiated signals and limitations of their potentialities arising from various random fluctuations of signals and antenna parameters. The statistical study of influence of different random and deterministic variations of electrical and design parameters of the antennas, control systems of the radiated signals with V-shaped frequency distribution over the aperture of a multi-position radiating system on the peak power level, duration and repetition period of the focused pulses is carried out. The parameters of the space-amplitude-phase-frequency control law must be stable for a time equal to the average duration of the pulses at the output of the emitters when forming a single space-time pulse, and when forming a sequence of space-time pulses during this pack of space-time pulses. The requirements concerning accuracy and stability of parameters of the signals' space-phase-frequency control law are considered. The analysis of the influence of various kinds of deviations from the given values of the parameters of the space-phase-frequency control law of emitted signals in the channels of a multi-position system of emitters during formation of space-time pulses sequences is carried out. It is shown that the influence of errors in the location of the phase centers of the emitters in the direction of radiation does not depend on the distance to the focusing point, but is significant and special measures are required to reduce them.

Key words: pulse; focusing; transmitter; antenna; model; system; power; frequency; deviation; accuracy.

3 fig. Ref: 15 items.

УДК 621.396.677.494

Оцінка вимог до параметрів сигналів при V-подібному розподілі частот у математичній моделі багатопозиційної системи випромінювачів / *А.І. Коваленко, С.В. Тітов, О.В. Тітова, О.С. Чорна* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2022. Вип. 209. С. 178 – 184.

Зроблено короткий огляд методів фокусування електромагнітного випромінювання багатопозиційною системою випромінювачів на основі взаємоузгодженого просторово-амплітудно-фазово-частотного управління випромінюваними сигналами та обмежень їх потенційних можливостей, що виникають через різні випадкові флуктуації параметрів сигналів і антен. Проведено статистичне дослідження впливу різних випадкових та детермінованих змін електричних та конструктивних параметрів антен, систем управління випромінюваними сигналами при V-подібному розподілі частот по апертурі багатопозиційної системи випромінювачів на рівень пікової потужності, тривалість та період повторення сфокусованих імпульсів. Параметри закону просторово-амплітудно-фазово-частотного управління повинні бути стабільні протягом часу, рівного усередненій тривалості імпульсів на виході випромінювачів при формуванні одиночного просторово-часового імпульсу, а при формуванні послідовності просторово-часових імпульсів – протягом тривалості цієї пачки просторово-часових імпульсів. Розглянуто вимоги до точності та стабільності параметрів закону просторово-фазово-частотного управління сигналами. Проведено аналіз впливу різноманітних відхилень від заданих значень параметрів закону просторово-фазово-частотного управління випромінюваними сигналами в каналах багатопозиційної системи випромінювачів при формуванні послідовностей просторово-часових імпульсів. Показано, що вплив помилок розташування фазових центрів випромінювачів у напрямку випромінювання не залежить від дальності до точки фокусування, але є суттєвим і потрібне вживання спеціальних заходів щодо їх зниження.

Ключові слова: імпульс; фокусування; випромінювач; антена; модель; система; потужність; частота; відхилення; точність.

Іл. 3. Бібліогр.: 15 назв.

УДК 621.396.677.494

Оценка требований к параметрам сигналов при V-образном распределении частот в математической модели многопозиционной системы излучателей / *А.И. Коваленко, С.В. Титов, Е.В. Титова, О.С. Черная* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2022. Вып. 209. С. 178 – 184.

Сделан краткий обзор методов фокусировки электромагнитного излучения многопозиционной системой излучателей на основе взаимосогласованного пространственно-амплитудно-фазово-частотного управления излучаемыми сигналами и ограничений их потенциальных возможностей, возникающих из-за различных случай-

ных флуктуаций параметров сигналов и антенн. Проведено статистическое исследование влияния различных случайных и детерминированных изменений электрических и конструктивных параметров антенн, систем управления излучаемыми сигналами при V-образном распределении частот по апертуре многопозиционной системы излучателей на уровень пиковой мощности, длительность и период повторения сфокусированных импульсов. Параметры закона пространственно-амплитудно-фазово-частотного управления должны быть стабильны в течение времени, равного усредненной длительности импульсов на выходе излучателей при формировании одиночного пространственно-временного импульса, а при формировании последовательности пространственно-временных импульсов – в течение длительности этой пачки пространственно-временных импульсов. Рассмотрены требования к точности и стабильности параметров закона пространственно-фазово-частотного управления сигналами. Проведен анализ влияния различного рода отклонений от заданных значений параметров закона пространственно-фазово-частотного управления излучаемыми сигналами в каналах многопозиционной системы излучателей при формировании последовательностей пространственно-временных импульсов. Показано, что влияние ошибок расположения фазовых центров излучателей в направлении излучения не зависит от дальности до точки фокусировки, но является существенным и требуется принятие специальных мер по их снижению.

Ключевые слова: импульс; фокусировка; излучатель; антенна; модель; система; мощность; частота; отклонение; точность.

Ил. 3. Библиогр.: 15 назв.

AUTOMATION AND COMPUTER INTEGRATED TECHNOLOGIES
АВТОМАТИЗАЦІЯ ТА КОМП'ЮТЕРНО-ІНТЕГРОВАНІ ТЕХНОЛОГІЇ
АВТОМАТИЗАЦИЯ И КОМПЬЮТЕРНО-ИНТЕГРИРОВАННЫЕ ТЕХНОЛОГИИ

UDC 004.896

Determining the coordinates of a mobile robot in an industrial space using BLE technology based on RSSI data received from base stations / *I.Sh. Nevliudov, S.P. Novoselov, O.V. Sychova, S.I. Tesliuk* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2022. №209. P. 185 – 191.

Existing global positioning technologies cannot be applied indoors, where the signal from satellites or communication towers is significantly reduced or completely absent due to signal weakening in the walls of the building. Wireless network technologies such as Bluetooth or Wi-Fi can also be used in the process of local determining the mobile platforms position in industrial premises. But such methods have a problem with providing the required accuracy. The relevance of these studies is associated with solving the problem of local positioning of mobile robots in a room with an accuracy of ten centimeters. The article presents a comparative analysis of determining coordinates' principles by the AOA, TOA, TDOA and RSSI methods. It is proposed to use BLE technologies based on the RSSI data received from base stations. Using the triangulation method, formulas are obtained for solving the problem of determining the coordinates of an object moving in space. The software and hardware complex architecture has been developed. It is proposed to use ESP32 modules as base radio stations. The RSSI value is very unstable, so the positioning accuracy will depend on the number of base stations and the additional software tools used.

Key words: base stations; RSSI data; local positioning; radio signals; BLE technology; triangulation

4 fig. Ref: 21 items.

УДК 004.896

Визначення координат мобільного робота у промисловому приміщенні з використанням технології BLE на основі даних RSSI, отриманих від базових станцій / *І.Ш. Невлюдов, С.П. Новоселов, О.В. Сичова, С.І. Теслюк* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2022. Вип. 209. С. 185 – 191.

Існуючі технології глобального позиціонування не можуть бути застосовані в приміщенні, де сигнал зі супутників або вишок зв'язку значно знижується або зовсім відсутній внаслідок ослаблення сигналу в стінах будівлі. Також в процесі локального визначення положення мобільних платформ у промислових приміщеннях можуть бути використані технології бездротових мереж, таких як Bluetooth чи Wi-Fi. Але у таких методів існує проблема з забезпеченням потрібної точності. Актуальність даних досліджень пов'язана із вирішенням проблеми локального позиціонування мобільних роботів в приміщенні з точністю до десятків сантиметрів. У статті подано порівняльний аналіз принципів визначення координат методами AOA, TOA, TDOA та RSSI. Запропоновано використовувати технологію BLE на основі даних RSSI, отриманих від базових станцій. За допомогою метода тріангуляції отримано формули для вирішення задачі визначення координат об'єкту, що рухається в просторі. Розроблено архітектуру програмно-апаратного комплексу. В якості базових станцій для радіозв'язку пропонується використовувати модулі ESP32. Значення RSSI дуже нестабільне, тому точність позиціонування буде залежати від кількості базових станцій та від використаних додаткових програмних інструментів.

Ключові слова: базові станції; дані RSSI; локальне позиціонування; радіосигнали; технологія BLE; тріангуляція.

Іл. 4. Бібліогр.: 21 назв.

УДК 004.896

Определение координат мобильного робота в промышленном помещении с использованием технологии BLE на основе данных RSSI, полученных от базовых станций / *И.Ш. Невлюдов, С.П. Новоселов, О.В. Сычева, С.И. Теслюк* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2022. Вып. 209. С. 185 – 191.

Существующие технологии глобального позиционирования не могут быть применены в помещении, где сигнал со спутников или вышек связи значительно снижается или вовсе отсутствует вследствие ослабления сигнала в стенах здания. Также в процессе локального определения положения мобильных платформ в промышленных помещениях могут быть использованы технологии беспроводных сетей, таких как Bluetooth или Wi-Fi. Но у таких методов существует проблема с обеспечением требуемой точности. Актуальность данных исследований связана с решением проблемы локального позиционирования мобильных роботов в помещении с точностью до десятка сантиметров. В статье проведен сравнительный анализ принципов определения координат методами AOA, TOA, TDOA и RSSI. Предложено использовать технологии BLE на основе данных RSSI, полученных от базовых станций. С помощью метода триангуляции получены формулы для решения задачи определения координат движущегося в пространстве объекта. Разработана архитектура программно-аппаратного комплекса. В качестве базовых радиостанций предлагается использовать модули ESP32. Значение RSSI очень нестабильное, поэтому точность позиционирования будет зависеть от количества базовых станций и использованных дополнительных программных инструментов.

Ключевые слова: базовые станции; данные RSSI; локальное позиционирование; радиосигналы; технология BLE; триангуляция.

Ил. 4. Библиогр.: 21 назв.

BIOMEDICAL RADIO ELECTRONICS
БІОМЕДИЧНА РАДІОЕЛЕКТРОНІКА
БИОМЕДИЦИНСКАЯ РАДИОЭЛЕКТРОНИКА

UDC 616.833

Modeling the electrical stimulation intensity dependence on stimulus frequency / *I. Prasol, O. Yeroshenko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2022. №209. P. 192 – 199.

The object of research is the process of electrical stimulation of human skeletal muscles during therapeutic therapy. The subject of study is a mathematical model of the electrostimulation characteristic, which relates the amplitude of muscle contraction and the frequency of the stimulating effect. The purpose of the work is to develop a mathematical model in the form of an analytical expression for describing the dependence of the amplitude of muscle contractions on the frequency of electrical stimuli. Methods used: methods of mathematical modeling, methods of structural and parametric identification of models, methods of approximation, methods of parametric optimization, methods of mathematical analysis. The results obtained: an analytical model in the form of a polynomial is proposed, which displays the dependence of the amplitude of muscle contraction on the frequency of stimuli; the degree of the polynomial is chosen and the coefficients of the model are obtained by parametric optimization; a model trajectory is built and the accuracy of modeling is estimated; an equation is obtained and its possible solutions are found to determine the optimal value of the stimulus frequency. The results can be used in the selection of individual effects of electrical stimulation during one session or with extrapolation over a number of sessions. Scientific novelty: an analytical description of the influence of the frequency of electrical stimuli on the mode of contraction of skeletal muscles has been obtained, which allows you to determine the individual optimal parameters of electromyostimulation.

Key words: electrical stimulation; skeletal muscle; muscle contraction; modeling; contraction intensity, stimulus frequency.

5 fig. Ref: 15 items.

УДК 616.833

Моделювання залежності інтенсивності електростимуляції від частоти слідування стимулів / *І.В. Прасол, О.А. Єрошенко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2022. Вип. 209. С. 192 – 199.

Об'єкт дослідження – процес електростимуляції скелетних м'язів людини під час лікувальної терапії. Предмет вивчення – математична модель електростимуляційної характеристики, яка пов'язує амплітуду скорочення м'язів та частоту стимулюючого впливу. Мета роботи – розробка математичної моделі для опису залежності амплітуди м'язових скорочень від частоти електричних стимулів. Методи, що використовуються: методи математичного моделювання, методи структурної та параметричної ідентифікації моделей, методи апроксимації, методи параметричної оптимізації, методи математичного аналізу. Отримані результати: запропоновано аналітичну модель у формі полінома, яка відображає залежність амплітуди скорочення м'язів від частоти стимулів; обрано ступінь полінома та отримано коефіцієнти моделі шляхом параметричної оптимізації; побудовано модельну траєкторію та оцінено точність моделювання; отримано рівняння та знайдено можливі його розв’язки для визначення оптимального значення частоти стимулів. Результати можливо використати для вибору індивідуальних впливів електростимуляції протягом одного сеансу або з екстраполяцією протягом декількох сеансів. Наукова новизна: отримано аналітичний опис впливу частоти електричних стимулів на режим скорочення скелетних м'язів, що дозволяє визначити індивідуальні оптимальні параметри електроміостимуляції.

Ключові слова: електростимуляція; скелетний м'яз; м'язове скорочення; моделювання; інтенсивність скорочення, частота стимулів.

Іл. 5. Бібліогр.: 15 назв.

УДК 616.833

Моделирование зависимости интенсивности электростимуляции от частоты следования стимулов / *И.В. Прасол, О.А. Ерошенко* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2022. Вып. 209. С. 192 – 199.

Объект исследования – процесс электростимуляции скелетных мышц человека в ходе лечебной терапии. Предмет изучения – математическая модель электростимуляционной характеристики, которая связывает амплитуду сокращения мышц и частоту стимулирующего воздействия. Цель работы – разработка математической модели в виде аналитического выражения для описания зависимости амплитуды мышечных сокращений от частоты электрических стимулов. Используемые методы: методы математического моделирования, методы структурной и параметрической идентификации моделей, методы аппроксимации, методы параметрической оптимизации, методы математического анализа. Полученные результаты: предложена аналитическая модель в форме полинома, которая отображает зависимость амплитуды сокращения мышц от частоты стимулов; выбрана степень полинома и получены коэффициенты модели путем параметрической оптимизации; построена модельная траектория и оценена точность моделирования; получено уравнение и найдены возможные его решения для определения оптимального значения частоты стимулов. Результаты могут быть использованы при подборе индивидуальных воздействий электростимуляции в течение одного сеанса или с экстраполяцией в течение ряда сеансов. Научная новизна: получено аналитическое описание влияния частоты электрических стимулов на режим сокращения скелетных мышц, что позволяет определить индивидуальные оптимальные параметры электромиостимуляции.

Ключевые слова: электростимуляция; скелетная мышца; мышечное сокращение; моделирование; интенсивность сокращения, частота стимулов.

Ил. 5. Библиогр.: 15 назв.

UDC 53.083.912

Evaluation of disorders of adaptive mechanisms in heart failure by microwave dielectrometry / *N.V. Khmil, V.G. Kolesnikov, O.L. Altuhov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2022. №209. P. 200 – 205.

Differential diagnosis of stress adaptive mechanisms is one of the areas of modern biomedical engineering and the most complex part of the pre-nosological diagnosis of cardiac pathology. One of the manifestations of disadaptation in heart failure is a violation of the mechanisms of realization of the intracellular chain "signal-function". The concept of imbalance in the functioning of the adenylate cyclase system and β-adrenergic receptors of the erythrocytes membrane and cardiomyocytes is considered in the pathogenesis of the heart.

The study of the dielectric constant (ε') of erythrocytes of patients with heart failure was performed using an instrument-recording complex based on microwave dielectrometry of the γ-dispersion region of free water dielectric permittivity. Testing of the β-adrenergic complex of the erythrocyte membrane by specific stimulators, blockers, and modulators was implemented at a fixed frequency of microwave radiofrequency generation (f = 37,7 GHz). Interpretation of the obtained experimental data was that the process of interaction of bioregulators with the biological system is accompanied by an increase or decrease in the relative amount of free water, which leads to a change in the real part of ε' complex dielectric constant. This allowed us to visualize the violation of the signal cell system at the molecular level, which manifested itself in the change of integral hydration by ε' parameter. It was shown that the change in the dielectric constant of the erythrocyte suspension at risk (patients with hereditary predisposition to dilated and ischemic cardiomyopathy) was significant relative to the dielectric parameters of erythrocyte samples from healthy donors; there was a tendency to block β-adrenergic receptors, with the combined action of adrenaline, PGE2 and cordanum, with $\Delta\varepsilon' = 0{,}009 \pm 0{,}008 \times 10^{-12}$ F/m. It should be noted the formation of preconditions for changes in the functioning of the adenylate cyclase system and the development of heart failure in the group at risk, is accompanied by dilated and ischemic cardiomyopathy.

The effectiveness of the microwave dielectrometry method for the assessment of violations of adaptation mechanisms through the adenylate cyclase system of the erythrocyte membrane in dilated and ischemic forms of cardiomyopathies is shown. The results of the study are the basis for the introduction of the dielectric constant criterion in the general algorithm of pre-nosological diagnosis of heart failure.

Key words: microwave dielectrometry; dielectric constant; prenosological diagnosis; erythrocytes; heart failure.

5 fig. Ref: 15 items.

УДК 53.083.912

Оцінка порушень адаптаційних механізмів при серцевій недостатності методом мікрохвильової діелектрометрії / *Н.В. Хміль, В.Г. Колесніков, О.Л. Алтухов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2022. Вип. 209. С. 200 – 205.

Диференціальна діагностика напруги адаптаційних механізмів є одним із напрямків сучасної біомедичної інженерії та найбільш складною частиною донозологічної діагностики серцевої патології. Одним із проявів дезадаптації при серцевій недостатності є порушення механізмів реалізації внутрішньоклітинного ланцюга

"сигнал-функція". У патогенезі серцевої недостатності розглядається концепція дисбалансу функціонування аденілатциклазної системи та β-адренорецепторів мембрани еритроцитів та кардіоміоцитів.

Проведено дослідження діелектричної проникності ε' еритроцитів хворих на серцеву недостатність за допомогою апаратурно-реєструючого комплексу на базі мікрохвильової діелектрометрії області γ-дисперсії діелектричної провідності вільної води. На фіксованій частоті генерації випромінювання НВЧ-діапазону радіохвиль (f = 37,7 ГГц) реалізовано тестування β-адренорецепторного комплексу мембрани еритроцитів специфічними стимуляторами, блокаторами та модуляторами. Інтерпретація отриманих експериментальних даних полягала в тому, що процес взаємодії біорегуляторів з біологічною системою супроводжується збільшенням або зменшенням відносної кількості вільної води, що призводить до зміни реальної частини комплексної діелектричної проникності ε'. Це дозволило візуалізувати порушення сигнальної клітинної системи на молекулярному рівні, що проявилося у зміні інтегральної гідратації за параметром ε'. Результати дослідження показали, що зміна діелектричної проникності суспензії еритроцитів групи ризику (пацієнти з спадковою схильністю до дилатаційної та ішемічної кардіоміопатії) була суттєвою відносно діелектричних параметрів зразків еритроцитів здорових донорів; спостерігалася тенденція до блокування β-адренорецепторів, при комбінованій дії адреналіну, ПГЕ2 та корданумуму, при цьому $\Delta\varepsilon' = 0{,}009 \pm 0{,}008 \times 10^{-12}$ Ф/м. Аналізуючи діелектричну проникність суспензії еритроцитів групи ризику, слід зазначити формування передумов до зміни в функціонуванні АЦС та розвитку серцевої недостатності, яку супроводжує дилатаційну та ішемічну кардіоміопатії. Показана ефективність методу мікрохвильової діелектрометрії для оцінки порушень адаптаційних механізмів через аденілатциклазну систему мембрани еритроцитів при дилатаційній та ішемічній формах кардіоміопатій. Результати дослідження є підґрунтям до впровадження критерію діелектричної проникності в загальний алгоритм донозологічної діагностики серцевої недостатності.

Ключові слова: мікрохвильова діелектрометрія; діелектрична проникність; донозологічна діагностика; еритроцити; серцева недостатність.

Іл. 5. Бібліогр.: 15 назв.

УДК 53.083.912

Оценка нарушений адаптационных механизмов при сердечной недостаточности методом микроволновой диэлектрометрии / *Н.В. Хмиль, В.Г. Колесников, А.Л. Алтухов* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2022. Вып. 209. С. 200 – 205.

Дифференциальная диагностика напряжения адаптационных механизмов является одним из направлений современной биомедицинской инженерии и наиболее сложной частью донозологической диагностики сердечной патологии. Одним из проявлений дезадаптации при сердечной недостаточности является нарушение механизмов реализации внутриклеточной цепи "сигнал-функция". В сердечном патогенезе рассматривается концепция дисбаланса функционирования аденилатциклазной системы и β-адренорецепторов мембраны эритроцитов и кардиомиоцитов.

Проведено исследование диэлектрической проницаемости ε' эритроцитов больных сердечной недостаточностью с помощью аппаратурно-регистрирующего комплекса на базе микроволновой диэлектрометрии области γ-дисперсии диэлектрической проводимости свободной воды. На фиксированной частоте генерации излучения СВЧ-диапазона радиоволн (f = 37,7 ГГц) реализовано тестирование β-адренорецепторного комплекса мембраны эритроцитов специфическими стимуляторами, блокаторами и модуляторами. Интерпретация полученных экспериментальных данных заключалась в том, что процесс взаимодействия биорегуляторов с биологической системой сопровождается увеличением или уменьшением относительного количества свободной воды, что приводит к изменению реальной части комплексной диэлектрической проницаемости ε'. Это позволило визуализировать нарушение сигнальной клеточной системы на молекулярном уровне, что проявилось в изменении интегральной гидратации по параметру ε'. Результаты исследования показали, что изменение диэлектрической проницаемости суспензии эритроцитов группы риска (пациенты с наследственной склонностью к дилатационной и ишемической кардиомиопатии) было существенным относительно диэлектрических параметров образцов эритроцитов здоровых доноров; наблюдалась тенденция к блокированию β-адренорецепторов, при комбинированном действии адреналина, ПГЭ2 и кордана, при этом $\Delta\varepsilon' = 0{,}009 \pm 0{,}008$ x 10-12 Ф/м. Анализируя диэлектрическую проницаемость суспензии эритроцитов группы риска, следует отметить формирование предпосылок к изменению в функционировании АЦС и развитию сердечной недостаточности, сопровождающейся дилатационной и ишемической кардиомиопатией. Показана эффективность метода микроволновой диэлектрометрии для оценки нарушений адаптационных механизмов через аденилатциклазную систему мембраны эритроцитов при дилатационной и ишемической формах кардиомиопатии. Результаты исследования являются основанием для внедрения критерия диэлектрической проницаемости в общий алгоритм донозологической диагностики сердечной недостаточности.

Ключевые слова: микроволновая диэлектрометрия; диэлектрическая проницаемость; донозологическая диагностика; эритроциты; сердечная недостаточность.

Ил. 5. Библиогр.: 15 назв.

RELATED PROBLEMS OF RADIO ENGINEERING
СУМІЖНІ ПРОБЛЕМИ РАДІОТЕХНІКИ
СМЕЖНЫЕ ПРОБЛЕМЫ РАДИОТЕХНИКИ

UDC 621.7.075

Modeling a screw extruder for FFF 3D printing / *I. Razumov-Fryziuk, D. Gurin, D. Nikitin, R. Strilets, D. Blyzniuk* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2022. №209. P. 206 – 214.

The article presents the development and modeling of a screw extruder for 3D printers operating on the FFF technology, namely, the Fused Filament Fabrication ("production by fusing threads"). Extruders, usually installed on FFF 3D printers, use a thermoplastic polymer filament as a material. There are two filament standards: 1.75mm and 2.85mm. The minimum cost of such a filament starts from $ 11 per kilogram (ABS plastic 1.75 mm). The cost of more expensive filaments can reach several thousand or even tens of thousands per kilogram (depending on the material, filler, the presence of inhibitors, dyes, etc.). The cost of the material is much higher than granulated primary plastics and even more so recycled materials. In addition, the extruder nozzle diameter is typically limited to 1.2mm for 1.75mm filament. Thus, when printing large products, for which the detail and roughness of vertical surfaces are not so important, increase in the diameter of the extruder nozzle will increase significantly the printing speed due to the increase in the thickness of the print layer and the width of the print line.

To produce filament, screw filament extruders are used, which work on the principle of injection molding machines. The authors propose a calculation of the parameters of a screw extruder for an FFF 3D printer, which will directly use granulated primary plastics or crushed plastic recyclables as a material. The use of a screw extruder will reduce the cost of the printed product and increase significantly the diameter of the extruder nozzle, which will significantly reduce the production time for large-sized products.

When designing a screw extruder, it is necessary to adhere to two main strategies: minimizing the weight and size parameters of the extruder and ensuring the required linear productivity. On the one hand, the extruder must be as light as possible to be able to increase the printing speed, on the other hand, it must provide the necessary linear performance to be able to extrude plastic at printing speeds. Modeling is made for nozzles with a diameter of 1mm and 5mm. According to the calculation results, the screw extruder has a 3-fold and 37-fold margin of linear productivity, respectively.

Key words: extruder; screw; 3D printer; additive technologies.

1 tab. 5 fig. Ref: 10 items.

УДК 621.7.075

Моделювання шнекового екструдера для FFF 3D друку / *Є.А. Разумов-Фризюк, Д.В. Гурін, Д.О. Нікітін, Р.Є. Стрілець, Д.С. Близнюк* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2022. Вип. 209. С. 206 – 214.

Представлено розробку та моделювання шнекового екструдера для 3D принтерів, що працюють за технологією FFF – Fused filament fabrication («виробництво способом наплавлення ниток»). Екструдери, які зазвичай встановлюються на FFF 3D принтерів, використовують як матеріал термопластичну полімерну нитку – філамент. Існує два стандарти філаменту 1,75мм та 2,85мм. Мінімальна вартість подібного філаменту починається від 11 $ за кілограм (ABS пластик 1,75 мм). Вартість дорожчих філаментів може досягати кількох тисяч і навіть десятків тисяч за кілограм (залежно від матеріалу, наповнювача, наявності інгібіторів, барвників тощо). Вартість матеріалу значно вище гранульованих первинних пластиків і тим більше вторинної сировини. Крім того, діаметр сопла екструдера, зазвичай, обмежується значенням 1,2 мм для філаменту 1,75 мм. Таким чином, при друкуванні великих виробів, для яких деталізація і шорсткість вертикальних поверхонь не настільки важливі, збільшення діаметра сопла екструдера значно збільшить швидкість друку через збільшення товщини шару друку і ширини лінії друку.

Для виробництва філаменту застосовуються шнекові екструдери філаменту, які працюють за принципом термопласт-автоматів. Автори пропонують розрахунок параметрів шнекового екструдера для FFF 3D принтера, який безпосередньо використовуватиме як матеріал гранульовані первинні пластики або подрібнену пластикову вторсировину. Застосування шнекового екструдера знизить собівартість друкованого виробу, а також дозволить значно збільшити діаметр сопла екструдера, що значно знизить час виробництва великогабаритних виробів.

При проєктуванні шнекового екструдера необхідно дотримуватися двох основних стратегій: мінімізації масогабаритних параметрів екструдера та забезпечення необхідної лінійної продуктивності. З одного боку, екструдер повинен бути максимально легким для збільшення швидкості друку, з іншого – він повинен забезпечити необхідну лінійну продуктивність для можливості екструзії пластику на швидкостях друку. Моделювання зроблено для сопел діаметром 1 та 5мм. За результатами розрахунків шнековий екструдер має трьохкратний і 37-кратний запас лінійної продуктивності відповідно.

Ключові слова: екструдер; шнек; 3D принтер; адитивні технології.

Табл. 1. Іл.5. Бібліогр.: 10 назв.

УДК 621.7.075

Моделирование шнекового экструдера для FFF 3D печати / *Е.А. Разумов-Фризюк, Д.В. Гурин, Д.О. Никитин, Р.Е Стрелец, Д.С. Близнюк* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2022. Вып. 209. С. 206 – 214.

Представлена разработка и моделирование шнекового экструдера для 3D принтеров, работающих по технологии FFF – Fused filament fabrication («производство способом наплавления нитей»). Экструдеры, которые обычно устанавливаются на FFF 3D принтеров, используют в качестве материала термопластичную полимерную нить – филамент. Существует два стандарта филамента 1,75 и 2,85 мм. Минимальная стоимость подобного филамента начинается от 11$ за килограмм (ABS пластик 1,75 мм). Стоимость более дорогих филаментов может достигать нескольких тысяч и даже десятков тысяч за килограмм (в зависимости от материала, наполнителя, наличия ингибиторов, красителей и т.д.). Стоимость материала значительно выше гранулированных первичных пластиков и тем более вторсырья. Кроме того, диаметр сопла экструдера, как правило, ограничивается значением 1,2 мм для филамента 1,75 мм. Таким образом, при печати больших изделий, для которых детализация и шероховатости вертикальных поверхностей не столь важны, увеличение диаметра сопла экструдера значительно увеличит скорость печати из-за увеличения толщины слоя печати и ширины линии печати.

Для производства филамента применяются шнековые экструдеры филамента, которые работают по принципу термопласт-автоматов. Авторы предлагают расчет параметров шнекового экструдера для FFF 3D принтера, который будет напрямую использовать в качестве материала гранулированные первичные пластики либо измельченное пластиковое вторсырье. Применение шнекового экструдера снизит себестоимость печатаемого изделия, а также позволит значительно увеличить диаметр сопла экструдера, что значительно снизит время производства крупногабаритных изделий.

При проектировании шнекового экструдера необходимо придерживаться двух основных стратегий: минимизации массогабаритных параметров экструдера и обеспечения необходимой линейной производительности. С одной стороны, экструдер должен быть максимально легким для возможности увеличения скорости печати, с другой – он должен обеспечить необходимую линейную производительность для возможности экструзии пластика на скоростях печати. Моделирование произведено для сопел диаметром 1 и 5 мм. По результатам расчетов шнековый экструдер имеет трехкратный и 37-кратный запас линейной производительности соответственно.

Ключевые слова: экструдер; шнек; 3D принтер; аддитивные технологии.

Табл. 1. Ил.5. Библиогр.: 10 назв.

UDC 621.317

Improvement of spectroscopic method for determining refractive index of filament sample material for 3D printing in terahertz range / *Yu.Ye. Khoroshailo, N.Ya. Zaichenko, O.B. Zaichenko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2022. №209. P. 215 – 225.

The article considers the topical problem of non-destructive filament defectoscopy for 3D printing. The subject of the research is the process of determining the refractive index of the filament material for 3D printing taking into account the reflections from sample opposite walls, which is studied by terahertz spectroscopy in the time domain. Reflections from opposite walls are called the Fabry-Perot effect, and interference members resulting from reflections from walls are traditionally taken into account by summation and represented as a series. The disadvantage of the model in the form of a simple summation is the rejection of the members of the series above the fourth, which leads to inaccuracies in the model. The main problem with terahertz spectroscopy and this study in particular is the contradiction between the rapid development of terahertz spectroscopy and the slow development of models used in terahertz spectroscopy, while the adjacent microwave region has a set of ready-made models. Models based on the description of a standing wave in the microwave tract with refinements, transferred to a new region of terahertz spectroscopy in the time domain. The scientific novelty lies in increasing accuracy by taking into account previously unaccounted for interference members. The analogy between the Fabry-Perot effect used in terahertz spectroscopy and the reflections in a microwave multiprobe multimeter suggested the following recommendations. First, because the phase distance between the sensors in the microwave multimeter is similar to the thickness of the sample in terahertz spectroscopy, therefore, there was choosen such a sample thickness that the interference members are compensated, and secondly, instead of simple sum up it is possibility apply algorithmic processing, the condition for this is the existence in addition to the main signal in the time domain of the recorded echo signals of much smaller amplitude, therefore, one can build a system of equations and by solving it to determine the desired refractive index parameters of the filament sample material.

Key words: method; spectroscopy; coefficient; refraction; terahertz; effect; Fabry Perot; model; interference; number; compensation; system of equations.

7 fig. Ref: 16 items.

УДК 621.317

Удосконалення спектроскопічного методу визначення коефіцієнта заломлення матеріалу зразка філаменту для 3D друку в терагерцевому діапазоні / *Ю.Є. Хорошайло, Н.Я. Зайченко, О.Б. Зайченко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2022. Вип. 209. С. 215 – 225.

Основною проблемою терагерцової спектроскопії та даного дослідження зокрема є протиріччя між швидким розвитком засобів терагерцової спектроскопії та відставанням моделей, що використовуються у терагерцевій спектроскопії, тоді як сусідня мікрохвильова область має набір готових моделей. У статті розглянуто актуальну проблему неруйнівної дефектоскопії філаменту для 3D друку. Предметом дослідження є процес визначення коефіцієнта заломлення матеріалу філаменту для 3D друку з урахуванням перевідбиттів від протилежних стінок, що досліджується методом терагерцової спектроскопії у часовій області. Перевідбиття від протилежних стінок називаються ефектом Фабрі – Перро, при цьому інтерференційні члени, що виникли через перевідбиття від стінок, традиційно враховуються додаванням і представляються у вигляді ряду. Недоліком моделі у вигляді простого додавання є відкидання членів ряду вище за четвертий, що призводить до неточностей моделі. Моделі, побудовані на описі стоячої хвилі в мікрохвильовому тракті з уточненнями, перенесені на нову область терагерцовой спектроскопії в часовій області. Наукова цінність полягає у підвищенні точності за рахунок обліку раніше неврахованих інтерференційних членів. Аналогія між ефектом Фабрі – Перро, що використовується в терагерцевій спектроскопії, з перевідбиттями в мікрохвильовому багатозондовому мультиметрі дозволила запропонувати такі рекомендації. По-перше, оскільки фазова відстань між датчиками в мікрохвильовому мультиметрі подібна до товщини досліджуваного зразка в терагерцовій спектроскопії, отже, можна підібрати таку товщину зразка, щоб інтерференційні члени компенсувалися, по-друге, можна просте підсумовування сигналів на виході зі зразка замінити алгоритмічною обробкою, умовою для цього є існування крім основного сигналу в часовій області реєстрованих сигналів відлуння значно меншої амплітуди, отже, можна побудувати систему рівнянь і шляхом її вирішення визначити шукані параметри коефіцієнта заломлення матеріалу зразка філаменту.

Ключові слова: метод; спектроскопія; коефіцієнт; заломлення; терагерц; ефект; Фабрі – Перро; модель; інтерференція; ряд; компенсація; система рівнянь.

Іл. 7. Бібліогр.: 16 назв.

УДК 621.317

Усовершенствование спектроскопического метода определения коэффициента преломления материала образца филамента для 3D печати в терагерцовом диапазоне / *Ю.Е. Хорошайло, Н.Я. Зайченко, О.Б. Зайченко* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2022. Вып. 209. С. 215 – 225.

Основной проблемой терагерцовой спектроскопии и данного исследования в частности является противоречие между быстрым развитием средств терагерцовой спектроскопии и отставанием моделей, используемых в терагерцовой спектроскопии, в то время как соседняя микроволновая область имеет набор готових моделей. В статье рассмотрена актуальная проблема неразрушающей дефектоскопии филамента для 3D печати. Предметом исследования является процесс определения коэффициента преломления материала филамента для 3D печати с учетом переотражения от противоположных стенок, исследуемый методом терагерцовой спектроскопи во временной области. Переотражения от противоположных стенок называются эффектом Фабри – Перро, при этом интерференционные члены, возникшие из-за переотражений от стенок, традиционно учитываются суммированием и представляются в виде ряда. Недостатком модели в виде простого суммирования является отбрасывание членов ряда выше четвертого, что приводит к неточностям модели. Модели, построенные на описании стоячей волны в микроволновом тракте, с оговорками перенесены на новую область терагерцовой спектроскопии во временной области. Научная ценность состоит в повышении точности за счет учета ранее неучтенных интерференционных членов. Аналогия между эффектом Фабри – Перро, используемым в террагерцовой спектроскопии с переотражениями в микроволновом многозондовом мультиметре, позволила предложить такие рекомендации. Во-первых, поскольку фазовое расстояние между датчиками в микроволновом мультиметре подобно толщине исследуемого образца в терагерцовой спектроскопии, следовательно, можно подобрать такую толщину образца, чтобы интерференционные члены компенсировались, во-вторых, можно простое суммирование сигналов на выходе из образца заменить алгоритмической обработкой. Предпосылкой для этого является существование помимо основного сигнала во временной области также регистрируемых сигналов эха значительно меньшей амплитуды, значит, можно построить систему уравнений и путем ее решения определить искомые параметры коэффициента преломления материала образца филамента.

Ключевые слова: метод; спектроскопия; коэффициент; преломление; терагерц; эффект; Фабри – Перро; модель; интерференция; ряд; компенсация; система уравнений.

Ил. 7. Библиогр.: 16 назв.

UDC 655.3.022

Study of color reproduction features at “Nargus” LLC / *O.V. Vovk, I.B. Chebotarova, D.V. Polenok* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2022. №209. P. 226 – 238.

The features of color recreation were studied at “Nagrus” LLC. For this, the quality control process at the enterprise and the statistics of rejects and the reasons for their occurrence were analyzed; the features of the use of inks in the process of flexo printing were considered and the stages of ink preparation for printing were described. The main factors that affect the quality of products at the stage of prepress and during the process of manufacturing flexo plates were also found.

The process of preparing pantone colors for printing a run was analyzed; a table of dependence of pantone deviations on various materials was created; a technique has been developed to increase the speed of paint selection and rec-

ommendations regarding its application. Factors that have the greatest influence on the quality of a flexographic plate during its manufacture were found, and a technique for the optimal choice of plates for non-absorbent materials was developed.

.

Key words: color; flexoprinting; paint; panton; photopolymer flexo form; MAH.

3 tab. 3 fig. Ref: 9 items.

УДК 655.3.022

Дослідження особливостей кольоровідтворення на підприємстві ТОВ «Наргус» / *О.В. Вовк, І.Б. Чеботарьова, Д.В. Поленок* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2022. Вип. 209. С. 226 – 238.

Досліджено особливості відтворення кольору на підприємстві ТОВ «Наргус». Для цього проаналізовано процес контролю якості на підприємстві та статистику браку та причини його виникнення; розглянуто особливості використання фарб в процесі флексодруку та описані етапи підготовки фарби до друку. Також виявлено основні фактори, що впливають на якість продукції на етапі додрукарської підготовки та під час процесу виготовлення флексоформ.

Проаналізовано процес підготовки пантонних кольорів до друку тиражу; створено таблицю залежності відхилень пантонів на різноманітних матеріалах; розроблено методику підвищення швидкості підбору фарби та рекомендації щодо її застосування. Виявлено чинники, які надають найбільший вплив на якість флексографської форми під час її виготовлення, та розроблено методику оптимального вибору формних пластин для невбираючих матеріалів.

Ключові слова: колір; флексодрук; фарба; пантон; фотополімерна флексографська форма; MAI.

Табл. 3. Іл. 3. Бібліогр.: 9 назв.

УДК 655.3.022

Исследование особенностей цветовоспроизведения на предприятии ООО «Наргус» / *А.В. Вовк, И.Б. Чеботарёва, Д.В. Поленок* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2022. Вып. 209. С. 226 – 238.

Исследованы особенности воссоздания цвета на предприятии ООО «Наргус». Для этого проанализированы процесс контроля качества на предприятии и статистика брака и причины его возникновения; рассмотрены особенности использования красок в процессе флексопечати и описаны этапы подготовки краски к печати. Также обнаружены основные факторы, которые влияют на качество продукции на этапе допечатной подготовки и во время процесса изготовления флексоформ.

Проанализирован процесс подготовки пантонных цветов к печати тиража; создана таблица зависимости отклонений пантонов на разнообразных материалах; разработана методика повышения скорости подбора краски и рекомендации относительно ее приложения. Обнаруженные факторы, которые предоставляют наибольшее влияние на качество флексографской формы во время ее изготовления, и разработана методика оптимального выбора формных пластин для невпитывающих материалов.

Ключевые слова: цвет; флексопечать; краска; пантон; фотополимерная флексографская форма; МАИ.

Табл. 3. Ил.3. Библиогр.: 9 назв.

UDC 621.391:519.246.8

Model for estimating statistical characteristics of the pre-stroke warehouse process based on average monthly temperatures analysis / *V.A. Tikhonov, V.M. Kartashov, O.V. Kartashov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2022. №209. P. 239 – 245.

The possibilities of an improved autoregression model and an integrated moving average (ARMAS) for the analysis of non-stationary data and the identification of long-term trends in the processes under study are considered. The proposed model can be used to study the observed processes in various areas of human activity: the analysis of the observed trajectories of the movement of aircraft, in particular unmanned aerial vehicles, meteorological processes that reflect the state of the atmosphere. The mathematical apparatus developed in the article was used to analyze changes in the atmospheric temperature time series observed for a long time, the average annual temperatures were estimated, followed by sliding smoothing with a low-frequency filter.

It is shown that the removal of the seasonal component in the ARPSS model eliminates or distorts significantly the trend and has little effect on the stationary component of the ARPSS process. The operation of de-trending has little effect on the properties of the seasonal component and the stationary component of the process. To assess the trend, the mean annual temperatures were preliminarily obtained. The use of moving averaging, which removes the seasonal component from the average monthly temperatures, makes it possible to find a weak long-term trend. The results obtained in the work can be used to analyze medium-term and long-term changes in atmospheric phenomena, to refine the results obtained by traditional methods of processing results and methods of mathematical statistics, as well as in other areas of human activity.

Key words: non-stationary processes; model, autoregression; moving average; long-term trends; temperature; trajectory; seasonal component.

8 fig. Ref: 15 items.

УДК 621.391:519.246.8

Модель оцінювання статистичних характеристик довгострокової складової випадкового процесу на прикладі аналізу середньомісячних температур / *В.А. Тихонов, В.М. Карташов, О.В. Карташов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2022. Вип. 209. С. 239 – 245.

Розглянуто можливості вдосконаленої моделі авторегресії та проінтегрованого ковзного середнього (АРПКС) для аналізу нестаціонарних даних та виділення довгострокових трендів досліджуваних процесів. Запропонована модель може бути використана для дослідження спостережуваних процесів у різних галузях людської діяльності: аналізу траєкторій руху літальних апаратів, що спостерігаються, зокрема безпілотних літальних апаратів, метеорологічних процесів, що відображають стан атмосфери. Розроблений математичний апарат використовувався для аналізу змін у тимчасових рядах температури атмосфери, що спостерігаються тривалий час, проведено оцінювання середньорічних температур з подальшим ковзним згладжуванням низькочастотним фільтром.

Показано, що видалення сезонної складової моделі АРПКС усуває або суттєво спотворює тренд і слабко впливає на стаціонарну складову процесу АРПКС. Операція видалення тренду слабко впливає на властивості сезонної складової і стаціонарну складову процесу. Для оцінки тренду попередньо було отримано середньорічні значення температур. Використання ковзного усереднення, що видаляє сезонну складову середньомісячних температур, дозволяє знайти слабкий довготривалий тренд. Отримані результати можуть використовуватися для аналізу середньострокових та довгострокових змін атмосферних явищ, уточнення результатів, одержаних традиційними методами обробки результатів та методами математичної статистики, а також в інших сферах людської діяльності.

Ключові слова: нестаціонарні процеси; модель; авторегресія; ковзна середня; довгострокові тренди; температура; траєкторія; сезонна складова.

Іл. 8. Бібліогр.: 15 назв.

УДК 621.391:519.246.8

Модель оценивания статистических характеристик долгосрочной составляющей случайного процесса на примере анализа среднемесячных температур / *В.А. Тихонов, В.М. Карташов, А.В. Карташов* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2022. Вып. 209. С. 239 – 245.

Рассмотрены возможности усовершенствованной модели авторегрессии и проинтегрированного скользящего среднего (АРПСС) для анализа нестационарных данных и выделения долгосрочных трендов исследуемых процессов. Предложенная модель может быть использована для исследования наблюдаемых процессов в различных областях человеческой деятельности: анализа наблюдаемых траекторий движения летательных аппаратов, в частности беспилотных летательных аппаратов, метеорологических процессов, отображающих состояние атмосферы. Разработанный математический аппарат использовался для анализа изменений в наблюдаемых длительное время временных рядах температуры атмосферы, произведено оценивание среднегодовых температур с последующим скользящим сглаживанием низкочастотным фильтром.

Показано, что удаление сезонной составляющей в модели АРПСС устраняет или существенно искажает тренд и слабо воздействует на стационарную составляющую процесса АРПСС. Операция удаления тренда слабо влияет на свойства сезонной составляющей и на стационарную составляющую процесса. Для оценки тренда предварительно были получены среднегодовые значения температур. Использование скользящего усреднения, удаляющего сезонную составляющую из среднемесячных температур, позволяет найти слабый долговременный тренд. Полученные результаты могут использоваться для анализа среднесрочных и долгосрочных изменений атмосферных явлений, уточнения результатов, полученных традиционными методами обработки результатов и методами математической статистики, а также в других областях человеческой деятельности.

Ключевые слова: нестационарные процессы; модель; авторегрессия; скользящее среднее; долгосрочные тренды; температура; траектория; сезонная составляющая.

Ил. 8. Библиогр.: 15 назв.

COLLECTION OF SCIENTIFIC PAPERS
RADIOTEKHNIKA
Issue 209
In English and Ukrainian

ЗБІРНИК НАУКОВИХ ПРАЦЬ
РАДІОТЕХНІКА
Випуск 209
Англійською та українською мовами

СБОРНИК НАУЧНЫХ ТРУДОВ
РАДИОТЕХНИКА
Выпуск 209
На английском и украинском языках

Коректор Л.І. Сащенко

Підп. до друку 30.06.2022. Формат 60x90/8. Папір офсет. Гарнітура Таймс. Друк. ризограф.
Ум. друк. арк**.** 13,4. Обл.-вид. арк. 12,3. Тираж 300 прим. Зам. № 485. 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.