

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 2 3

Kharkiv
Kharkiv National
University of Radio Electronics
2025

UDC 621.3

The collection is included in the List of scientific professional publications of Ukraine, category «Б», technical and physical-mathematical sciences (approved by orders of the Ministry of Education and Science from 17.03.2020 № 409; from 02.07.2020 № 886; from 24.09.2020 № 1188) by specialties: 105 – Applied Physics and Nanomaterials; 125 – Cybersecurity and information protection; 163 – Biomedical Engineering; 171 – Electronics; 172 – Electronic communications and Radio Engineering; 173 – Avionics; 174 –Automation and Computer-Integrated Technologies and Robotics; 175 – Metrology and information-measuring technique; 176 – Micro- and Nanosystem Technology.

Website: rt.nure.ua

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

The authors are responsible for the content of the article.

Editorial Team

S.O. Sheiko, 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. Gretsikh, *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
Ye.V. Kotukh, PhD, Assoc. prof., Dnipro UT, Ukraine
A.S. Kulik, *Dr. Sc. (Tech.), prof.*, NAU «KhAI», 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
I.V. Svyd, *PhD, Assoc. prof.*, KNU, Ukraine
V.V. Semenets, *Dr. Sc. (Tech.), prof.*, NURE, Ukraine
S.I. Tarapov, *Dr. Sc. (Phys.-Math.), prof.*, member-cor. NASU, IRE NASU, 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.), 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*), Irena Vorgul (*United Kingdom*), Waldemar Wójcik (*Польша*).

Responsible for the issue: S.O. Sheiko, 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 № 12 dated 24.12.2025.

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

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

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 2 3

Харків
Харківський національний
університет радіоелектроніки
2025

УДК 621.3

Збірник включено до Переліку наукових фахових видань України, категорія "Б", технічні та фізико-математичні науки (затверджено наказами МОНУ від 17.03.2020 № 409; від 02.07.2020 № 886; від 24.09.2020 № 1188) за спеціальностями: 105 – Прикладна фізика та наноматеріали; 125 – Кібербезпека та захист інформації; 163 – Біомедична інженерія; 171 – Електроніка; 172 – Електронні комунікації та радіотехніка; 173 – Авіоніка; 174 – Автоматизація, комп'ютерно-інтегровані технології та робототехніка; 175 – Метрологія та інформаційно-вимірні технології; 176 – Мікро- та наносистемна техніка.

Сайт: rt.nure.ua

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

За зміст статті відповідальні автори.

Редакційна колегія

С.О. Шейко, *к.т.н., доц., ХНУРЕ, Україна (головний редактор)*
О.Г. Аврунін, *д.т.н., проф., ХНУРЕ, Україна*
Д.В. Агеев, *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*
Є.В. Котух, *к.т.н., доц., НТУ «Дніпровська Політехніка», Україна*
А.С. Кулік, *д.т.н., проф., НАУ ім. М.Є. Жуковського «ХАІ», 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*
І.В. Свид, *к.т.н., доц., ХНУ, Україна*
В.В. Семенець, *д.т.н., проф., ХНУРЕ, Україна*
С.І. Тарапов, *д.ф.-м.н., проф., член-кор. НАНУ, ІРЕ НАНУ, 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., проф., ХНУРЕ, Україна*

Міжнародна редакційна колегія

Boris Chichkov (*Німеччина*), Marianna Ivashina (*Швеція*), Konstyantyn Markov (*Німеччина*),
Georgiy Sevskiy (*Німеччина*), Larysa Titarenko (*Польща*), Vitaliy Zhurbenko (*Данія*),
Irena Vorgul (*United Kingdom*), Waldemar Wójcik (*Польща*).

Відповідальні за випуск: С.О. Шейко, *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 № 12 від 24.12.2025.

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

Використання матеріалів можливе лише за згодою редколегії.

CONTENT

SYSTEMS AND METHODS OF INFORMATION PROTECTION

<i>Y.O. Lohachova, M.V. Yesina, D.Yu. Holubnychyi</i> Assessment of the effectiveness of international standards and regulatory acts governing artificial intelligence models for Ukraine	7
<i>Ya.A. Derevianko D.Yu. Gorbenko</i> Theoretical justification and practical implementation of entropy extractors based on national cryptographic algorithms	18
<i>K.E. Lysytskyi, I.V. Lysytska, I.M. Galtseva, E.P. Kolovanova</i> Evolution of architectures of block symmetric ciphers	31
<i>R.I. Mordvinov</i> Systematization of Zero-Knowledge Proof Methods	38
<i>V.I. Zabolotny, Y.M. Holoborodko, D.M. Zabolotny, D.O. Abrosymov</i> Quantitative model of passive speech information concealment means using the nonlinear attenuators	44
<i>P.V. Shulik, Ph.D., D.S. Balagura, Ph.D., V.V. Prosolov, D.O. Viukhin</i> Creating information security systems based on open portable trusted execution environment (OP-TEE), KVM/QEMU intel trust domain extensions	51
<i>S.Ya. Hilgurt, L.V. Kovalchuk, A.M. Davydenko</i> Overview of approaches to building secure, interference-resistant streaming video transmission systems for UAV	57
<i>I.V. Oleshko, V.I. Lutsenko, O.Y. Petrenko, O.A. Melnykova</i> Evaluation of the Effectiveness of AI-Based Attacks on Fingerprint Biometric Authentication Systems	66
<i>O.I. Fediushyn, P.V. Shulik, V.V. Prosolov, D.O. Viukhin, O.V. Chechui</i> Using Deep Learning Methods for Visualization and Detection of Malware	75
<i>A.A. Telnova, T.O. Hrinenko, O.P. Nariezhnii</i> Analysis of the resistance of post-quantum digital signature algorithms FULLECA, WAVE, BISCUIT, and RYDE	85
<i>T.I. Korobeinikova, N.V. Kravchuk</i> ML-WAF Information Technology for Classification and Blocking of Injection Attacks in a Containerized Web Environment	100
<i>M.O. Yevdokymenko, V.Kh. Chakryan, V.V. Yevdokymenko</i> Ethical principles and normative regulation of professional activity in cybersecurity: international standards, Ukrainian context, and practical guidelines	111
<i>Y.V. Kotukh</i> Unified cryptographic coprocessor architecture for post-quantum cryptography in 6G network equipment	121

RADIO-ELECTRONIC AND INFORMATION SYSTEMS

<i>L.I. Melnikova, O.V. Linnyk, S.V. Shtangei</i> Hierarchical clustering using a Kohonen neural network for secured wireless sensor networks	126
<i>V.M. Bezruk, Y.M. Holoborodko, V.I. Zabolotny</i> Detection of New Radio Emissions in Automated Radio Monitoring	133
<i>I.O. Romanenko, A.L. Yalovets</i> Critical analysis of known missile guidance methods	138

BIOMEDICAL ENGINEERING

<i>A. A. Sokolov, O. G. Avrunin, Ya.V. Nosova, T.V. Nosova</i> Evaluation of the effectiveness of distance determination using the ARCore framework in low-light conditions	144
<i>S.O. Filimonov, L.O. Averianova</i> Simulation of a slice phantom of human vertebra trabecular tissue for the study of its CT reconstruction	151

PHYSICS OF DEVICES, ELEMENTS AND SYSTEMS

<i>O.D. Menyailo, O.V. Grigorieva, V.G. Makhonin</i> Optimization of fluctuating power of diesel generators used in avionics systems	157
<i>I.M. Bondarenko, O.S. Hnatenko, A.V. Gritsunov, O.G. Pashchenko, H.M. Bendeberia, M.A. Kopot, S.V. Hryshkov</i> Spectral Simulation of Mode Competition in a Magnetron with an Essential Influence of Space Charge	163
<i>D.V. Sliusar, O.M. Chugai, I.V. Kolodiy, S.V. Oliynyk, O.O. Poluboiarov, Y.A. Voloshyn, S.M. Kulish</i> Composition, structure and microhardness of multicomponent tungsten carbide based coatings formed using the inverse magnetron sputtering system	172
<i>P.V. Trofimov</i> BLDC motor control systems analysis	178

ABSTRACTS	194
-----------	-----

ЗМІСТ

СИСТЕМИ І МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ

<i>Є.О. Логачова, М.В. Єсіна, Д.Ю. Голубничий</i> Оцінка ефективності застосування міжнародних стандартів та регуляторних актів з регулювання моделей штучного інтелекту для України	7
<i>Я.А. Дерев'янка, Д.Ю. Горбенко</i> Теоретичне обґрунтування та практична реалізація екстракторів ентропії на основі національних криптографічних алгоритмів	18
<i>К.Є. Лисицький, І.В. Лисицька, І.М. Гальцева</i> Еволюція архітектур блокових симетричних шифрів	31
<i>Р.І. Мордвінов</i> Систематизація методів доказу з нульовим розголошенням	38
<i>В.І. Заболотний, Ю.М. Голобородько, Д.М. Заболотний, Д.О. Абросімов</i> Кількісна модель засобів пасивного приховування мовної інформації нелінійними атенюаторами	44
<i>П.В. Шулік, Д.С. Балагура, В.В. Просолов, Д.О. В'юхін</i> Створення систем захисту інформації на базі open portable trusted execution environment (op-tee), kvm/qemu та intel trust domain extensions	51
<i>С.Я. Гільгурт, Л.В. Ковальчук, А.М. Давиденко</i> Огляд підходів до побудови захищених завадостійких систем передачі потокового відео з БпЛА	57
<i>І.В. Олешко, В.І. Луценко, О.Є. Петренко, О.А. Мельникова</i> Оцінка ефективності атак з використанням штучного інтелекту на системи біометричної автентифікації за відбитками пальців	66
<i>О.І. Федюшин, П.В. Шулік, В.В. Просолов, Д.О. В'юхін, О.В. Чечуй</i> Використання методів глибокого навчання для візуалізації та виявлення шкідливого програмного забезпечення	75
<i>А.А. Тельнова, Т.О. Грінченко, О.П. Нарезжній</i> Аналіз стійкості алгоритмів пост квантового цифрового підпису FULEECA, WAVE, BISCUIT TA RYDE	85
<i>Т.І. Коробейнікова, Н.В. Кравчук</i> Інформаційна технологія ML-WAF для класифікації та блокування ін'єкційних атак у контейнеризованому веб-середовищі	100
<i>М.О. Євдокименко, В.Х. Чакрян, В.В. Євдокименко</i> Етичні засади та нормативне регулювання професійної діяльності в сфері кібербезпеки: міжнародні стандарти, український контекст і практичні орієнтири	111
<i>Є.В. Котух</i> Щодо уніфікованої архітектури криптографічного копроцесора для постквантової криптографії в обладнанні мереж 6G (англ.)	121

РАДІОЕЛЕКТРОННІ ТА ІНФОРМАЦІЙНІ СИСТЕМИ

<i>Л.І. Мельнікова, О.В. Лінник, С.В. Штангей</i> Ієрархічна кластеризація для безпечної комунікації в сенсорних мережах з нейромережею Кохонена (англ.)	126
<i>В.М. Безрук, Ю.М. Голобородько, В.І. Заболотний</i> Виявлення нових радіовипромінювань при автоматизованому радіоконтролі	133
<i>І.О. Романенко, А.Л. Яловець</i> Критичний аналіз відомих методів наведення ракет	138

БІОМЕДИЧНА ІНЖЕНЕРІЯ

<i>А.А. Соколов, О.Г. Аврунін, Я.В. Носова, Т.В. Носова</i> Оцінка ефективності визначення відстані засобами фреймворку ARCore в умовах низького освітлення	144
<i>С.О. Філімонов, Л.О. Авер'янова</i> Моделювання фантома зрізу трабекулярної тканини хребця людини для дослідження його КТ-реконструкції	151

ФІЗИКА ПРИЛАДІВ, ЕЛЕМЕНТІВ І СИСТЕМ

<i>О.Д. Меняйло, О.В. Григор'єва, В.Г. Махонін</i> Оптимізація флуктуаційних властивостей діодних генераторів вбудованих систем авіоніки	157
<i>І.М. Бондаренко, О.С. Гнатенко, О.В. Грицунов, О.Г. Пащенко, Г.М. Бендеберя, М.А. Копоть, С.В. Гришков</i> Спектральне моделювання конкуренції видів коливань в магнетроні з суттєвим впливом просторового заряду	163
<i>Д.В. Слюсар, О.М. Чугай, І.В. Колодій, С.В. Олійник, О.О. Полубояров, Ю.А. Волошин, С.М. Куліш</i> Склад, структура та мікротвердість багатокомпонентних покриттів на основі карбиду вольфраму, сформованих методом інверсного магнетронного розпилення (англ.)	172
<i>П.В. Трофімов</i> Аналіз систем керування двигунами BLDC (англ.)	178

РЕФЕРАТИ	194
----------	-----

SYSTEMS AND METHODS OF INFORMATION PROTECTION СИСТЕМИ І МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ

УДК 004.056.55

DOI:10.30837/rt.2025.4.223.01

Є.О. ЛОГАЧОВА, М.В. ЄСІНА, канд. техн. наук, Д.Ю. ГОЛУБНИЧИЙ, канд. техн. наук

ОЦІНКА ЕФЕКТИВНОСТІ ЗАСТОСУВАННЯ МІЖНАРОДНИХ СТАНДАРТІВ ТА РЕГУЛЯТОРНИХ АКТІВ З РЕГУЛЮВАННЯ МОДЕЛЕЙ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ УКРАЇНИ

Вступ

Технології в Україні стрімко розвиваються. Україна – одна з перших країн у світі, що просувається на шляху масштабної діджиталізації. Одним із важливих щаблів розвитку у сучасному світі є правильна адаптація до використання технологій штучного інтелекту (ШІ).

Оскільки Україна ще не впровадила активно власні рішення, розглянемо досвід інших країн та спробуємо обрати найкращу концепцію розвитку. Одні країни орієнтовані на впровадження жорстких обмежень, інші роблять усе, щоб не обмежувати розвиток технології.

З метою оцінювання можливостей інтеграції досвіду інших країн у галузі штучного інтелекту для України було проведено оцінку адекватності кожного з підходів в рамках українського простору. Для оцінювання використано різні математичні методики, які є універсальними у проведенні багатьох дослідницьких оцінок.

1. Обґрунтування вибору апаратно-програмного забезпечення та методу оцінювання

Для дослідження було обрано удосконалену методику оцінювання для порівняння різних підходів за певними обраними критеріями. Дана методика є універсальною і може застосовуватись у різних випадках і для різних методик чи систем.

Необхідними даними для проведення оцінки є обрані критерії, на основі яких буде проведено оцінку експертів, а після – отримано коефіцієнти для порівняння.

Методика ґрунтується на експертному оцінюванні за обраними критеріями. Для вибору експертів було враховано їх компетентність у даній галузі. В якості вихідних даних отримуються певні коефіцієнти, що знаходяться за визначеними математичними виразами. Спираючись на дані, отримані від експертів, спочатку здійснюють математичну обробку відповідно до правил, визначених у кожному методі оцінювання, а далі – на основі отриманих результатів проводиться програмне моделювання.

В якості середовища для проведення розрахунків та обробки даних обрано MathCad. Адже саме це середовище містить необхідний пакет інструментів для роботи.

2. Послідовність дій оцінювання

Для оцінювання виконано наступні дії, які фактично є універсальним алгоритмом для проведення подібних оцінювань [1, 2]:

- вибір експертів за рівнем їх компетентності;
- вибір критеріїв (умовних та безумовних) для оцінювання;
- проведення оцінки за безумовними критеріями;
- на підставі безумовного інтегрального критерію ухвалюється рішення – залежно від отриманої оцінки – щодо доцільності подальшого порівняння та аналізу;
- за умови отримання позитивної оцінки – проведення оцінювання за умовними критеріями;
- опис результатів та висновки.

3. Дослідження за безумовними критеріями та його результати

Для дослідження було обрано декілька різних та часом дещо схожих підходів, запропонованих різними країнами або об'єднаннями для регулювання безпеки моделей штучного інтелекту. Для оцінки відібрано наступні країни та їх підходи: ЄС (AI Act), США (NIST AI RMF), ISO/IEC 23894, Велика Британія (White Paper), ОАЕ, Канада (AIDA), Південна Корея (AI Basic Act), Китай, Албанія [3–11].

Під безумовними критеріями розуміються ті, що є обов'язковими для виконання. Тобто ті досліджувані підходи, що не відповідають безумовним критеріям, не будуть задіяні у оцінці за умовними критеріями.

У якості безумовних критеріїв у нашій оцінці було обрано наступні п'ять показників:

- K_{s1} – валідність;
- K_{s2} – гнучкість;
- K_{s3} – етичність;
- K_{s4} – складність;
- K_{s5} – прогресивність.

Під валідністю мається на увазі реалізованість методу (регуляторного акту чи стандарту) – чи вже впроваджено на практиці, чи тільки заплановано на майбутнє.

Гнучкість – критерій, що описує інтегрованість підходу (регуляторного акту чи стандарту) у різні сфери.

Етичність характеризує те, чи метод справляється із захистом прав людини і чи не порушує підхід усталені норми етики та моралі.

Складність характеризує наявність ускладнень при інтеграції у країні, в нашому контексті – в Україні.

Прогресивність – критерій для визначення того чи сприяє метод нормальному розвитку технології.

Оскільки перелічені часткові критерії належать до безумовних, відбір здійснюється за допомогою бінарної логічної змінної, а саме «так» чи «ні» або 1/0. Таким чином, безумовний критерій може бути представлений у вигляді [1, 2]:

$$(K_{s1}, K_{s2}, K_{s3}, K_{s4}, K_{s5}) \in (1, 0). \quad (1)$$

Враховуючи названі безумовні критерії та (1), функцію відповідності адекватності методу (регуляторного акту чи стандарту) можна записати у вигляді [1, 2]:

$$f_{\text{фв}}() = (K_{s1} \wedge K_{s2} \wedge K_{s3} \wedge K_{s4} \wedge K_{s5}) = K_s. \quad (2)$$

Отже, якщо $f_{\text{фв}} = 1$, значить метод відповідає вимогам. Ті методи, що відповідають вимогам, будуть розглянуті далі [1, 2]. Результати порівняння відносно безумовних критеріїв наведено у табл. 1.

Таблиця 1

Результати порівняння відносно безумовних критеріїв

Метод \ Критерій	K_{s1}	K_{s2}	K_{s3}	K_{s4}	K_{s5}	K_s
ЄС (AI Act)	1	1	1	1	1	1
США (NIST AI RMF)	1	1	1	1	1	1
ISO/IEC 23894	1	1	1	1	1	1
Велика Британія (White Paper)	1	1	1	1	1	1
ОАЕ	0	1	0	0	1	0
Канада (AIDA)	1	1	1	1	1	1
Південна Корея (AI Basic Act)	1	1	1	1	1	1
Китай	1	1	1	1	1	1
Албанія	0	1	0	0	1	0

За отриманими результатами негативну оцінку отримали підходи, що описані у документах Албанії та ОАЕ [6, 7]. Усі інші будуть досліджені далі на основі умовних критеріїв та інтегрального умовного критерію та потенційно розглянуті як можливі підходи, що доступні для застосування в Україні.

4. Оцінювання за допомогою методу попарних порівнянь

В якості умовних критеріїв обрано часткові критерії, наведені у табл. 2. Наступним кроком було побудовано табл. 3, в якій наведено оцінку вкладу кожного критерію.

Під час парного порівняння експерт оцінює об'єкти попарно, визначаючи, який із двох є важливішим. Усі можливі комбінації об'єктів подаються у вигляді матриці попарних порівнянь. Під час проведення парних порівнянь необхідно відповісти на запитання: який із двох елементів є важливішим, має більший вплив, вищу ймовірність або перевагу. Зазвичай при порівнянні критеріїв визначають, який із них є значущішим відносно одне одного [1, 12].

Таблиця 2

Умовні часткові критерії оцінки ЕП

№	Критерії	Позначення
1	Рівень прозорості алгоритмів і систем прийняття рішень, тобто пояснюваність процедур, вимог та інших дій, зазначених у документі.	K_{y1}
2	Перспективність інтеграції регуляторного акту, методу, стандарту в Україні.	K_{y2}
3	Рівень гнучкості документу у застосуванні в різних сферах.	K_{y3}
4	Можливість запобігання виникненню етичних ризиків, пов'язаних з порушенням прав та свобод людини.	K_{y4}
5	Рівень інституційної підтримки та державної залученості.	K_{y5}
6	Вплив на перспективність розвитку технології окремо та у інших технологічних галузях.	K_{y6}

Для оцінки кожного критерію побудовано матрицю попарних порівнянь.

Таблиця 3

Попарне порівняння критеріїв для визначення важливості

Критерії	K_{y1}	K_{y2}	K_{y3}	K_{y4}	K_{y5}	K_{y6}	q_i	r_i
K_{y1}	1	1	2	0,5	4	2	1,41421356	0,18940253
K_{y2}	1	1	1	0,33	2	3	1,12246205	0,15032889
K_{y3}	0,5	1	1	0,2	3	1	0,81818882	0,10957824
K_{y4}	2	3	6	1	6	3	2,94168275	0,39397315
K_{y5}	0,25	0,5	0,33	0,1667	1	0,1428	0,31580809	0,04229549
K_{y6}	0,5	0,33	1	0,33	7	1	0,85435347	0,1144217

Відношення узгодженості має значення 7,466708745.

Таким чином, отримано розуміння того, який з критеріїв буде відігравати найбільшу роль при оцінюванні.

Далі було проведено окреме оцінювання за певним критерієм (табл. 4).

Таблиця 4

Матриця попарних порівнянь по критерію K_{y1}

Методи (документи)	ЄС (AI Act)	США (NIST AI RMF)	ISO/IEC 23894	Велика Британія (White Paper)	Канада (AIDA)	Південна Корея (AI Basic Act)	Китай	q_j	r_j
ЄС (AI Act)	1	1	1	2	2	2	3	1,574610106	0,20586303
США (NIST AI RMF)	1	1	1	2	2	2	3	1,574610106	0,20586303
ISO/IEC 23894	1	1	1	2	2	2	3	1,574610106	0,20586303
Велика Британія (White Paper)	0,5	0,5	0,5	1	1	1	2	0,820335356	0,10724986
Канада (AIDA)	0,5	0,5	0,5	1	1	1	2	0,820335356	0,10724986
Південна Корея (AI Basic Act)	0,5	0,5	0,5	1	1	1	2	0,820335356	0,10724986
Китай	0,333333	0,333333	0,333333	0,5	0,5	0,5	1	0,463987849	0,06066133

Розрахунки вектору пріоритетів проведено на основі добутку вектору пріоритетів першого рівня, отриманого раніше у табл. 4, та матриці отриманих значень.

$$t := (0.1840253 \quad 0.15032889 \quad 0.10957824 \quad 0.39397315 \quad 0.04229549 \quad 0.1144217)$$

$$L := \begin{pmatrix} 0.20586303 & 0.20586303 & 0.20586303 & 0.10724986 & 0.10724986 & 0.10724986 & 0.06066133 \\ 0.21271988 & 0.1119198 & 0.21271988 & 0.21271988 & 0.1119198 & 0.1119198 & 0.02608095 \\ 0.0967747 & 0.178227688 & 0.29745684 & 0.178227688 & 0.0967747 & 0.0967747 & 0.05566529 \\ 0.3063667 & 0.18875129 & 0.1270202 & 0.16133543 & 0.1085707 & 0.06507043 & 0.04241527 \\ 0.24590539 & 0.059441995 & 0.03712039 & 0.09752467 & 0.09752467 & 0.16272092 & 0.29976202 \\ 0.1218512 & 0.17672839 & 0.03630266 & 0.17672839 & 0.12185127 & 0.30904115 & 0.05749687 \end{pmatrix}$$

$$t1 := t \cdot L = (0.226 \quad 0.171 \quad 0.158 \quad 0.159 \quad 0.108 \quad 0.115 \quad 0.057)$$

Рис. 1. Розрахунок результуючого вектору пріоритетів

В результаті отримано чисельні дані, за якими найкращий результат показав європейський підхід – ЄС (AI Act) – 0,226, а найгірші значення у контексті обраних критеріїв отримав китайський підхід до регулювання ІІІ – 0,057. Значення інших розглянутих підходів налічують: США (NIST AI RMF) – 0,171; ISO/IEC 23894 – 0,158; Велика Британія (White Paper) – 0,159; Канада (AIDA) – 0,108; Південна Корея (AI Basic Act) – 0,115.

5. Оцінювання методом визначення вагових коефіцієнтів за допомогою шкали Фішберна

Даний метод полягає у тому, що за основу беруться оцінки певної кількості експертів, у нашому випадку їх було п'ять. Експерти оцінювали важливість того чи іншого критерію, ранжуючи їх – табл. 5.

Таблиця 5

Ранжування критеріїв експертами

Експерти \ Показники	x_1	x_2	x_3	x_4	x_5	x_6
1	2	1	4	3	5	6
2	5	1	3	4	2	6
3	3	2	4	2	6	5
4	5	1	4	2	6	3
5	3	2	5	1	6	4

Надалі проведено розрахунки для визначення значень вагових коефіцієнтів за формулою [1, 2, 13]:

$$a_i = \frac{2 \cdot (m - i + 1)}{m \cdot (m + 1)},$$

де a_i – ваги i -го показника, i – номер показника, m – кількість показників.

Результати визначення значень вагових коефіцієнтів для критеріїв наведено у табл. 6.

Таблиця 6

Значення вагових коефіцієнтів та їх середнє значення

Експерти \ Показники	x_1	x_2	x_3	x_4	x_5	x_6
1	0,23809524	0,28571429	0,14285714	0,19047619	0,0952381	0,04761905
2	0,0952381	0,28571429	0,19047619	0,14285714	0,23809524	0,04761905
3	0,19047619	0,23809524	0,14285714	0,28571429	0,04761905	0,0952381
4	0,0952381	0,28571429	0,14285714	0,23809524	0,04761905	0,19047619
5	0,19047619	0,23809524	0,0952381	0,28571429	0,04761905	0,14285714
w_i	0,16190476	0,26666667	0,14285714	0,22857143	0,0952381	0,1047619

Далі було проведено такі ж дії для кожного з підходів окремо. Приклад розрахунків наведено у табл. 7.

Таблиця 7

Значення вагових коефіцієнтів та їх середнє значення для ЄС (AI Act)

Показники Експерти	x_1	x_2	x_3	x_4	x_5	x_6
1	0,238095238	0,28571429	0,19047619	0,14285714	0,04761905	0,0952381
2	0,285714286	0,19047619	0,14285714	0,23809524	0,04761905	0,0952381
3	0,19047619	0,23809524	0,0952381	0,28571429	0,04761905	0,14285714
4	0,285714286	0,23809524	0,14285714	0,19047619	0,04761905	0,0952381
5	0,238095238	0,28571429	0,0952381	0,19047619	0,14285714	0,04761905
w_i	0,247619048	0,24761905	0,13333333	0,20952381	0,06666667	0,0952381

Надалі було проведено саме оцінювання та отримано результати – рис. 2. Найкращий результат отримав канадський підхід Канада (AIDA) – 0,267. А найгірший результат отримав США (NIST AI RMF) – 0,162.

Інші підходи отримали наступні показники: ЄС (AI Act) – 0,247; китайський підхід – 0,168; ISO/IEC 23894 – 0,185; Велика Британія (White Paper) – 0,185; Південна Корея (AI Basic Act) – 0,191.

$$w1 := (0.1619046 \ 0.26666667 \ 0.14285714 \ 0.22857143 \ 0.095231 \ 0.1047619)$$

$$L_Fish := \begin{pmatrix} 0.247619048 & 0.24761905 & 0.13333333 & 0.20952318 & 0.66666667 & 0.0952381 \\ 0.142857143 & 0.1714257 & 0.1428514 & 0.1428514 & 0.2 & 0.2 \\ 0.26666667 & 0.1904619 & 0.11428571 & 0.24761905 & 0.05714286 & 0.12380952 \\ 0.2 & 0.18095238 & 0.21904762 & 0.25714286 & 0.0952381 & 0.0461905 \\ 0.21904619 & 0.2 & 0.20952381 & 0.22857143 & 0.952381 & 0.0461905 \\ 0.20952318 & 0.20952318 & 0.15238095 & 0.28571429 & 0.0461905 & 0.0952381 \\ 0.24619048 & 0.12380952 & 0.07619048 & 0.24761905 & 0.21904762 & 0.06666667 \end{pmatrix}$$

$$V_Fish := w1$$

$$V_Fish = (0.162 \ 0.267 \ 0.143 \ 0.229 \ 0.095 \ 0.105)$$

$$Fish_rez := L_Fish \cdot V_Fish^T$$

$$Fish_rez^T = (0.247 \ 0.162 \ 0.185 \ 0.185 \ 0.267 \ 0.191 \ 0.168)$$

Рис. 2. Обчислення результуючого вектору пріоритетів

6. Оцінювання методом визначення вагових коефіцієнтів на основі методу ранжування

Припустимо, що існує m часткових показників і n експертів, які оцінюють їхню важливість для певної системи. У нашому випадку це знову ж п'ять експертів. Найвищий ранг (оцінку) m отримує показник, який вважається найважливішим, далі – показники з меншими рангами відповідно до зниження значущості, а ранг 1 присвоюється найменш важливому показнику. У цьому разі вагові коефіцієнти розраховуються за формулою [1, 2, 14]:

$$w_j = \frac{r_j}{\sum_{j=1}^m r_j}.$$

Як і у попередніх випадках, спершу було проведено розрахунки вагових коефіцієнтів для критеріїв – табл. 8.

Таблиця 8

Значення вагових коефіцієнтів

Показники Експерти	x_1	x_2	x_3	x_4	x_5	x_6
1	6	5	2	4	3	1
2	5	4	1	6	3	2
3	6	4	3	5	2	1
4	5	3	2	6	4	1
5	6	4	2	5	1	3
$r_j = \sum_{i=1}^n r_{ij}$	28	20	10	26	13	8
w_j	0,26666667	0,19048	0,09524	0,24762	0,12381	0,07619

У наступних кроках розраховано вагові коефіцієнти для кожного з підходів, які ми розглянули. Приклад такого розрахунку наведено у табл. 9.

Далі за схожим принципом розрахунку результуючого вектору проведено розрахунки та отримано результат – рис. 3, за яким найкращий показник отримав європейський підхід – документ AI Act – 0,197. Найгірші результати показали Велика Британія White Paper – 0,176 та США NIST AI RMF – 0,177. Інші підходи отримали оцінки: ISO/IEC 23894 – 0,186; китайський підхід – 0,183; Південна Корея (AI Basic Act) – 0,187; Канада (AIDA) – 0,195.

Таблиця 9

Значення вагових коефіцієнтів для Велика Британія (White Paper)

Показники Експерти	x_1	x_2	x_3	x_4	x_5	x_6
1	3	5	6	4	2	1
2	4	6	5	3	1	2
3	3	6	5	4	2	1
4	4	6	5	3	2	1
5	3	6	5	4	1	2
$r_j = \sum_{i=1}^n r_{ij}$	17	29	26	18	8	7
w_j	0,16190476	0,27619	0,24762	0,17143	0,07619	0,06667

$$w2 := (0.26666667 \ 0.19048 \ 0.09524 \ 0.24762 \ 0.12381 \ 0.07619)$$

$$L_Koeff := \begin{pmatrix} 0.21904762 & 0.19048 & 0.12381 & 0.28571 & 0.12381 & 0.05714 \\ 0.16190476 & 0.2851 & 0.2381 & 0.17143 & 0.06667 & 0.07619 \\ 0.28571429 & 0.20952 & 0.21905 & 0.13333 & 0.09524 & 0.05714 \\ 0.16190476 & 0.27619 & 0.24762 & 0.17143 & 0.07619 & 0.06667 \\ 0.20952381 & 0.21905 & 0.14286 & 0.2851 & 0.0619 & 0.06667 \\ 0.17142857 & 0.1619 & 0.0619 & 0.27619 & 0.24762 & 0.06667 \\ 0.18095238 & 0.14286 & 0.08571 & 0.2381 & 0.27619 & 0.07619 \end{pmatrix}$$

$$V_Koeff := w2$$

$$V_Koeff = (0.267 \ 0.19 \ 0.095 \ 0.248 \ 0.124 \ 0.076)$$

$$Koeff_rez := L_Koeff \cdot V_Koeff^T$$

$$Koeff_rez^T = (0.197 \ 0.177 \ 0.186 \ 0.176 \ 0.195 \ 0.187 \ 0.183)$$

Рис. 3. Обчислення результуючого вектору пріоритетів

7. Оцінювання методом визначення вагових коефіцієнтів на основі методу приписування балів

У методі приписування балів маємо m показників, важливість яких оцінюють n експертів. Експерт визначає, наскільки важливим є кожний показник для досліджуваної системи, і виставляє йому оцінку за шкалою від 0 до 10.

Допускається використання дробових значень, якщо експерт вважає, що показник заслуговує проміжної оцінки. Також кілька показників можуть отримати однаковий бал, якщо їх важливість вважається рівною.

Наступним кроком розраховується вага кожного коефіцієнта [1, 2]:

$$r_{ij} = \frac{h_{ij}}{\sum_{j=1}^m h_{ij}}, \quad \sum_{j=1}^m r_{ij} = 1,$$

де r_{ij} – ваги j -го показника, визначені i -м експертом; h_{ij} – бал i -го експерта, виставлений j -му показнику, n – кількість експертів, m – кількість показників.

В результаті вагові коефіцієнти визначались за формулами [1, 2]:

$$w_j = \frac{\sum_{i=1}^n r_{ij}}{\sum_{j=1}^m \sum_{i=1}^n r_{ij}}; \quad \sum_{j=1}^m w_j = 1.$$

Розрахунок вагових коефіцієнтів для критеріїв наведено у табл. 10.

Таблиця 10

Значення вагових коефіцієнтів

Показники Експерти	x_1	x_2	x_3	x_4	x_5	x_6	$\sum_{j=1}^m h_{ij}$	Ваги показників					
								r_{i1}	r_{i2}	r_{i3}	r_{i4}	r_{i5}	r_{i6}
1	9	8	5	10	7	6	45	0,2	0,17778	0,11111	0,22222	0,15556	0,13333
2	7	10	5	9	8	6	45	0,15555556	0,22222	0,11111	0,2	0,17778	0,13333
3	6	7	9	8	5	10	45	0,13333333	0,15556	0,2	0,17778	0,11111	0,22222
4	8	6	4	10	7	5	40	0,2	0,15	0,1	0,25	0,175	0,125
5	6	9	5	10	8	7	45	0,13333333	0,2	0,11111	0,22222	0,17778	0,15556
							$\sum_{i=1}^n r_j$	0,82222222	0,90555556	0,63333333	1,07222222	0,79722222	0,76944444
							w_j	0,16444444	0,18111111	0,12666667	0,21444444	0,15944444	0,15388889

Далі було проведено такі ж розрахунки для кожного з підходів, приклад наведено у табл. 11.

Таблиця 11

Значення вагових коефіцієнтів для ISO/IEC 23894

Показники Експерти	x_1	x_2	x_3	x_4	x_5	x_6	$\sum_{j=1}^m h_{ij}$	Ваги показників					
								r_{i1}	r_{i2}	r_{i3}	r_{i4}	r_{i5}	r_{i6}
1	9	8	9	7	7	8	48	0,1875	0,16666667	0,1875	0,14583333	0,14583333	0,16666667
2	10	8	9	6	7	7	47	0,21276596	0,17021277	0,19148936	0,12765957	0,14893617	0,14893617
3	8	7	8	7	6	7	43	0,18604651	0,1627907	0,18604651	0,1627907	0,13953488	0,1627907
4	9	7	8	7	6	7	44	0,20454545	0,15909091	0,18181818	0,15909091	0,13636364	0,15909091
5	9	8	8	6	6	8	45	0,2	0,17777778	0,17777778	0,13333333	0,13333333	0,17777778
							$\sum_{i=1}^n r_j$	0,99085792	0,83653882	0,92463183	0,72870785	0,70400136	0,81526222
							w_j	0,19817158	0,16730776	0,18492637	0,14574157	0,14080027	0,16305244

В результаті обчислено значення результуючого вектору пріоритетів (рис. 4) та отримано результат оцінювання: найкращий результат за розрахунками отримали ЄС (AI Act) та Велика Британія (White Paper) – 0,169. Найгірший результат показав китайський метод – 0,161. Хоча варто відмітити, що розходження між усіма методами мінімальні: США (NIST AI RMF) – 0,167; ISO/IEC 23894 – 0,164; Канада (AIDA) – 0,163; Південна Корея (AI Basic Act) – 0,162.

```
w3 := (0.16444444 0.18111111 0.12666667 0.21444444 0.15444444 0.15388889)

L_Point := (0.18559759 0.19759419 0.12088985 0.1895959 0.16525484 0.141006593
0.18368019 0.18309992 0.16125155 0.17913884 0.13563563 0.15719386
0.19817158 0.16730776 0.18492637 0.14574157 0.14080027 0.16305244
0.20007323 0.1744411 0.14047564 0.19998073 0.13187249 0.1531568
0.16796373 0.17222652 0.20166662 0.13462316 0.1301903 0.19332967
0.16244218 0.15809436 0.19657724 0.12821462 0.20508788 0.14958372
0.13253901 0.15516997 0.18277929 0.10947515 0.21906104 0.20097554)

V_Point := w3

V_Point = (0.164 0.181 0.127 0.214 0.154 0.154)

Point_rez := L_Point * V_Point^T

Point_rez^T = (0.169 0.167 0.164 0.169 0.163 0.162 0.161)
```

Рис. 4. Обчислення результуючого вектору пріоритетів

8. Оцінювання методом визначення вагових коефіцієнтів на основі числового способу

Останнім застосованим методом став метод визначення вагових коефіцієнтів на основі числового способу. У цьому методі для кожного показника обчислюється коефіцієнт відносного розкиду [1, 2]:

$$\delta_i = \frac{x_{i\max} - x_{i\min}}{x_{i\max}}.$$

Оскільки значення самих показників можна було отримати з будь-якого попереднього обчислення, було обрано значення обчислень за шкалою Фішберна. Після обчислення вагових коефіцієнтів [1, 2]:

$$w_i = \frac{\delta_i}{\sum_{i=1}^m \delta_i}.$$

Розрахунки вагових коефіцієнтів для критеріїв наведено у табл. 12.

Таблиця 12

Значення вагових коефіцієнтів

Показники Оцінювання	x_1	x_2	x_3	x_4	x_5	x_6
$x_{i\min}$	0,0952381	0,23809524	0,0952381	0,1428571	0,0476191	0,0476191
$x_{i\max}$	0,23809524	0,28571429	0,1904762	0,2857143	0,2380952	0,1904762
δ_i	0,59999998	0,16666667	0,5	0,5	0,8	0,75
w_i	0,18090452	0,05025126	0,1507538	0,1507538	0,241206	0,2261307

Далі, як і у попередніх методах, повторено розрахунки для усіх досліджуваних підходів регулювання ШІ. Приклад розрахунків наведено у табл. 13. А після обчислення результуючого вектору пріоритетів – рис. 5. За даним методом найкращий результат отримали китайський підхід – 0,385 та ЄС (AI Act) – 0,18. Найгірший результат показала Велика Британія (White Paper) – 0,048. Інші методи отримали наступні результати: США (NIST AI RMF) – 0,156; ISO/IEC 23894 – 0,156; Канада (AIDA) – 0,059; Південна Корея (AI Basic Act) – 0,111.

Таблиця 13

Значення вагових коефіцієнтів для Канади (AIDA)

Показники Оцінювання	x_1	x_2	x_3	x_4	x_5	x_6
$x_{i\min}$	0,19047619	0,14285714	0,1428571	0,1428571	0,0952381	0,0476191
$x_{i\max}$	0,23809524	0,23809524	0,2857143	0,2857143	0,0952381	0,0476191
δ_i	0,2	0,40000002	0,5	0,5	0	0
w_i	0,125	0,08450705	0,1056338	0,1056338	0	0

$$w4 := (0.18090452 \ 0.05025126 \ 0.1507538 \ 0.1507528 \ 0.241206 \ 0.2261307)$$

$$L_Num := \begin{pmatrix} 0.11111111 & 0.11111112 & 0.1666667 & 0.1666667 & 0.2222222 & 0.2222222 \\ 0.16901409 & 0.17605634 & 0.1690141 & 0.1690141 & 0.1760563 & 0.1408451 \\ 0.06944445 & 0.16666668 & 0.2777778 & 0.1388889 & 0.2083333 & 0.1388889 \\ 0.08450704 & 0.08450705 & 0.084507 & 0.1056338 & 0 & 0 \\ 0.125 & 0.08450705 & 0.1056338 & 0.1056338 & 0 & 0 \\ 0.23529411 & 0.47058824 & 0.2941177 & 0 & 0 & 0 \\ 0.15151515 & 0.39215679 & 0.5882353 & 0.3921569 & 0.2352941 & 0.5882353 \end{pmatrix}$$

$$V_Num := w4$$

$$V_Num = (0.181 \ 0.05 \ 0.151 \ 0.151 \ 0.241 \ 0.226)$$

$$Num_rez := L_Num \cdot V_Num^T$$

$$Num_rez^T = (0.18 \ 0.165 \ 0.165 \ 0.048 \ 0.059 \ 0.111 \ 0.385)$$

Рис. 5. Обчислення результуючого вектору пріоритетів

9. Висновки за результатами оцінювання

Після оцінювання адекватності різних міжнародних підходів регулювання штучного інтелекту щодо застосування в Україні отримано результати, які схематично наведено на рис. 6.

За результатами, описаними раніше та наведеними на рис. 6, видно, що найкращими за різними методами оцінювання виявились ЄС (AI Act) та Канада (AIDA). Причому ЄС (AI Act) показує доволі стабільні значення, що свідчить про збалансованість та зрілість регуляторної системи, де враховуються як прозорість алгоритмів, так і етична складова та інституційна підтримка.

Китайський підхід до регулювання штучного інтелекту показав найгірші результати майже за всіма методиками, тобто він є одним із найменш ймовірно інтегрованих для України.

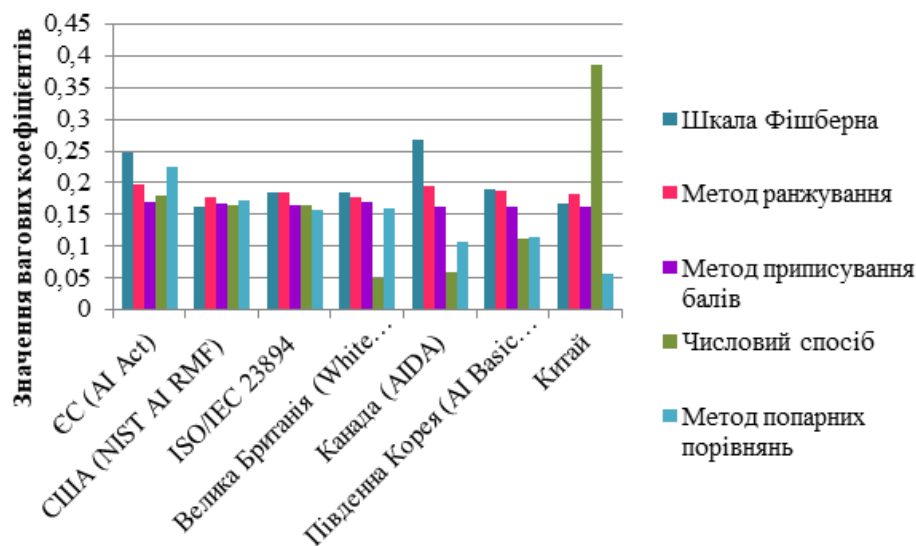


Рис. 6. Ілюстрація результатів оцінювання

США (NIST AI RMF) та ISO/IEC 23894 мають близькі результати з незначною перевагою першого. Обидва документи роблять акцент на гнучкості й стандартизації. Це робить їх доволі хорошими прикладами для України.

Велика Британія демонструє середні показники за всіма методами, що відповідає її гнучкому, ринково-орієнтованому підходу, заснованому на принципах «регулювання через довіру». Цей підхід забезпечує помірну ефективність, але нижчу централізованість.

Південна Корея має дещо нижчі значення, однак показує відносну збалансованість, але все ж це робить її не найкращим прикладом для наслідування у випадку України.

Усереднене оцінювання результатів для кожного з підходів наведено у табл. 14.

Таблиця 14

Усереднене оцінювання результатів

Методи (документи)	Середній результат
ЕС (AI Act)	0,2038
США (NIST AI RMF)	0,1684
ISO/IEC 23894	0,1716
Велика Британія (White Paper)	0,1474
Канада (AIDA)	0,1584
Південна Корея (AI Basic Act)	0,1532
Китай	0,1908

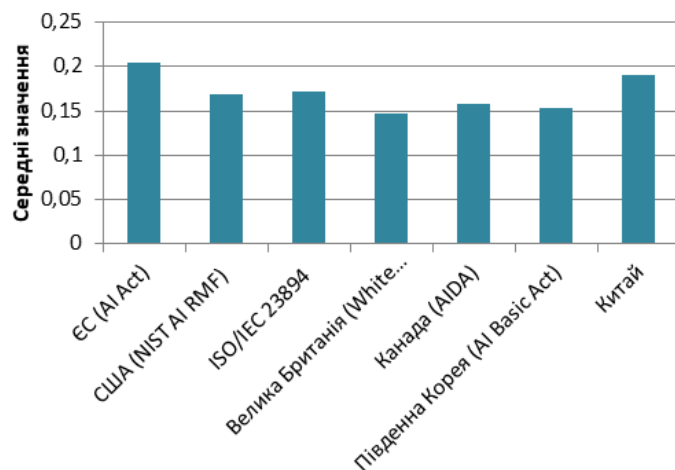


Рис. 7. Усереднене оцінювання результатів

Висновки

У результаті дослідження і проведення оцінювання ми дійшли висновків, що одними з найкращих прикладів регулювання ШІ для України є ЄС (AI Act) та Канада (AIDA). Адже саме вони показали найстабільніші позитивні результати.

А серед прикладів, які навряд знайдуть успішний шлях інтеграції в Україні, є китайський підхід, який хоч і доволі цікаво побудований, та все ж акцентує увагу більше не на пріоритетних для України критеріях.

Список літератури:

1. Горбенко І. Д. Методи, методика та результати порівняльного аналізу електронних підписів згідно ДСТУ ISO/IEC 14888-3:2014 / І. Д. Горбенко, М. В. Єсіна // Вісник Нац. ун-ту “Львівська політехніка”: Серія “Автоматика, вимірювання та керування”. Львів : Львівська політехніка, 2016. № 852. С. 9–22.
2. Горбенко Ю. І., Ганзя Р. С., Акользіна О. С. Електронні підписи на основі ідентифікаторів та бінарного відображення // Прикладна радіоелектроніка. 2015. Т. 14. № 4. С. 284–290.
3. EU AI Act: first regulation on artificial intelligence. [Електронний ресурс]. Режим доступу: <https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence>.
4. Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile. [Електронний ресурс]. Режим доступу: <https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf>.
5. Information technology – Artificial intelligence – Guidance on risk management [Електронний ресурс]. Режим доступу: <https://cdn.standards.iteh.ai/samples/77304/cb803ee4e9624430a5db177459158b24/ISO-IEC-23894-2023.pdf>.
6. AI Watch: Global regulatory tracker – United Arab Emirates. [Електронний ресурс]. Режим доступу: <https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-uae>.
7. Albania turns to AI to beat corruption and join EU [Електронний ресурс]. Режим доступу: <https://www.politico.eu/article/albania-use-ai-artificial-intelligence-join-eu-corruption/>.
8. Interim Measures for the Management of Generative Artificial Intelligence Services [Електронний ресурс]. Режим доступу: <https://www.chinalawtranslate.com/en/generative-ai-interim/#gsc.tab=0>.
9. A pro-innovation approach to AI regulation 3 August 2023 [Електронний ресурс]. Режим доступу: https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper?utm_source=chatgpt.com#part-7-conclusion-and-next-steps.
10. The Artificial Intelligence and Data Act (AIDA) – Companion document. [Електронний ресурс]. Режим доступу: <https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act-aida-companion-document>.
11. South Korea Artificial Intelligence (AI) Basic Act [Електронний ресурс]. Режим доступу: <https://www.trade.gov/market-intelligence/south-korea-artificial-intelligence-ai-basic-act>.
12. Oletsky O. Enhancing Consistency of Pairwise Comparisons on the Base of Linear Algebraic Equations. NaUKMA Research Papers. Computer Science. 2023. Т. 5. С. 85–91. [Електронний ресурс]. Режим доступу: <http://nrpcmp.ukma.edu.ua/article/view/275238>.
13. Lyashenko, E. M., Klymash, M. P., Lyashko, O. A. On creation of expert knowledge base for estimation of state of organizational systems // International Journal of Fuzzy Systems and Advanced Applications. 2014. Vol. 1. P. 7–13.
14. Alguliyev R. M., Nabibayova G. Ch., & Abdullayeva S. R. Evaluation of websites by many criteria using the algorithm for pairwise comparison of alternatives // I.J. Intelligent Systems and Applications. 2020. Vol. 12, No. 6. P. 64–74. <https://doi.org/10.5815/ijisa.2020.06.05>.

Надійшла до редколегії 15.10.2025

Відомості про авторів:

Логачова Єлизавета Олегівна – Харківський національний університет імені В. Н. Каразіна, студентка кафедри кібербезпеки інформаційних систем, мереж і технологій, навчально-науковий інститут комп’ютерних наук та штучного інтелекту; Україна; e-mail: lohachova2020kb11@student.karazin.ua; ORCID: <https://orcid.org/0000-0002-9815-466X>

Єсіна Марина Віталіївна – канд. техн. наук, доцент, Харківський національний університет імені В. Н. Каразіна, завідувачка кафедри кібербезпеки інформаційних систем, мереж і технологій, навчально-наукового інституту комп’ютерних наук та штучного інтелекту; ПАТ “Інститут Інформаційних Технологій”, науковий співробітник-консультант; Україна; e-mail: m.v.yesina@karazin.ua; ORCID: <https://orcid.org/0000-0002-1252-7606>

Голубничий Дмитро Юрійович – канд. техн. наук, доцент, ПАТ “Інститут Інформаційних Технологій”, начальник наукового відділу; Україна; ORCID: <https://orcid.org/0000-0002-6873-7004>

Я.А. ДЕРЕВ'ЯНКО, Д.Ю. ГОРБЕНКО

ТЕОРЕТИЧНЕ ОБҐРУНТУВАННЯ ТА ПРАКТИЧНА РЕАЛІЗАЦІЯ ЕКСТРАКТОРІВ ЕНТРОПІЇ НА ОСНОВІ НАЦІОНАЛЬНИХ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ

Вступ

Рекомендації щодо застосування ентропії під час формування випадкових даних наведено у NIST Special Publication 800-90B [1], де визначається порядок збору та оцінки ентропії з відповідних джерел шуму, а також порядок застосування екстракції ентропії з отриманих даних, щоб результат відповідав певним вимогам щодо ентропії на біт, рівномірності та непередбачуваності.

Першим та найважливішим кроком для побудови екстрактора є правильний вибір джерела шуму (ДШ). ДШ – це основа безпеки для джерела ентропії і для RNG в цілому, оскільки воно містить недетермінований процес, що і надає ентропію. Якщо недетермінована активність ДШ виробляє щось інше, ніж двійкові дані, процес відбору зразків включає в себе процес оцифрування.

ДШ поділяються на фізичні – використовують спеціальне обладнання для генерування випадковості та нефізичні – використовують системні дані або введення користувача системи для генерування випадковості.

Для побудови екстрактора необхідним є збір вибірок з певного ДШ, оцінка його ентропії за цими вибірками і подальша обробка з використанням певного криптографічного примітиву. Для подальшого отримання послідовностей довільної довжини на основі виходу з екстрактора можливим є застосування різноманітних криптографічних примітивів для розширення виходу екстрактора ентропії.

У статті проаналізовано існуючі рекомендації щодо побудування екстракторів ентропії на основі криптографічних примітивів, виконано теоретичне обґрунтування можливості застосування національних алгоритмів у якості подібних екстракторів, а також наведено приклади практичної реалізації екстракторів на основі національних криптографічних алгоритмів. Актуальність розробки цих нових засобів отримання випадковості обґрунтована важливістю використання результатуючих даних з високими показниками рівномірності та непередбачуваності при обчисленні загальносистемних параметрів та генеруванні ключів квантовостійких стандартизованих криптографічних перетворень.

1. Принципи побудови екстрактора ентропії та криптографічні компоненти, що для цього використовуються

Згідно з [1] побудова екстрактора ентропії має обов'язково включати наступні кроки:

- вибір найбільш відповідного ДШ та збір зразків з нього;
- оцінка ентропії ДШ на основі зібраних «сирих» даних;
- застосування рекомендованого довіреного криптографічного примітиву для виконання екстракції ентропії з зібраних зразків;
- оцінка ентропії на виході екстрактора.

1.1. Вибір джерела шуму та збір зразків

Саме ДШ в кінцевому рахунку відповідає за непередбачуваність бітових рядків, що виводяться екстрактором ентропії, тому важливим є вибір правильного ДШ з найбільш відповідними показниками ентропії. Важливим кроком при побудові екстрактора ентропії є коректне отримання ентропії з ДШ для виконання подальшої екстракції.

У [1] припускається, що значення вибірки (тобто символи) з ДШ складаються з бітових рядків фіксованої довжини. Рекомендації щодо збору зразків наступні.

Для валідації (тобто оцінки ентропії ДШ) повинен бути зібраний послідовний набір даних, що складається щонайменше з 1 000 000 значень, отриманих з ДШ (тобто необроблені дані). Якщо генерація 1 000 000 послідовних зразків неможлива, допускається конкатенація декількох менших наборів послідовних зразків (згенерованих з використанням того самого ДШ). Менші набори повинні містити щонайменше 1000 зразків. Об'єднаний набір даних повинен містити не менше 1 000 000 зразків [1].

Отже, для виконання наступного кроку – оцінки ентропії ДШ – необхідно отримати достатню кількість «сирих» зразків з ДШ.

1.2. Оцінка ентропії джерела шуму на основі «сирих» даних

Наступним важливим кроком є кількісна оцінка ентропії ДШ шляхом оцінки отриманих вибірок. У [1] передбачено проведення оцінки *min*-ентропії, яка відповідає найбільш консервативному способу вимірювання непередбачуваності набору і тому використовується як оцінка в найгіршому випадку. Також для більш повної оцінки у даній роботі передбачається обчислення ентропії Шеннона [2] та колізійна ентропія [3].

Методи оцінки *min*-ентропії засновані на двох підходах. Перший базується на ентропійній статистиці, а другий – на предикторах. У [1] визначаються такі оцінки: найпоширенішого значення, колізій, Маркова, стиснення, *t*-кортежу, найдовшого повторюваного підрядка, найпоширеніших значень у фіксованому вікні, прогнозування затримки, MultiMMC та LZ78Y.

В свою чергу ентропія Шеннона та колізійна ентропія розраховується для отримання незміщеної ентропії шляхом застосування методів корекції. Основними з них є [2]:

- Miller-Madow correction (MM);
- Jackknife (UnveilJ);
- Best Upper Bound (BUB);
- Chao-Chen (CS);
- James-Stein (SHR);
- Schürmann (SHU).

Таким чином, подальше виконання екстракції потребує впровадження оцінки *min*-ентропії ДШ, оскільки така оцінка є мірою ентропії для найгіршого випадку. Впровадження оцінок ентропії Шеннона та колізійної ентропії є опціональним і залежить від бажаної швидкості та складності роботи екстрактора

1.3. Криптографічні примітиви для екстракції ентропії з отриманих «сирих» даних

Згідно з [1] екстрактор ентропії отримує вхідні дані від джерела шуму та генерує вихід джерела ентропії. Розмір входу та виходу екстрактора ентропії в бітах, позначених як n_{in} та n_{out} відповідно, є фіксованими. Виходи ДШ об'єднуються для побудови n_{in} -бітового входу для функції екстракції. Ентропія входу, позначена h_{in} , залежить від кількості зразків, необхідних для побудови n_{in} -бітового входу. Якщо потрібно w зразків, то h_{in} оцінюється як $w \times h$ біт. Розмір входу екстрактора має бути кратним розміру виходу джерела шуму.

Оскільки екстрактор ентропії є детермінованим, ентропія виходу не перевищує h_{in} . Однак екстрактор може зменшити ентропію виходу. Ентропія виходу екстрактора позначається як h_{out} , тобто h_{out} бітів ентропії міститься в n_{out} бітах виходу. Ентропія виходу також залежить від внутрішньої будови екстрактора.

У [1] найвужча внутрішня ширина (Narrowest Internal Width) в межах екстрактора позначається як n_w .

Загальну схему роботи екстрактора ентропії згідно з NIST 800-90B наведено на рис. 1.

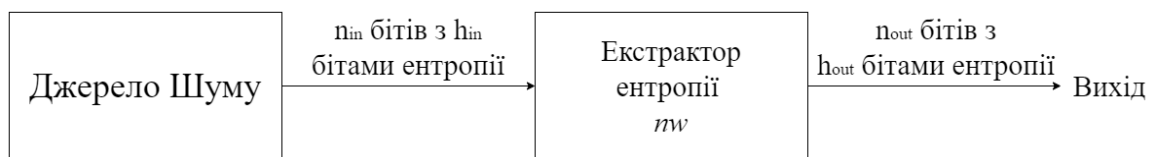


Рис. 1. Загальна схема роботи екстрактора ентропії

Як видно з рисунку, компонент приймає і повертає фіксовану кількість бітів. Важливо також, що ентропія, яку отримує екстрактор, не може перевищувати ентропію отриманих від ДШ даних, які подаються на його вхід.

1.3.1. Рекомендовані NIST криптографічні примітиви

У [1] визначено перевірені та рекомендовані NIST криптографічні примітиви, які необхідно застосовувати з метою екстракції ентропії з отриманих з ДШ даних, щоб вихідні дані задовольняли певним вимогам щодо ентропії на біт, рівномірності та непередбачуваності.

Серед них визначено три алгоритми з ключем [1]:

- HMAC, як зазначено в FIPS 198, з будь-якою затвердженою геш функцією, зазначеною в FIPS 180 або FIPS 202;
- CMAC, як зазначено в SP 800-38B, з блоковим шифром AES (FIPS 197);
- CBC-MAC, з блоковим шифром AES.

Та три алгоритми без ключа [1]:

- будь-яка затверджена геш функція, зазначена в FIPS 180 або FIPS 202;
- Hash_df, як зазначено в SP 800-90A, з використанням будь-якої затвердженої геш функції, зазначеної в FIPS 180 або FIPS 202;
- Block_Cipher_df, як зазначено в SP800-90A з використанням блочного шифру AES (FIPS 197).

Параметри екстракторів на представлених криптографічних примітивах наведені в табл. 1. У ній міститься інформація про найвужчу внутрішню ширину (Narrowest Internal Width) в межах екстрактора та розмір вихідних даних після екстракції.

Таблиця 1

Найвужча внутрішня ширина та довжина виходу перевірених функцій екстракції

Функція (компонент) екстракції	Найвужча внутрішня ширина (Narrowest Internal Width) n_w	Довжина виходу екстрактора n_{out}
HMAC	Розмір виходу геш функції	Розмір виходу геш функції
CMAC	Розмір блоку шифру	Розмір блоку шифру
CBC-MAC	Розмір блоку шифру	Розмір блоку шифру
Геш функція	Розмір виходу геш функції	Розмір виходу геш функції
Hash_df	Розмір виходу геш функції	Розмір виходу геш функції
Block_Cipher_df	Розмір ключа шифру	Розмір ключа шифру

1.3.2. Національні криптографічні примітиви, які можливо застосувати у якості екстракторів

Аналіз рекомендованих NIST криптографічних примітивів та їх порівняння зі специфікацією національних стандартів України вказує на можливість застосування для виконання екстракції ентропії наступних алгоритмів та режимів: HMAC та алгоритм Hash_df з використанням геш функції Купина (ДСТУ 7564:2014) [4] та CMAC і алгоритм Block_Cipher_df з використанням блокового шифру Калина (ДСТУ 7624:2014) [5]. Режим CBC-MAC не визначено у [5], тому його застосування не є доцільним. При цьому використання [4] як самостійного екстрактора не рекомендовано, оскільки національна геш функція не належить до універсального геш-сімейства (як, наприклад, SHA), що в свою чергу означає, що її екстракційні властивості не доведено. У табл. 2 надано режими національних алгоритмів, які можливо застосовувати з метою екстракції та їх властивості.

Найвужча внутрішня ширина та довжина виходу перевірених функцій екстракції

Функція (компонент) екстракції	Найвужча внутрішня ширина (Narrowest Internal Width) n_w	Довжина виходу екстрактора n_{out}
HMAC/Hash_df для Купина-256	Розмір виходу геш функції (256 біт)	Розмір виходу геш функції (256 біт)
HMAC/Hash_df для Купина-512	Розмір виходу геш функції (512 біт)	Розмір виходу геш функції (512 біт)
СМАС для Калина-128/128, Калина-128/256	Розмір блоку шифру (128 біт)	Розмір блоку шифру (128 біт)
СМАС для Калина-256/256, Калина-256/512	Розмір блоку шифру (256 біт)	Розмір блоку шифру (256 біт)
СМАС для Калина-512/512	Розмір блоку шифру (512 біт)	Розмір блоку шифру (512 біт)
Block_Cipher_df для Калина-128/128	Розмір ключа шифру (128 біт)	Розмір ключа шифру (128 біт)
Block_Cipher_df для Калина-128/256, Калина-256/256	Розмір ключа шифру (256 біт)	Розмір ключа шифру (256 біт)
Block_Cipher_df для Калина-Калина-256/512, Калина-512/512	Розмір ключа шифру (512 біт)	Розмір ключа шифру (512 біт)

Як видно з табл. 2, національні криптографічні примітиви надають змогу створення екстракторів з виходами довжини 128, 256 та 512 з хорошими показниками рівномірності та непередбачуваності. Далі виходи екстракторів можна використовувати для формування довгих послідовностей з використанням експандерів (блокових шифрів у режимі CTR, поточних шифрів тощо).

1.4. Оцінка ентропії на виході екстрактора

Зважаючи на те, що вихідна ентропія після виконання екстракції, як вказано у [1] не може зрости, проте може зменшитися, NIST рекомендує оцінювати ентропію на виході:

При використанні перевірених (довіренних) NIST компонентів:

Для оцінки передбачена формула

$$h_{out} = \text{Output_Entropy}(n_{in}, n_{out}, n_w, h_{in}), \quad (1)$$

де алгоритм обчислення $\text{Output_Entropy}(n_{in}, n_{out}, n_w, h_{in})$ наступний:

Вхід:

n_{in} – розмір входу екстрактора ентропії в бітах;

n_{out} – розмір виходу екстрактора ентропії в бітах;

n_w – найвужча внутрішня ширина екстрактора ентропії в бітах;

h_{in} – ентропія входу.

Вихід:

h_{out} – значення оцінки ентропії після виконання екстракції.

$$1 \text{ Нехай } P_{high} = 2^{-h_{in}} \text{ та } P_{low} = \frac{(1 - P_{high})}{2^{n_{in}} - 1}$$

$$2 \text{ } n = \min(n_{out}, n_w)$$

$$3 \text{ } \psi = 2^{n_{in}-n} P_{low} + P_{high}$$

$$4 \text{ } U = 2^{n_{in}-n} + \sqrt{2n(2^{n_{in}-n}) \ln(2)}$$

$$5 \text{ } \omega = U \times P_{low}$$

$$6 \text{ Повернення } -\log_2(\max(\psi, \omega))$$

Алгоритм 1. Обчислення ентропії на виході екстрактора

Отже, джерело ентропії оцінюється за мінімальною ентропією на вихід екстрактора, h_{out} . Перевірені NIST екстрактори можуть претендувати на повну ентропію на виході.

Для наочного прикладу оцінки нехай теоретичний екстрактор матиме наступні значення: $n_{in} = 256$, $n_{out} = 128$, $h_{in} = 128$, $nw = 128$.

Тобто маємо певний криптографічний примітив з найвужчою внутрішньою шириною 128 бітів, вхідну послідовність довжиною 256 бітів з 128 бітами ентропії (0,5 на біт) і розмір виходу екстрактора 128 бітів. За алгоритмом 1 отримаємо h_{out} : $\psi = 5.88 \times 10^{-39}$, $\omega = 2.94 \times 10^{-39}$, $-\log_2(\max(\psi, \omega)) = 127.000000000000...92$.

Таким чином, ентропія на виході такого екстрактора буде майже повною, тобто 127 бітів ентропії на 128 бітів виходу.

Необхідно зауважити, що усічення виходу такого екстрактора є допустимим. В такому випадку оцінка ентропії зменшується до пропорції на виході (наприклад, при усіченні 8-бітного виходу з 6 бітами ентропії до 6 біт ентропія зменшується до $3/4 \times 6 = 4.5$ біт).

При використанні неперевірених (недовірених) NIST компонентів:

Для неперевірених NIST екстракторів ентропія на виході залежить від ентропії та розміру входу (h_{in} і n_{in}), розміру виходу (n_{out}), розміру найвужчої внутрішньої ширини (nw) та ентропії послідовного набору даних на виході екстрактора. Екстракція для збирання такого набору повинна виконуватися екстрактором, що оцінюється.

Отримання набору даних відбувається наступним чином:

Для валідації екстрактора повинен бути зібраний послідовний набір даних, що складається щонайменше з 1 000 000 послідовних виходів. Вихідні дані екстрактора повинні бути об'єднані в тому порядку, в якому вони були згенеровані, і розглядатися як двійковий рядок для цілей тестування. Ентропія такого набору даних повинна оцінюватися з використанням IID тестів для IID даних та поп-IID тестів для поп-IID даних. Проте, оскільки поп-IID тести є доволі консервативними, вони можуть занижувати реальне значення $\min$ -ентропії [1]. Отримана оцінка ентропії на біт такого набору буде h' .

Отже, ентропія виходу екстрактора на неперевіреному криптографічному примітиві оцінюється за формулою

$$h_{out} = \min(\text{Output_Entropy}(n_{in}, n_{out}, nw, h_{in}), 0.999n_{out}, h' \times n_{out}) \quad (2)$$

1.5. Криптографічні примітиви для розширення виходу з екстрактора

У більш нових версіях ядра Linux застосовується довірена NIST конструкція DRBG [6, 7] у якості генератора – за замовчуванням використовується CTR DRBG з AES-256. Тобто у якості компонента розширення використовується блоковий шифр у потоковому режимі. Для заповнення генератора (seeding) використовується seed, отриманий за рахунок екстракції з пулу ентропії. На основі цього генератор має змогу обчислювати псевдовипадкові значення з хорошими показниками рівномірності.

Зважаючи на це, можливим є застосування національних алгоритмів блокового шифрування Калина (ДСТУ 7624:2014) [5] та потокового шифрування Струмок (ДСТУ 8845:2019) [9] до виходу з екстрактора, для його розширення та формування випадкової послідовності довільної довжини.

Значення максимальної довжини генерації за запит, а також максимальної кількості таких запитів слід обмежити рекомендованими у [8] параметрами – кількість байт на запит «згенерувати» DRBG становить 2^{19} біт або 2^{16} байт, а кількість дозволених запитів до примусового повторного заповнення – 2^{48} .

У наступному розділі представлено практичні реалізації екстракторів на основі криптографічних примітивів та алгоритмів, що описані у п. 1.3.

2. Практична реалізація екстракторів на основі національних стандартів

Для практичної реалізації екстракторів необхідно повторити кроки, описані у розд. 1, використовуючи реальні ДШ та криптографічні примітиви.

2.1. Отримання даних з джерел шуму та оцінка їх ентропії за рекомендаціями NIST 800-90B

Згідно з вимогами [1] оцінка ентропії ДШ потребує послідовного набору даних зі щонайменше з 1 000 000 зразків. У якості ДШ були обрані наступні:

- нефізичне ДШ у вигляді запитів на переривання (IRQ) – у якості зразків використовується часова відмінність дельт часу між мітками часу переривань, що викликані пристроями введення (взаємодії з користувачем)/мережевими пристроями;
- нефізичне ДШ у вигляді дельт часу між мітками часу апаратних подій, отриманих з використанням спеціальних системних функцій: `add_input_randomness` (обробка подій введення), `add_disk_randomness` (обробка подій роботи з дисками) із застосуванням модулю `kprobe`.

2.1.1. Процес отримання даних з ДШ на основі IRQ

Для отримання ентропії з ДШ на основі джитеру дельт часу між запитами на переривання (IRQ) використовується ОС Linux та принцип загальної обробки IRQ в Linux. В основі лежить функція API драйвера високого рівня `request_irq()`, основне призначення якої виклик заданої функції (обробника) кожного разу при виникненні заданого типу переривання.

Для збору ентропії було створено модулі ядра. Ці модулі виконують перехоплення IRQ для пристроїв введення (миші) та мережевого адаптера. Як вказано вище, вони використовують `request_irq()`, до якої передається функція обробник. Ця функція обчислює дельту часу між перериваннями, а також відмінність цих часових дельт. З результуючої відмінності дельт часу беруться вісім наймолодших бітів (LSB) та поміщаються до буфера ентропії.

Для реалізації можливості зчитування даних з буфера ентропії у просторі користувача всередині модулів створюються відповідні символьні псевдопристрої. Під час використання користувач з програмного коду викликає ці пристрої і зчитує необхідну/доступну кількість ентропії у бінарний файл доти, доки не буде зібрано необхідну кількість. У випадку реалізації екстрактора необхідно зчитати більше ніж 1,048,576 зразків з ДШ, бо вибірка з джерела шуму відбувається по 8 біт, тобто побайтово. Така кількість обрана, щоб задовольняти умові з [1] щодо розміру вибірки і додатково, щоб зібрати повний 1 МБ «сирих» випадкових даних. У алгоритмах 2 та 3 наведено модулі у вигляді псевдокоду.

- 1 Ініціалізація буфера ентропії
- 2 Вибір необхідних пристроїв для обробки переривань (шляхом аналізу `/proc/interrupts`)
- 3 Визначення спінлоку та черги очікування (Спінлок (`entropy_lock`) використовується для захисту одночасного доступу до буфера між контекстами IRQ і процесу. Черга очікування (`entropy_wait_queue`) дозволяє блокувати читання, коли ще немає достатньої кількості даних)
- 4 Ініціалізація стану для обчислення джитеру (стан містить значення часу у мілісекундах, коли відбулося останнє переривання і значення останньої дельти між перериваннями)
- 5 Реалізація функції оцінки доступної ентропії у буфері
- 6 Реалізація функції обробки переривань – `my_interrupt_handler` (обчислення нової дельти часу та джитера з попередньою дельтою)
- 7 Реалізація функції ініціалізації модуля
- 8 Реалізація функції вивільнення модуля
- 9 Реалізація функції зчитування з буфера до простору користувача з використанням створеного символьного псевдопристрою
- 10 Визначення структури, яка відповідатиме за функції, що викликатимуться через стандартний узагальнений інтерфейс псевдопристрою

Алгоритм 2. Модуль ядра Linux для збору ентропії з використанням обробки IRQ

2.1.2. Процес отримання даних з ДШ на основі системних функцій з використанням модулю kprobe

Для отримання ентропії з ДШ на основі системних функцій `add_input_randomness` (введення), `add_disk_randomness` (диски) також було створено модулі ядра. У них використовується `kprobe`, завдяки якому при виклику потрібних системних функцій викликається і необхідний обробник. Як і у випадку `IRQ` обробник обчислює дельту часу між викликами системних функцій і відмінність цих часових дельт. І далі з результату також отримуються вісім наймолодших бітів (LSB), які записуються до буфера ентропії.

Всередині модулів також створюються символічні псевдопристрої для можливості використання даних, отриманих модулем у користувацькому просторі.

- 1 Ініціалізація буфера ентропії
- 2 Визначення `kprobe` для перехоплення викликів функцій
- 3 Визначення спіллоку та черги очікування
- 4 Ініціалізація стану для обчислення джитеру (стан містить значення часу у мілісекундах, коли відбулося останнє переривання і значення останньої дельти між перериваннями)
- 5 Реалізація функції оцінки доступної ентропії у буфері
- 6 Реалізація функції обробки
- 7 Реалізація функції ініціалізації модуля
- 8 Реалізація функції вивільнення модуля – `__exit irq_entropy_exit`
- 9 Реалізація функції зчитування з буфера до простору користувача
- 10 Визначення структури, яка відповідатиме за функції, що викликатимуться через стандартний узагальнений інтерфейс псевдопристрою

Алгоритм 3. Модуль ядра Linux для збору ентропії з використанням `kprobe`

З використанням кожного з описаних модулів було зібрано набір зразків (байтів) довжини $> 1\,000\,000$, згідно з рекомендаціями NIST 800-90B [1]. Для подальшого використання представлених ДШ у процесі екстракції необхідно оцінити значення ентропії отриманих наборів даних шляхом застосування тестів `min-ентропії`, визначених у [1].

2.1.3. Оцінка ентропії обраних ДШ на основі отриманих вибірок за рекомендаціями NIST 800-90B

Для отриманих з ДШ вибірок було виконано оцінку показників мінімальної ентропії згідно з рекомендаціями NIST, показників ентропії Шеннона та колізійної ентропії. Результати для кожного з використаних ДШ наведені на рис. 2–4.

Результати вказують на те, що вибірки з ДШ на основі мережевих подій та подій роботи з дисками мають дещо вищі значення ентропії, ніж ДШ на основі введення користувача. Проте показники є доволі високими і на достатньому рівні.

Нижче наведено псевдокод реалізацій екстракторів ентропії на основі національних стандартів.

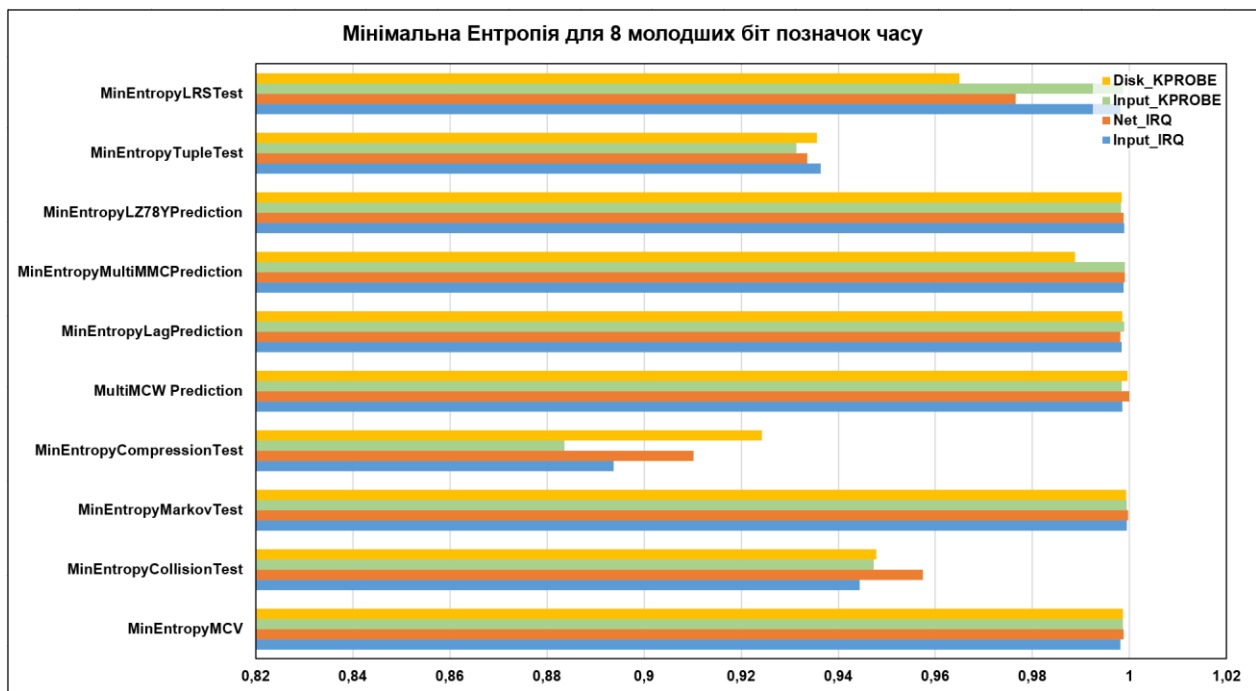


Рис. 2. Оцінки мінімальної ентропії обраних ДШ

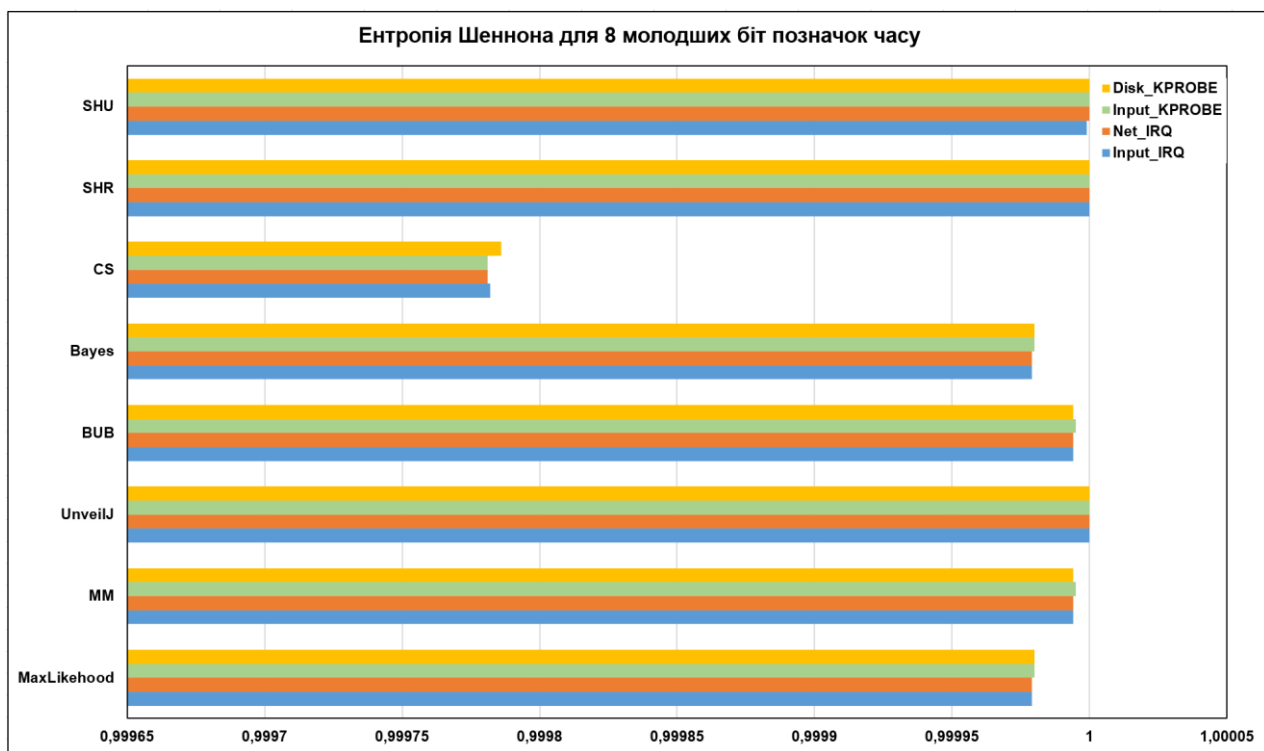


Рис. 3. Оцінки ентропії Шеннона обраних ДШ

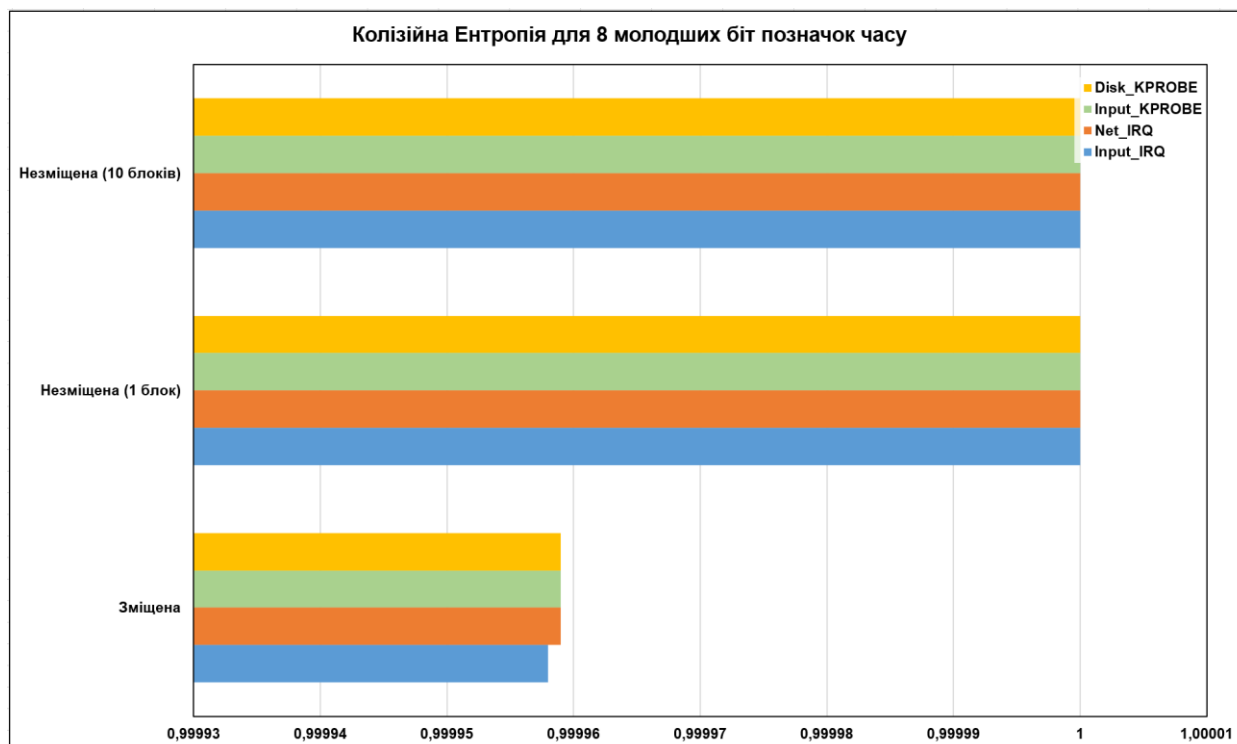


Рис. 4. Оцінки колізійної ентропії обраних ДШ

2.2. Реалізація екстрактора з використанням НМАС режиму геш функції Купина

Для реалізації екстрактора ентропії можливим є застосування криптопримітиву НМАС. Оскільки функція гешування Купина [4] не є перевіреною (довіреною) NIST, вихід екстрактора, побудованого з її використанням, потребуватиме додаткової оцінки за принципом, наведеним раніше.

Далі наведено реалізацію НМАС з використанням ДСТУ 7564:2014 «Купина» у вигляді псевдокоду. Для коректної реалізації НМАС важливо враховувати рекомендації [10, 11].

Вхід:

sk – ключ, відповідного рівня безпеки;
key_len – довжина ключа;
data – дані, для яких обчислюється MAC;
len – довжина даних.

Вихід:

mac – значення результуючого MAC необхідної довжини (в залежності від обраного режиму).

1 Виділення пам'яті для всіх даних, необхідних для обчислення MAC

buf[BLOCKSIZE + BLOCKSIZE / 2]

2 Виділення пам'яті для обчислення конкатенації ($K_0 \oplus ipad$) та data

temp[(BLOCKSIZE + len)]

3 if довжина ключа > BLOCKSIZE

Гешування ключа для отримання рядка та доповнення нулями до BLOCKSIZE

else if довжина ключа < BLOCKSIZE

Доповнення нулями до BLOCKSIZE

4 Виконання XOR для ключа та ipad

$K_0 \oplus ipad$ (ipad = байт 0x36 повторений BLOCKSIZE разів)

5 Конкатенація з вхідними даними

$K_0 \oplus ipad \parallel data$

6 Застосування Куруна256 або Куруна512 для обчислення гешу в залежності від обраного режиму
 $\text{Куруна256_}(512)(\text{buf} + \text{BLOCKSIZE}, \text{temp}, \text{BLOCKSIZE} + \text{len});$
 7 Виконання XOR для ключа та opad
 $K_0 \oplus \text{opad}$ (opad = байт 0x5C повторений BLOCKSIZE разів)
 8 Об'єднання з попередньо обчисленим гешем
 9 Застосування Куруна256 або Куруна512 для обчислення гешу для
 $K_0 \oplus \text{opad} \parallel H((K_0 \oplus \text{ipad}) \parallel \text{data})$
 $\text{Куруна512}(\text{buf}, \text{buf}, \text{BLOCKSIZE} + \text{BLOCKSIZE} / 2);$

Алгоритм 4. Куруна-НМАС

Вихідними даними алгоритму є сформований над вхідними даними МАС з використанням криптографічного алгоритму НМАС.

Загальний принцип використання екстрактора на основі режиму НМАС геш функції Калина наступний:

- отримання з розглянутих у п. 2.1 ДШ такої кількості даних, щоб ентропія вхідного рядка була максимально можливою для виходу обраного екстрактора (ентропія = nw – найвужчий внутрішній ширині екстрактора);
- застосування екстрактора для екстракції з вхідних даних рівномірного виходу довжиною nw з ентропією близькою до або рівною nw (256 бітний рядок з ентропією ≈ 256).

Схематичне зображення процесу виконання екстракції показано на рис. 5.

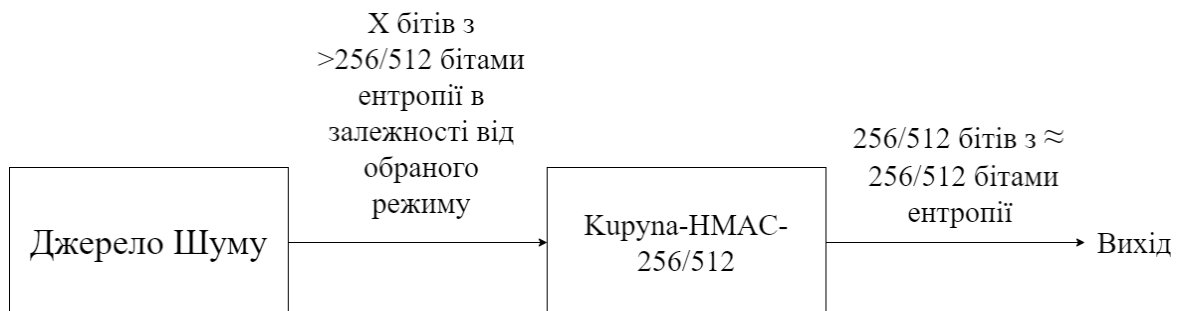


Рис. 5. Схематичне зображення екстрактору на основі Куруна-НМАС

На виході такого екстрактора, як показано на рисунку, очікується рядок довжини, яка відповідає розміру виходу геш функції з показниками ентропії, що $\approx$ ентропії вхідних даних.

2.3. Реалізація екстрактора з використанням алгоритму Hash_df за вимогами NIST 800-90A та NIST 800-90B на основі геш функції Куруна

Для реалізації екстрактора ентропії також можливим є використання алгоритму Hash_df (hash derivation function) – отримання похідної величини. Такий алгоритм схвалено для застосування у якості екстрактора ентропії у [1]. Сам алгоритм описано у [8]. У даному пункті наведено реалізацію Hash_df з використанням Куруни. Для коректної реалізації Hash_df важливо враховувати рекомендації [8].

Перевагою даного алгоритму над НМАС є відсутність необхідності у випадковому ключі, оскільки Hash_df є безключовою функцією.

Вхід:

input – дані, для яких обчислюється геш;

input_len – довжина даних;

no_of_bits_to_return – кількість бітів, які повинен повернути Hash_df (Для Hash_df довжина виводу, зазначена в табл. 1, 2 (Розмір виходу геш функції), використовується як вхідний параметр no_of_bits_to_return для виклику Hash_df [8])

Вихід:

result – результат виконання Hash_df.

1 Обчислення кількості ітерацій як no_of_bits_to_return/outlen (Оскільки згідно з [1, 8] для екстрактора ентропії no_of_bits_to_return=outlen цей крок може бути пропущений)

len = ceil(no_of_bits_to_return/KUPYNA_OUTLEN);

2 Виділення пам'яті для результату

temp = malloc(len*KUPYNA_OUTLEN);

3 Встановлення лічильника рівним 1

counter = 1;

4 Обчислення довжини конкатенації counter || no_of_bits_to_return || input

concat_len = len + 4 + input_len;

5 Виділення пам'яті для конкатенації

concat = malloc(concat_len);

6 Виконання конкатенації потрібних елементів

concat[0] = counter;

bits_to_return[4];

u32_to_bytes(bits_to_return, no_of_bits_to_return);

memcpy(concat + 1, bits_to_return, 4);

memcpy(concat + 5, input_string, input_len);

7 Застосування гешування до конкатенації

Kupyna256/512(concat, concat_len, digest);

8 Повернення отриманого гешу

result = digest

Алгоритм 5. Kupyna-Hash_df

Загальний принцип використання екстрактора на основі алгоритму Hash_df з геш функцією Купина такий самий як і для режиму НМАС.

Схематичне зображення процесу виконання екстракції показано на рис. 6.

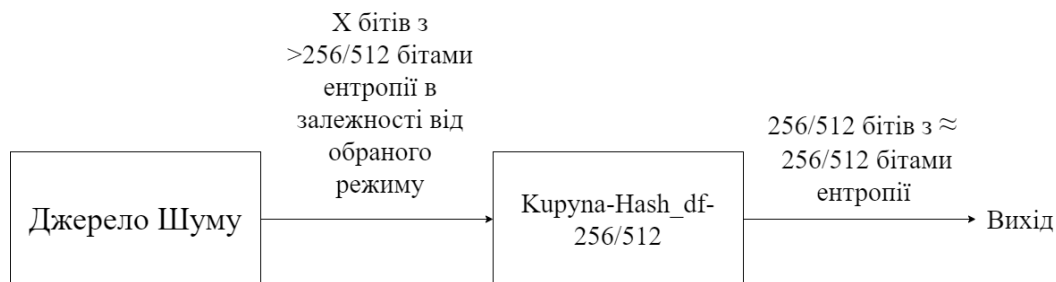


Рис. 6. Схематичне зображення екстрактору на основі алгоритму Hash_df з геш функцією Купина

На виході такого екстрактора, як показано на рисунку, очікується рядок довжини, яка відповідає розміру виходу геш функції з показниками ентропії, що $\approx$ ентропії вхідних даних.

2.4. Реалізація екстрактора з використанням СМАС режиму блокового шифру Калина

Ще одним можливим для використання у екстракторі криптографічним алгоритмом є СМАС. У стандарті Калина визначено використання алгоритму у такому режимі. У даному пункті наведено реалізацію СМАС з використанням Калини у вигляді псевдокоду.

```

Вхід:
input – дані, для яких обчислюється геш;
input_len – довжина даних;
q – довжина імітовставки (рекоменд. q = block_size)
ctx – контекст алгоритму Калина або (Раундові ключі (rnd_key), Розмір блоку
(nb), Розмір ключа (nk), Кількість раундів (nr))
Вихід:
h – обчислена імітовставка.
1 Доповнення повідомлення нулями, доки input_len mod block_size ≠ 0
2 if повідомлення було доповнене,
     $K_{\delta} = 1$ 
else
     $K_{\delta} = 0$ 
3 Встановлення бітів імітовставки C в нуль
4 Зашифрування  $K_{\delta}$ 
    KalynaEncipher(((uint64_t*)K_sigma, ctx, (uint64_t*)K_sigma);
5 Розбиття повідомлення на n блоків довжини block_size
6 Цикл від 1 до n-1
    Виконання XOR для C та оригінального повідомлення
    Зашифрування отриманого XOR та присвоєння результату імітовставці
7 Для останнього блоку
    Виконання XOR для C, оригінального повідомлення та  $K_{\delta}$ 
    Зашифрування отриманого XOR та присвоєння результату імітовставці

```

Алгоритм 6. Kalyna-CMAC

Загальний принцип використання екстрактора на основі СМАС режиму алгоритму Калина такий самий як і для попередніх екстракторів – отримання необхідної кількості даних з ДШ і виконання екстракції.

Схематичне зображення процесу виконання екстракції показано на рис. 7.

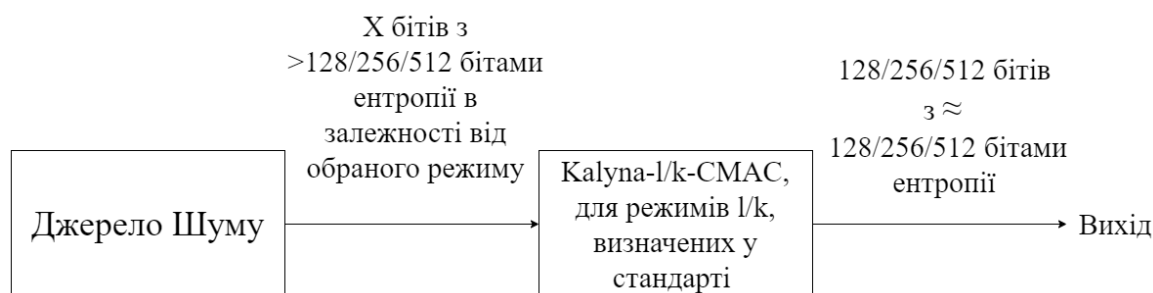


Рис. 7. Схематичне зображення екстрактору на основі Калина-СМАС

На виході такого екстрактора очікується рядок довжини, яка відповідає розміру блоку шифру з показниками ентропії, що $\approx$ ентропії вхідних даних.

Висновки

1. Проведено аналіз існуючих рекомендацій щодо побудування екстракторів ентропії на основі криптографічних примітивів. Цей процес потребує вибору відповідного джерела шуму, збору достатньо великого набору зразків з даного ДШ, для можливості подальшої

оцінки та виконання екстракції ентропії з використанням довіреного криптографічного компонента. Для усіх функцій і усіх режимів отримано прискорення не менше ніж в два рази, для більшості функцій та режимів прискорення більше ніж в три рази.

2. Виконано теоретичне обґрунтування можливості застосування національних криптографічних алгоритмів для виконання екстракції на основі подібності криптографічних примітивів та режимів, що застосовуються, до довірених NIST.

3. Наведено приклади практичної реалізації екстракторів на основі національних криптографічних алгоритмів з детальним описом та реалізацією всіх необхідних кроків. Зокрема показано практичну реалізацію процесу збирання зразків з нефізичних ДШ та оцінки показників ентропії цих ДШ за існуючими міжнародними рекомендаціями. Представлено практичну реалізацію кроку екстракції на основі національних алгоритмів ґешування та блокового шифрування.

4. У подальших дослідженнях планується розробка алгоритму екстракції `block_cipher_df` на основі алгоритму блокового шифрування Калина, перевірка відповідності виходів екстракторів на основі національних криптографічних алгоритмів необхідним вимогам щодо ентропії, а також застосування компонентів розширення виходу екстракторів на основі національних алгоритмів для отримання послідовностей довільної довжини.

Список літератури:

1. Turan M.S., Barker E., Kelsey J., McKay K., Baish M., Boyle M. (2018). NIST SP 800-90B. Recommendation for the Entropy Sources Used for Random Bit Generation. Available at: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90B.pdf>
2. Rodríguez L., Madarro-Capó E., Legón-Pérez C., Rojas O., Sosa-Gómez G. (2021). Selecting an Effective Entropy Estimator for Short Sequences of Bits and Bytes with Maximum Entropy. Available at: <https://doi.org/10.3390/e23050561>
3. Skorski M. (2016). Improved Estimation of Collision Entropy in High and Low-Entropy Regimes and Applications to Anomaly Detection. Available at: <https://eprint.iacr.org/2016/1035.pdf>
4. ДСТУ 7564:2014. Інформаційні технології. Криптографічний захист інформації. Функція ґешування. (2015).
5. ДСТУ 7624:2014. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення. (2016).
6. Müller S., Mayer S., Dr. Holz C., Dr. Hohenegger A. (2022). Documentation and Analysis of the Linux Random Number Generator. Version 5.0. Available at: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/LinuxRNG/LinuxRNG_EN_V5_0.pdf?blob=publicationFile&v=3
7. Müller S. (2025). Linux/dev/random—ANewApproach. Available at: <https://www.chronox.de/lrng/releases/v59/lrng-v59.pdf>
8. Barker E., Kelsey J. (2015). NIST SP 800-90A Rev. 1. Recommendation for Random Number Generation Using Deterministic Random Bit Generators. NIST. Available at: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf>
9. ДСТУ 8845:2019. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного потокового перетворення. (2019).
10. FIPS PUB 198-1. (2008). The Keyed-Hash Message Authentication Code (HMAC). Available at: <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.198-1.pdf>
11. Krawczyk H., Bellare M., Canetti R. (1997). RFC 2104. HMAC: Keyed-Hashing for Message Authentication. Available at: <https://datatracker.ietf.org/doc/html/rfc2104>

Надійшла до редколегії 23.10.2025

Відомості про авторів:

Дерев'янюк Ярослав Андрійович – Харківський національний університет імені В. Н. Каразіна, аспірант кафедри кібербезпеки інформаційних систем, мереж і технологій, навчально-наукового інституту комп'ютерних наук та штучного інтелекту, АТ «Інститут Інформаційних технологій», науковий співробітник-консультант; Україна; e-mail: varik0009258@gmail.com; ORCID: <https://orcid.org/0000-0002-3290-3373>

Горбенко Дмитро Юрійович – Харківський національний університет імені В.Н. Каразіна, студент кафедри кібербезпеки інформаційних систем, мереж і технологій, навчально-наукового інституту комп'ютерних наук та штучного інтелекту, АТ «Інститут інформаційних технологій», молодший інженер-програміст; Україна; e-mail: jsciiitua@gmail.com

*К.Є. ЛИСИЦЬКИЙ, PhD., І.В. ЛИСИЦЬКА, д-р техн. наук, І.М. ГАЛЬЦЕВА,
Є.П. КОЛОВАНОВА, канд. техн. наук*

ЕВОЛЮЦІЯ АРХІТЕКТУР БЛОКОВИХ СИМЕТРИЧНИХ ШИФРІВ

Вступ

Історія сучасних блокових симетричних шифрів (БСШ) – це історія пошуку оптимального поєднання двох фундаментальних принципів, сформульованих Клодом Елвудом Шенноном у 1949 р.: заплутування (confusion) та дифузії (diffusion).

Сучасні ітеративні блокові шифри, що перетворюють фіксований блок відкритого тексту на блок шифротексту за допомогою багаторазового застосування раундової функції, базуються переважно на двох архітектурних моделях: Мережі Фейстеля та Мережі Підстановки-Перестановки (SPN).

Формальний початок сучасної криптографії заклав американський математик Клод Елвуд Шеннон у відомій роботі "Теорія зв'язку в секретних системах" [1]. Фундаментальні принципи, які дозволяють отримати криптографічно стійке перетворення, згідно з Шенноном:

- заплутування (Confusion): розповсюдження впливу одного знаку відкритого тексту на багато знаків шифртексту, що дозволяє приховати статистичні властивості відкритого тексту. Спрямований на ускладнення зв'язку між ключем і шифротекстом. Досягається за допомогою нелінійних операцій, насамперед через використання S-блоків (Substitution-boxes);
- дифузія (Diffusion): використання таких шифруючих перетворень, які ускладнюють відновлення взаємозв'язку статистичних властивостей відкритого та шифрованого текстів. Спрямований на поширення впливу одного біта відкритого тексту (або ключа) на якомога більше бітів шифротексту. Досягається за допомогою лінійних операцій, таких як Р-блоки (Permutation-boxes).

Шеннон запропонував концепцію "product ciphers", в якій послідовно застосовують операції заміни та перестановки, заклавши основи для обох головних структур БСШ. Обидві основні типові структури – Мережа Фейстеля та SPN-мережа – були розроблені в рамках одного дослідного проєкту фірми IBM під назвою Lucifer (1971–1973) [2].

1. Огляд основних типових структур БСШ

1.1. Мережа Фейстеля

Мережа Фейстеля (Feistel Network) (винахідник: Хорст Фейстель (Horst Feistel), IBM) [3, 4]. Вперше застосована у другій версії шифру Lucifer (запатентована в 1971 р.). Проєкт "Люцифер" був скоріше експериментальним, але став базисом для алгоритму Data Encryption Standard (DES). В 1977 р. DES став стандартом в США на шифрування даних і до останнього часу широко використовувався в криптографічних системах. Ітеративна структура алгоритму дозволяла спростити його реалізацію в програмних і апаратних середовищах. В 1987 р. були розроблені алгоритми FEAL і RC2. Широке поширення мережі Фейстеля отримали в 1990-і роки, коли з'явилися такі алгоритми, як Blowfish, CAST-128, TEA, XTEA, XXTEA, RC5, RC6 та ін. Ця конструкція була широко вивчена криптографами в силу її великого поширення.

Мережа Фейстеля, як відомо, має наступну структуру. Вхідний блок ділиться на кілька рівної довжини підблоків, званих гілками. У разі, якщо блок має довжину 64 біта, використовуються дві гілки по 32 біта кожна. Кожна гілка обробляється незалежно від іншої, після чого здійснюється циклічний зсув всіх гілок вліво. Таке перетворення виконується кілька циклів або раундів. У разі двох гілок кожен раунд має структуру, показану на рис. 1.

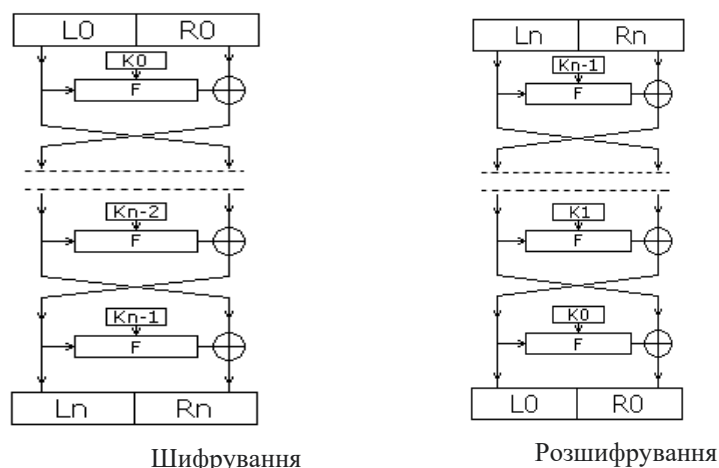


Рис. 1. Структура мережа Фейстеля

Функція F називається твірною. Кожен раунд складається з обчислення функції F для однієї гілки і побітового виконання операції XOR результату F з іншою гілкою. Після цього гілки міняються місцями. Вважається, що оптимальне число раундів – від 8 до 32. Важливим є те, що збільшення кількості раундів значно збільшує криптостійкість алгоритму. Можливо, ця особливість і вплинула на настільки активне поширення мережі Фейстеля, так як для більшої криптостійкості досить просто збільшити кількість раундів, не змінюючи сам алгоритм. Мережа Фейстеля є оборотною навіть у тому випадку, якщо функція F не є такою, тому що для розшифрування не потрібно обчислювати F^{-1} . При розшифруванні на вхід подається зашифрований текст, і ключі використовуються в зворотному порядку.

В 1988 р. Майкл Любі (Michael Luby) і Чарльз Ракофф (Charles Rackoff) дослідили криптостійкості мережі Фейстеля і довели, що якщо раундова функція є псевдовипадковою і використовувані ключі незалежні у кожному раунді, то трьох раундів буде достатньо для того, щоб блочний шифр був псевдовипадковою перестановкою, тоді як чотирьох раундів буде достатньо для того, щоб зробити сильну псевдовипадкову перестановку [5].

Псевдовипадковою перестановкою Любі і Ракофф назвали таку, яка стійка до атаки з адаптивним вибором відкритого тексту, а сильною псевдовипадковою перестановкою – псевдовипадкову перестановку стійку до атаки з використанням обраного шифрованого тексту.

Надалі, в 1997 р., Моні Наор (Moni Naor) і Омер Рейнголда (Omer Reingold) запропонували спрощений варіант конструкції Любі – Ракофф з чотирьох раундів, де в якості першого і останнього раунду використовуються дві попарно незалежні перестановки. Два середніх раунди конструкції Наор – Рейнголда ідентичні раундам в конструкції Любі – Ракофф [6].

Більшість же досліджень присвячено вивченню конкретних алгоритмів. У багатьох блокових шифрах на основі мережі Фейстеля були знайдені ті чи інші уразливості, проте в більшості випадків ці уразливості є суто теоретичними.

1.2. Мережа підстановки-перестановки (SPN)

Структура SPN була менш популярною, ніж структура Фейстеля, до 2000-х років, коли вона стала архітектурною основою для AES (Advanced Encryption Standard), демонструючи високу ефективність у програмному забезпеченні [7].

У 2000 р. було завершено міжнародний проєкт по створенню алгоритму шифрування AES (Advanced Стандарт шифрування). В результаті інтенсивної спільної роботи провідних криптологів світу було глибоко проаналізовані та досліджені властивості 15 алгоритмів – кандидатів на стандарт симетричного блочного шифра XXI століття. Після завершення проєкту досліджувався алгоритм Rijndael спеціальними підрозділами Агентства національної безпеки США на відповідність заданому рівню стійкості, можливостей і умов застосування

для захисту несекретної інформації в державних і комерційних структурах США. Таким чином, для заміни алгоритму DES і Triple DES (FIPS-46-3) було прийнято новий алгоритм симетричного блокового шифрування, який офіційно введено в дію в якості федерального стандарту США – AES (FIPS-197). Структуру SPN мережі представлено на рис. 2.

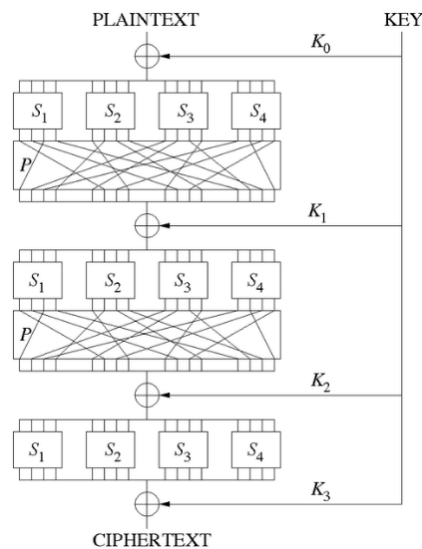


Рис. 2. Схема трираундової SPN мережі, що шифрує 16 біт вхідного тексту в 16 біт вихідного

Крім того, в 2000 р. був розпочатий проєкт NESSIE (Нові європейські схеми для підписів, цілісності та шифрування), метою якого є створення кількох криптографічних примітивів, серед яких є і симетричний блоковий шифр [8]. По суті, до цього часу проєкт уже був обраний законодавчо та було прийнято попереднє рішення про те, що серед блокових алгоритмів найкраще підходять Rijndael, Camellia і Шакал-2. Вони і були рекомендовані в якості стандартів Європейського Союзу [9].

1.3. Конструкція Лея – Мессі

Розроблена Сюецзя Леєм та Джеймсом Л. Мессі (1990) як альтернатива структурі ланцюг Фейстеля. Вона використовує операцію на основі різниці між двома половинами блоку, що забезпечує швидшу дифузію. Найвідоміший приклад – шифр IDEA [10,11]. Схема Лея – Мессі є альтернативною високорівневою конструкцією блокових симетричних шифрів. На її основі побудовано алгоритми FOX, «Мухомор» та ін. Основною перевагою схеми Лея – Мессі, як і ланцюга Фейстеля, є можливість побудови інволютивного перетворення, тобто розшифрування реалізовано практично аналогічно до зашифрування при використанні зворотного порядку раундових з'єднань [12]. Конструкція Лея – Мессі представлена на рис. 3.

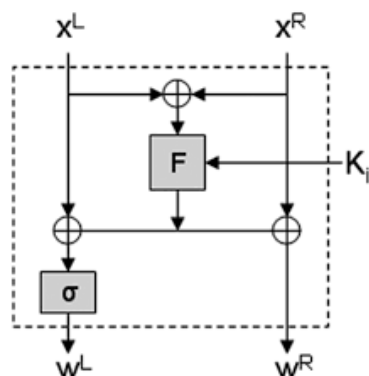


Рис. 3. Конструкція Лея – Мессі

Додатковою перевагою цієї конструкції є відсутність вимог до бієктивності раундової функції (як у SPN-структур), що спрощує розробку та реалізацію. Головна перевага схеми Лея – Мессі над мережею Фейстеля полягає у швидшій дифузії та забезпеченні бієктивності (оборотності) шифру, навіть якщо раундова функція не є інвертованою. Тобто конструкція Лея – Мессі є елегантною альтернативою, що забезпечує високу стійкість при збереженні зручності інволютивного обернення. Важливі характеристики типових конструкцій БСШ представлено у табл. 1.

Таблиця 1

Характеристики типових конструкцій БСШ

Характеристика	Мережа Лея – Мессі (LM)	Мережа Фейстеля (FN)	Мережа SPN
Поділ блоку	Ділиться на дві половини.	Ділиться на дві половини.	Обробляється як ціле.
Вимоги	Не вимагає інвертування (може бути довільною).	Не вимагає інвертування (може бути довільною).	Повинна бути інвертованою (як частина раунду).
Оборотність	Досягається легко завдяки симетричній структурі.	Досягається легко завдяки структурі.	Вимагає окремих обернених операцій у кожному шарі.
Дифузія	Дуже швидка. Змішує обидві частини одночасно.	Повільніша (інформація передається через XOR).	Дуже швидка (завдяки Р-блоку).
Кількість раундів (загальна)	Зазвичай менша кількість раундів, ніж FN, для забезпечення безпеки.	Зазвичай більша кількість раундів для досягнення необхідної безпеки.	Кількість раундів середня (залежить від розміру блоку та раундової функції).
Паралелізм (шифрування)	Високий. Операції в раунді можуть виконуватись паралельно.	Низький/Середній. Обчислення лівої частини залежить від правої з попереднього раунду.	Високий. Операції в межах шару (S-блоки) можуть виконуватись паралельно.
Обернення (дешифрування)	Використовує ту саму функцію раунду та ті самі ключі в оберненому порядку.	Використовує ту саму функцію раунду та ті самі ключі в оберненому порядку.	Використовує обернені функції раунду та ключі в оберненому порядку.

1.4. Гібриди та інші конструкції

Криптографи почали активно досліджувати альтернативні структури, щоб подолати обмеження або покращити доказову безпеку класичних моделей. Наприклад узагальнена Мережа Фейстеля (GFN) використовує поділ блоку на більш ніж дві частини. Це дозволяє більш гнучко проєктувати шифри для великих блоків, як, наприклад, CAST-256 та RC6 [13]. Існують також інші архітектури або їх гібриди.

Конструкції ARX (Add-Rotate-XOR) виникли як пряма відповідь на необхідність створення надшвидких симетричних шифрів, які ідеально працюють на сучасних 32- та 64-бітних процесорах (ПК, сервери, мобільні пристрої). Конструкції ARX (Add-Rotate-XOR) особливо ефективні в програмному забезпеченні але їхня безпека повністю залежить від нелінійності модульного додавання. Приклади: ChaCha20 [14], Speck. Шифри Salsa20/ChaCha20 (хоча вони часто класифікуються як потокові шифри, їхня внутрішня функція є блоковою ARX-структурою).

Традиційні S-блоки (особливо великі, як в AES) вимагають доступу до таблиці підстановок, що може призводити до кеш-промахів (cache misses) та вносити затримки (латентність). Крім того, операції з таблицями можуть бути вразливими до атак по сторонніх каналах (timing attacks).

У ARX-конструкціях функцію нелінійного заплутування (Confusion), яку зазвичай виконує S-блок, забезпечує операція модульного додавання, оскільки вона не є лінійною, на відміну від XOR та циклічного зсуву.

Рекурсивна (вкладена) Мережа Фейстеля – це мережа Фейстеля, де сама раундова функція також є невеликою 3-раундовою мережею Фейстеля. Перетворення створює "матрьошку" з криптографічних структур. Типові приклади – шифр MISTY1 [15] та його наступник KASUMI (який використовується в стандартах мобільного зв'язку 3G/GSM) використовують цю вкладену структуру [16]. Рекурсивний дизайн спрощує математичний доказ того, що шифр є стійким до диференціального та лінійного криптоаналізу.

Ці конструкції забезпечують необхідні криптографічні властивості: плутанину (залежність шифротексту від ключа) та дифузію (поширення впливу бітів відкритого тексту по всьому шифротексту) протягом кількох раундів.

Таким чином, сучасна архітектура БСШ є прямим наслідком фундаментальних принципів Шеннона та практичних реалізацій IBM, які започаткували епоху Фейстеля та SPN, що домінує й сьогодні. Однак криптографи постійно досліджують нові архітектури для оптимізації безпеки та продуктивності у різних обчислювальних середовищах.

2. Місце БСШ у постквантовій криптографії

Алгоритм Гровера (Grover's algorithm) [17] є найвідомішою квантовою атакою на симетричні шифри. Він не "ламає" симетричні шифри, як алгоритм Шора, але прискорює атаку повним перебором (brute-force attack). Для симетричного шифру з ключем довжиною L біт, час, необхідний для повного перебору, пропорційний $O(2^L)$. Тобто Алгоритм Гровера може зменшити кількість операцій, необхідних для пошуку ключа, до $O(\sqrt{2^L})$ або $O(2^{\frac{L}{2}})$.

Щоб зберегти необхідний "постквантовий" рівень безпеки у 2^{128} (який вважається сьогодні стандартним для довгострокового захисту), просто подвоюють довжину ключа. Саме тому AES-256 є квантово-стійким до атаки Гровера. Його 2^{128} операцій все ще залишаються обчислювально нездійсненними для будь-якого комп'ютера (навіть квантового) у доступному майбутньому [18].

Таким чином, у постквантову еру блокові симетричні шифри залишаються критично важливими і продовжуватимуть використовуватися, вимагаючи лише переходу на довші ключі (128-бітна безпека вимагає 256-бітного ключа) [19].

3. Зміна пріоритетів

Сучасна еволюція БСШ є відповіддю не лише на теоретичні атаки, але й на практичні обмеження апаратного забезпечення. З поширенням Інтернету Речей (IoT) та вбудованих систем, криптографи змістили фокус з пошуку найстійкішого шифру на пошук найефективнішого шифру для обмежених ресурсів. Традиційні шифри (як AES) були оптимізовані для програмної швидкості на потужних процесорах, використовуючи великі S-блоки (8x8 біт в AES) і складні операції (MixColumns). У легкій криптографії пріоритет змінюється.

Один з напрямків – ідея мінімалізму раундової функції. Алгоритми, орієнтовані на апаратну реалізацію, такі як PRESENT (блоковий шифр для RFID-міток), використовують дуже маленькі S-блоки (4x4 біти) та прості перестановки, щоб мінімізувати площу кристала (Gate Count) [20]. Це вимагає значного збільшення кількості раундів для компенсації повільнішої дифузії та слабшого заплутування на раунд.

Також для програмної реалізації на 32- або 64-бітних процесорах, де S-блоки можуть бути неефективними, конструкції ARX (Add-Rotate-XOR) домінують (ChaCha20, Speck) [21].

Вони використовують лише операції, які процесор виконує за один такт, забезпечуючи високу швидкість і мінімальну латентність [22].

Мінімізація Gate Count: замість швидкості, головна мета – зменшити кількість логічних вентилів (Gates) на кристалі, що прямо впливає на вартість виробництва, розмір чипа та енергоспоживання [23].

Використання простих операцій: для досягнення цієї мети шифри, подібні до PRESENT, використовують дуже маленькі S-блоки (4x4 біти): Це значно зменшує апаратні витрати на реалізацію таблиці підстановок, порівняно з 8x8 блоками AES.

Прості глобальні перестановки: складні лінійні шари (як MixColumns в AES) замінюються простими побітовими перестановками.

Компенсація для збереження криптостійкості досягається через значне збільшення кількості раундів. Наприклад, шифр PRESENT має 31 раунд, що значно більше, ніж 10 – 14 раундів AES, але його апаратний розмір залишається мінімальним.

Цей мінімалістичний підхід критично важливий для пристроїв з вкрай обмеженими ресурсами:

- RFID-мітки (ідеальне застосування PRESENT);
- бездротові сенсорні мережі (WSN);
- датчики IoT з живленням від батарейок.

Мінімалізм раундової функції – це архітектурна адаптація БСШ до вимог економічності та енергоефективності, при цьому зберігається необхідний рівень стійкості через ітеративне повторення.

Висновки

Сучасна архітектура блокових симетричних шифрів є прямим наслідком і постійною реалізацією двох фундаментальних принципів, сформульованих Клодом Шенноном у 1949 р.: Заплутування (Confusion) та Дифузії (Diffusion). Історія БСШ – це історія пошуку оптимального балансу між цими двома властивостями для забезпечення криптографічної стійкості. Цей пошук породив дві класичні ітеративні структури, розроблені IBM: мережу Фейстеля (FN) та мережу Підстановки-Перестановки (SPN).

Незважаючи на домінування SPN після конкурсу AES, криптографи активно досліджують альтернативні та гібридні конструкції (Лея – Мессі, GFN, Рекурсивна FN). Це продиктоване не лише теоретичними міркуваннями (доказова безпека, як у MISTY1), але й потребою в оптимізації для різних обчислювальних середовищ.

Симетричні блокові шифри зберігають свою критичну важливість у постквантовій криптографії. Хоча алгоритм Гровера теоретично зменшує ефективну довжину ключа вдвічі, це не призводить до їхньої повної компрометації.

Таким чином, сучасна архітектура БСШ є динамічною галуззю, що ефективно адаптується до квантових загроз та вимог мінімалізму апаратного забезпечення.

Список літератури:

1. Shannon C. E. A communication theory of secrecy systems // Bell System Technical Journal. 1949. Vol. 28, № 4. P. 656–715.
2. Feistel H. Cryptography and computer privacy // Scientific American. 1973. Vol. 228, № 5. P. 15–23.
3. Stallings W. Cryptography and Network Security: Principles and Practice (8th ed.). Pearson, 2023.
4. ISO/IEC 18033-3:2010. Information technology – Security techniques – Encryption algorithms. Part 3: Block ciphers. International Organization for Standardization, 2010.
5. Luby M., & Rackoff C. Pseudorandomness and Cryptographic Applications // Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing. ACM, 1988. P. 348–355.
6. Naor M., & Reingold O. On the Construction of Pseudorandom Permutations: Luby-Rackoff Revisited // Journal of Cryptology. 1999. Vol. 12, № 1. P. 29–66.
7. NIST (National Institute of Standards and Technology). FIPS PUB 197: Advanced Encryption Standard (AES). Washington, D.C. : U.S. Department of Commerce, 2001.
8. Schneier B., & Whiting D. A performance comparison of the AES submissions // AES Conference Proceedings. NIST, 1999.

9. NESSIE Consortium. NESSIE Project Final Report. [Електронний ресурс]. 2003. URL: [Вставити офіційне посилання на звіт NESSIE].
10. Lai X., & Massey J. L. A Proposal for a New Block Encryption Standard. Advances in Cryptology–EUROCRYPT '90. Springer, Berlin, Heidelberg, 1991. P. 389–404.
11. Preneel B. The International Data Encryption Algorithm (IDEA) // The Handbook of Security. Auerbach Publications, 2003.
12. Menezes A. J., van Oorschot P. C., & Vanstone S. A. Handbook of Applied Cryptography. Boca Raton : CRC Press, 1997. P. 250–252.
13. Schneier B., Mook D., & Mook J. The CAST-256 algorithm. Software for Data Security, 1999.
14. Bernstein D. J. ChaCha, a variant of Salsa20. Advances in Cryptology – SAC 2008. Springer, 2008. P. 138–170.
15. Matsui M. New block encryption algorithm MISTY. Fast Software Encryption – FSE '97. Springer, 1997. P. 54–68.
16. 3GPP TS 35.202. 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Specification of the 3GPP confidentiality and integrity algorithms; Document 2: KASUMI specification. 2004.
17. Grover L. K. A fast quantum mechanical algorithm for database search // Proceedings of the twenty-eighth annual ACM symposium on Theory of computing. 1996. P. 212–219.
18. NIST SP 800-57 Part 1 Rev. 5. Recommendation for Key Management: Part 1 – General. NIST, 2020.
19. Bernstein D. J., & Lange T. Post-quantum cryptography // Nature. 2017. Vol. 549, № 7671. P. 188–194.
20. Andres C., Biryukov A., D'Haeseleer J., Indesteege S., & Leurent G. PRESENT: An Ultra-Lightweight Block Cipher. CHES 2007. Springer, 2007. P. 450–464.
21. Bernstein D. J. ChaCha, a variant of Salsa20. Advances in Cryptology – SAC 2008. Springer, 2008. P. 138–170.
22. Eisenbarth T., Gong L., & Kniffler A. A Survey of Lightweight Cryptography Implementations on FPGAs // IACR Transactions on Cryptographic Hardware and Embedded Systems, 2021.
23. Beaulieu S., Shors J., Smith J., Treatman-Clark S., Weeks B., & Wingers L. The SIMON and SPECK lightweight block ciphers // 4th Workshop on RFID Security, 2013.

Надійшла до редколегії 10.10.2025

Відомості про авторів:

Лисицький Костянтин Євгенійович – PhD, Харківський національний університет імені В. Н. Каразіна, доцент кафедри математичного моделювання і аналізу даних; навчально-науковий інститут комп'ютерних наук та штучного інтелекту; Національний аерокосмічний університет "Харківський авіаційний інститут", ст. викладач кафедри комп'ютерних систем, мереж і кібербезпеки; Україна; e-mail: constantin.lisickiy@gmail.com; ORCID: <https://orcid.org/0000-0002-7772-3376>

Лисицька Ірина Вікторівна – д.т.н., професор, Харківський національний університет імені В. Н. Каразіна, професор кафедри кібербезпеки інформаційних систем, мереж і технологій, навчально-науковий інститут комп'ютерних наук та штучного інтелекту; Харківський національний університет радіоелектроніки, професор кафедри безпеки інформаційних технологій; Україна; e-mail: ivlisitska@karazin.ua; ORCID: <https://orcid.org/0000-0001-6758-9516>

Гальцева Ірина Михайлівна – старший викладач кафедри кібербезпеки інформаційних систем, мереж і технологій; Харківський національний університет імені В. Н. Каразіна; навчально-науковий інститут комп'ютерних наук та штучного інтелекту; Україна; e-mail: irina.galceva@karazin.ua

Колованова Євгенія Павлівна – канд. техн. наук, Харківський національний університет імені В.Н. Каразіна, доцент кафедри кібербезпеки інформаційних систем, мереж і технологій; навчально-науковий інститут комп'ютерних наук та штучного інтелекту; Харківський національний університет радіоелектроніки, доцент кафедри безпеки інформаційних технологій; Україна; e-mail: e.kolovanova@gmail.com; ORCID: <https://orcid.org/0000-0002-0326-2394>

*Р.І. МОРДВІНОВ, канд. техн. наук***СИСТЕМАТИЗАЦІЯ МЕТОДІВ ДОКАЗУ З НУЛЬОВИМ РОЗГОЛОШЕННЯМ****Вступ**

Приватність та безпека інформації є ключовими вимогами сучасних інформаційних систем. Докази з нульовим розголошенням (ZKP) – це криптографічні протоколи, що дають змогу одній стороні (доказуючому) довести іншій (верифікатору) істинність деякого твердження, не розкриваючи при цьому ніяких додаткових даних, окрім самого факту істинності [1]. Концепція ZKP була вперше сформульована в 1980-х роках у роботах Голдвассер, Мікалі та Ракова [1], де було введено поняття «складності знання» інтерактивних доказів. Відтоді теорія доказів з нульовим знанням інтенсивно розвивалася: було показано, що за наявності односторонніх функцій будь-яка належна до NP мова має доведення з нульовим знанням [6]. Класичними прикладами є протоколи ідентифікації, як-от схема Фіата–Шаміра [3] чи протокол Шнорра [5], що дозволяють довести знання секретного ключа без його розголошення.

Актуальність технологій ZKP стрімко зросла у 2010-х роках у зв'язку з потребою забезпечення конфіденційності в блокчейнах, фінансових транзакціях та інших сферах [7, 11]. Поява практичних реалізацій, зокрема стислих неінтерактивних доказів знання (zk-SNARK) [7] і масштабованих прозорих доказів (zk-STARK) [8], продемонструвала можливість використання ZKP в реальних застосунках – від анонімних криптовалютних платежів до перевірки правильності виконання обчислень на стороні. Це зумовило потребу у впорядкуванні знань про різні методи ZKP, їх класифікації та оцінці сильних і слабких сторін.

Методи доказу з нульовим розголошенням можна класифікувати за кількома ключовими ознаками [2, 11]. Однією з базових є тип взаємодії між доказуючим і верифікатором. За цим критерієм розрізняють інтерактивні протоколи ZKP та неінтерактивні. В інтерактивних протоколах потрібен багаторазовий обмін повідомленнями: верифікатор надсилає випадкові виклики (запити), на які доказуючий відповідає, і така процедура повторюється кілька раундів для досягнення високого рівня довіри [3, 4]. Натомість неінтерактивні докази дозволяють обмежитися одним повідомленням від доказуючого, яке верифікатор може перевірити самостійно без подальших запитань [7]. Перетворення інтерактивного протоколу на неінтерактивний можливе, наприклад, за допомогою геш-евристики Фіата–Шаміра [3, 23]. Неінтерактивні ZKP є особливо привабливими для практичних застосувань (наприклад, у блокчейнах), оскільки не потребують онлайн-взаємодії сторін.

Другим важливим критерієм є математична основа та структура протоколу. За цією ознакою в роботі пропонується виділити алгебраїчні та стохастичні методи доказу. Алгебраїчні методи ґрунтуються на використанні алгебраїчних структур та рівнянь над ними: наприклад, групи з обчислювально складними задачами (дискретний логарифм, факторизація тощо) або поліноміальні представлення обчислень [7, 8]. Такі протоколи часто будуються як σ -протоколи (Sigma-protocols) з трьохходовою схемою «зобов'язання-виклик-відповідь» і мають строгі алгебраїчні властивості (наприклад, лінійність відповідей), що спрощує доказ коректності та нульового розголошення [2, 5]. Натомість стохастичні методи спираються на випадковість та ймовірнісне переконання верифікатора. До них належать, наприклад, класичні протоколи Блума для NP-повних задач (графовий ізоморфізм, гамільтонів цикл тощо), де доказуючий приховує секрет випадковим чином і з певною ймовірністю проходить перевірку [4]. Характерною рисою стохастичних протоколів є наявність ненульової ймовірності обману, тому для надійності їх повторюють багаторазово, зменшуючи цю ймовірність до незначної величини (наприклад, 2^{-20} або менше) [4]. Таким чином, алгебраїчні методи зазвичай дають детермінований результат за один раунд (спираючись на

складні алгебраїчні припущення), тоді як стохастичні потребують статистичного підходу з повторенням раундів.

Наступний критерій – умови початкової довіри. Деякі сучасні протоколи потребують так званої довіреної установки (trusted setup): одноразової генерації загальних параметрів, які потім використовуються для побудови доказів [7]. Приклад – zk-SNARK, де на етапі ініціалізації генерується пара ключів (для доказуючого і верифікатора) з використанням випадкових секретних значень, що мають бути знищені після процедури. Якщо зловмисник отримає доступ до “токсичних” залишків цієї установки, він зможе підробляти докази [7]. Наявність довіреної установки вважається недоліком, адже вимагає абсолютної чесності учасників на початковому етапі. Альтернативою є прозорі (transparent) протоколи, які не потребують секретної установки – всі їх параметри генеруються відкрито, наприклад, з публічного випадкового “маяка” [8]. До прозорих належать zk-STARK та низка новітніх систем, що підвищує довіру до них, оскільки відпадає ризик компрометації прихованих параметрів.

Важливими класифікаційними характеристиками також є тип гарантії нульового знання (перфектне, статистичне чи обчислювальне нульове знання [2]) та вид доказової моделі (доказ знання проти доказу існування). Перфектне нульове розголошення означає, що верифікатор взагалі не може отримати інформацію про секрет (у сильному теоретичному сенсі рівності розподілів), статистичне допускає мізерну похибку, а обчислювальне – гарантує нульове знання лише за припущення обмеженості обчислювальних можливостей верифікатора [2]. Більшість практичних схем (наприклад, zk-SNARK) забезпечують обчислювальне нульове знання, оскільки спираються на криптографічні примітиви (хеш-функції, шифрування тощо) [7]. Щодо доказової моделі, то протоколи можуть доводити саме знання секрета (arguments of knowledge) або просто факт існування рішення без його розкриття. Докази знання потребують додаткової властивості – повноти по знанню, яка гарантує, що доказуючий не лише переконує в істинності твердження, а й володіє певною інформацією (наприклад, приватним ключем) [1, 2]. ZKP-протоколи за визначенням часто розглядаються як докази знання.

Також важливо зазначити і постквантові підходи для доказу з нульовим розголошенням. Незважаючи на успіхи zk-SNARK та zk-STARK, питання стійкості протоколів ZKP до атак квантових обчислювачів залишається відкритим. Прозорі хеш-базовані схеми на зразок zk-STARK уже володіють постквантовою стійкістю, проте мають великий розмір доказів (десятки чи сотні кілобайт). Альтернативним напрямом є використання решіткових крипто-систем. Розроблено низку рішень на решітках, що теоретично забезпечують постквантове нульове розголошення. Наприклад, схема на основі задач SIS/LWE демонструє ZK-доказ знання з гарантією стійкості до квантових атак, однак ціна – дуже громіздкі докази (порядку сотень кілобайт) [13]. Це ускладнює практичне застосування таких схем. В останні роки запропоновано нові техніки оптимізації решіткових доказів. Зокрема, на CRYPTO 2023 представлено гібридну схему з «точними/релаксованими» доказами на решітках, що суттєво підвищує ефективність перевірки округлень і пов'язаних примітивів [14]. Подібні роботи спрямовані на скорочення розміру і часу перевірки решіткових ZK-доказів без втрати безпеки. Водночас ідеї квантових доказів з нульовим знанням поки що носять переважно академічний характер. Існують концепції «сліпих» квантових доказів, у яких обмін повідомленнями відбувається квантовими станами замість класичних бітів, або протоколи перевірки квантових обчислень із класичним верифікатором. Втім, такі квантові ZKP перебувають на ранніх стадіях досліджень і далекі від практичного застосування. Отже, досягнення постквантової стійкості ZKP наразі спираються на класичні криптосистеми (хеші, решітки тощо) та потребують подальшого вдосконалення для досягнення прийнятної продуктивності. Вирішення цих проблем є критично важливим, адже впровадження стійких до квантових атак ZKP дозволить зберегти безпечність блокчейн-систем і конфіденційність даних у майбутньому еру квантових обчислень.

Одним із проривів останніх років стало впровадження рекурсивних доказів – техніки, що дозволяє вкладати один ZK-доказ у інший, утворюючи ланцюжок доказів. Це означає, що можна породити короткий доказ правильності одразу серії тверджень, де кожне наступне твердження підтверджує коректність попереднього. Рекурсія фактично реалізує ідею інкрементально верифікованих обчислень (IVC). Сучасні системи, такі як Halo 2 та Nova, демонструють практичність цього підходу – вони дозволяють доводити коректність довготривалих обчислювальних процесів, розбиваючи їх на кроки і перевіряючи кожен крок рекурсивно. Nova, зокрема, є одним із найпростіших і найшвидших рекурсивних доказових механізмів: вона потребує лише сталого обсягу обчислень для верифікації незалежно від числа кроків, а її доказувач працює дуже ефективно. Ключова ідея Nova – використання схем складання (folding schemes), що зводять перевірку двох тверджень NP до перевірки одного, з меншим навантаженням. SuperNova розвиває ці ідеї далі, дозволяючи доводити правильність виконання довільних програм без побудови універсальних схем (тобто без «універсальних» кіл) [16]. Рекурсивні докази відкривають шлях до масштабування блокчейн-систем: з їх допомогою тисячі транзакцій можуть бути «згорнуті» в один стислий доказ, придатний для публікації в основному ланцюжку (т.зв. zk-Rollup). Це дуже підвищує пропускну здатність мережі та знижує витрати, адже навантаження на основний блокчейн мінімізується [17]. Дійсно, у системах StarkNet, zkSync, Polygon та ін. вже реалізовано таку масштабованість: L2-ланцюжки генерують ZK-докази правильності великих пакетів транзакцій, і мережа L1 валідує лише цей доказ замість усіх транзакцій. Іншим напрямом оптимізації є агрегація доказів, що дозволяє об'єднувати кілька незалежних ZK-доказів у один. Агрегування спрощує масову верифікацію: наприклад, метод SnarkPack дає змогу звести 8192 окремих SNARK-доказів в один пакет за 8,7 с, який перевіряється за 163 мс. Такий підхід експоненційно прискорює перевірку порівняно з поодинокими доказами [15]. Комбінація рекурсії та агрегування забезпечує значне підвищення ефективності: рекурсія скорочує загальний обсяг даних (шляхом вкладення доказів), а агрегування зменшує витрати на їх перевірку. Завдяки цьому сучасні протоколи можуть гарантувати як скейлінг, так і збереження приватності: блокчейн-операції, складні обчислення чи навіть цілі програми можуть бути доказані з нульовим розголошенням настільки ефективно, що це придатно для практичного використання у реальних системах.

Отже, для систематизації методів ZKP доцільно використовувати такі ключові критерії: інтерактивність (наявність багаторазового обміну vs. одноразові схеми), необхідність довіреної установки (наявність vs. відсутність), алгебраїчна чи стохастична природа протоколу, тип нульового розголошення (перфектне/статистичне/обчислювальне), криптографічні припущення (на яких завданнях ґрунтується безпека) та ефективність (обсяг переданих даних і обчислювальні витрати). На основі цих ознак буде здійснюється класифікація основних підходів до побудови доказів з нульовим знанням.

Перші практичні реалізації ZKP для доказу знання секрета у групах із складною задачею дискретного логарифма (DL) ґрунтуються на трьохходових σ -протоколах – схемі Фіата–Шаміра, Шнорра та їх численних узагальненнях [3]. Сучасні варіанти активно застосовують:

- Σ -протоколи над еліптичними кривими – в основі протоколів ідентифікації й e-cash;
- Σ -протоколи для знання факторизації (e.g., Okamoto-Uchiyama) – у системах e-vote;
- Σ -протоколи з агрегуванням – забезпечують паралельне об'єднання доказів і зменшують розмір повідомлень.

Починаючи з роботи Pinocchio (2013) й особливо статті Ben-Sasson та ін. [4] неінтерактивні докази стали практичними для великих обчислень. Характерні риси:

- довірена токсична установка (trusted setup);
- лінійна ($O(n)$) генерація доказу, але логарифмічна верифікація;
- розмір доказу < 1 кБ;
- обчислювальна модель Rank-1 Constraint System (R1CS).

До сучасних представників належать Groth16 [5], PLONK [9], Halo 2 [10], які оптимізують розмір ключів та підтримують рекурсивне об'єднання доказів.

zk-STARK [6] усуває потребу у довірній установці, спираючись лише на довільні хеш-функції та коди Ріда–Соломона. Властивості:

- прозорість: всі параметри одержують із публічного випадкового джерела;
- постквантова стійкість;
- докази десятки/сотні КБ, але непотрібні токсичні залишки;
- складність перевірки – quasi-linear у розмірі трасування обчислення.

STARK-технології вже застосовуються у L2-мережах Ethereum (StarkNet).

Протоколи Блума–Фельдмана, Goldreich–Micali–Wigderson та ін. доводять NP-твердження зі статистичним нульовим знанням, використовуючи багаторазові випадкові commit-challenge-response-раунди [2]. Вони універсальні (існують для будь-якої NP-мови), проте потребують багатьох раундів і значного обсягу передачі ($\approx O(n \cdot k)$, де k – кількість повторів для зниження ймовірності шахрайства).

Lattice-based ZKP для задач NTRU або SIS/LWE надають постквантову стійкість, але поки мають великі розміри доказу (сотні кілобайт) [11].

Сліпий квантовий доказ (QZKP) пропонує передавати квантові стани замість класичних повідомлень.

Zero-Knowledge Machine Learning Proofs: доведення коректності inferencing-моделі без розкриття параметрів (дослідження 2023 – 2025 рр.) [12].

У табл. 1 наведено порівняння описаних вище підходів.

Таблиця 1

Порівняльний аналіз підходів

Підхід	Trusted Setup	Розмір доказу	Час генерації	Час перевірки	Безпека	Типові застосунки
Σ -протокол (DL) [18]	Ні	64-128Б	$O(1/\epsilon)$	$O(1/\epsilon)$	Обчисл. ZK, EUF-CMA	Ідентифікація, e-cash
zk-SNARK (Groth16) [19, 20]	Так	128-192Б	$O(n \log n)$	$O(1)$	Обчисл. ZK, DL	Приватні платежі (Zcash)
zk-SNARK (PLONK) [19, 20]	Так	624-2400Б	$O(n \log n)$	$O(n \log n)$	Обчисл. ZK, DL	L2 Rollups
zk-STARK [6, 7, 21]	Ні	50-200КБ	$O(n \log n)$	$O(n \log n)$	Постквант., ш.хеш	Масштабований CI
Bulletproofs [7]	Ні	$O(\log n)$ $\cong$ (3-6КБ)	$O(n \log n)$	$O(n)$	Обчисл. ZK, DL	Конфіденц. транзакції (Monero)
Lattice ZKP [22]	Ні	13-400 КБ	$O(n \log n)$	$O(n \log n)$	Постквант. SIS	e-ID, PKE

П р и м і т к а : n – розмір вхідних даних/схеми; CI – computational integrity.

Перспективи та відкриті проблеми:

1. Постквантова стійкість. Хеш-базовані STARK є перспективною, однак потрібно зменшити розмір доказу та час перевірки [6].

2. Рекурсивні та агреговані докази. Halo 2, Nova та SuperNova дозволяють вкладати докази у докази, що критично для масштабованості блокчейн-L2 [10].

3. Захист метаданих. Навіть за ZK-доказів бокові канали (розмір, час, мережеві патерни) можуть розкривати приватність; потрібні протоколи укриття трафіку.

4. Zero-Knowledge ML. Перевірка коректності виконання НН-моделей із приватними вагами залишається відкритою задачею за обмежень продуктивності [12].

Висновки

У статті систематизовано сучасні методи доказу з нульовим розголошенням за ознаками інтерактивності, математичної природи, потреби у довіреній установці та типу гарантій нульового знання. Алгебраїчні zk-SNARK і прозорі zk-STARK довели практичність ZKP для широкого спектра прикладних задач – від конфіденційних платежів до захищених хмарних обчислень. Порівняльний аналіз показав компроміси між ефективністю та безпекою: SNARKи забезпечують мінімальний розмір доказу, але вимагають trusted setup; STARKи ж прозорі й постквантові, однак громіздкі. Подальші дослідження зосереджено на рекурсивних схемах, постквантових конструкціях, стандартизації та інтеграції у високорівневі застосунки, зокрема машинне навчання й Інтернет речей. Розв'язання цих проблем забезпечить нові можливості для безпечних та приватних інформаційних технологій.

Список літератури:

1. Meiklejohn S., Mercer R. ZKProof Community Reference. ZKProof Community Docs. 2022. Режим доступу: <http://docs.zkproof.org/reference.pdf>
2. Lindell Y. How To Simulate It – A Tutorial on the Simulation Proof Technique // IACR Cryptology ePrint Archive. 2016. No. 046. Режим доступу: <https://eprint.iacr.org/2016/046.pdf>
3. Boneh D., Shoup V. A Graduate Course in Applied Cryptography. 2020. Ch. 19, 23. Режим доступу: <https://crypto.stanford.edu/~dabo/cryptobook/>
4. Ben-Sasson E., Chiesa A., Genkin D., Tromer E., Virza M. Succinct Non-Interactive Zero Knowledge for a von Neumann Architecture // IACR Cryptology ePrint Archive. 2013. No. 879. Режим доступу: <https://eprint.iacr.org/2013/879.pdf>
5. Groth J. On the Size of Pairing-Based Non-interactive Arguments // IACR Cryptology ePrint Archive. 2016. No. 260. Режим доступу: <https://eprint.iacr.org/2016/260.pdf>
6. Ben-Sasson E., Bentov I., Horesh Y., Riabzev M. Scalable, transparent, and post-quantum secure computational integrity // IACR Cryptology ePrint Archive. 2018. No. 046. Режим доступу: <https://eprint.iacr.org/2018/046.pdf>
7. Bünz B., Bootle J., Boneh D., et al. Bulletproofs: Short Proofs for Confidential Transactions and More // IACR Cryptology ePrint Archive. 2017. No. 1066. [Електронний ресурс]. Режим доступу: <https://eprint.iacr.org/2017/1066.pdf>
8. Ben-Sasson E., Chiesa A., Spooner N. Interactive Oracle Proofs // Theory of Cryptography Conference (TCC 2016-B). Lecture Notes in Computer Science. Vol. 9985. Springer, 2016. P. 163–190.
9. Gabizon A., Williamson Z., Ciobotaru O. PLONK: Permutations over Lagrange-Bases for Oecumenical Non-interactive Arguments of Knowledge // IACR Cryptology ePrint Archive. 2019. No. 953. Режим доступу: <https://eprint.iacr.org/2019/953.pdf>
10. Bowe S., Gabizon A., Green M., et al. Halo 2: Recursive Proof Composition without a Trusted Setup // IACR Cryptology ePrint Archive. 2019. No. 1021. Режим доступу: <https://eprint.iacr.org/2019/1021.pdf>
11. Lyubashevsky V., Seiler G. Zero-Knowledge Proofs from Lattices: New Techniques // Advances in Cryptology – CRYPTO 2022. Lecture Notes in Computer Science. Vol. 13508. Springer, 2022. P. 66–92. DOI: 10.1007/978-3-031-15979-4_3
12. Hao M., Chen H., et al. zk-ML: Scalable Zero-knowledge Proofs for Non-linear Functions in Machine Learning // IACR Cryptology ePrint Archive. 2025. No. 507. Режим доступу: <https://eprint.iacr.org/2025/507.pdf>
13. Rafaël Del Pino: Efficient lattice-based zero-knowledge proofs and applications p. 49. Режим доступу: <https://theses.hal.science/tel-02445482v1/document>
14. Muhammed F. Esgin, Ron Steinfeld, Dongxi Liu, Sushmita Ruj: Efficient Hybrid Exact/Relaxed Lattice Proofs and Applications to Rounding and VRFs. Режим доступу: <https://eprint.iacr.org/2022/141.pdf>
15. Nicolas Gailly, Mary Maller, Anca Nitulescu: SnarkPack: Practical SNARK Aggregation. [Financial Cryptography and Data Security: 26th International Conference, FC 2022, Grenada, May 2-6, 2022, Revised Selected Papers](https://www.financecryptographyanddatasecurity.com/2022/05/26/financial-cryptography-and-data-security-26th-international-conference-fc-2022-grenada-may-2-6-2022-revised-selected-papers/) P. 203–229
16. Roy Lu: Moore's Law for Zero Knowledge Proofs. Stanford Blockchain Review Volume 3, Article No. 2. Режим доступу: <https://review.stanfordblockchain.xyz/p/22-moores-law-for-zero-knowledge>
17. Shashidhara R. Promise of Zero-Knowledge Proofs (ZKPs) for Blockchain Privacy and Security: Opportunities, Challenges, and Future Directions. Security and Privacy 8(1) September 2024. Режим доступу: https://www.researchgate.net/publication/384056745_Promise_of_Zero-Knowledge_Proofs_ZKPs_for_Blockchain_Privacy_and_Security_Opportunities_Challenges_and_Future_Directions#:~:text=other%20zk,processes%20transac
18. Ivan Damgard: On Σ -protocols. CPT 2010, v.2. Режим доступу: <https://www.cs.au.dk/~ivan/Sigma.pdf>
19. Garg S. et al. zkSaaS: Zero-Knowledge SNARKs as a Service (USENIX Security 2023). Режим доступу: <https://eprint.iacr.org/2023/905.pdf>

20. Arka Rai Choudhuri, Sanjam Garg, Aarushi Goel, Sruthi Sekar, Rohit Sinha: SublonK: Sublinear Prover PLONK // Proceedings on Privacy Enhancing Technologies. 2024. No 3. P. 314–335. Режим доступу: <https://petsymposium.org/popets/2024/popets-2024-0080.pdf>
21. Kimi Wu: Revealing The All Mysterious zk-STARKs. Режим доступу: <https://medium.com/coinmonks/reveal-mysterious-zk-starks-42d00679c05b>
22. Ngoc Khanh Nguyen, George O'Rourke: More Efficient Lattice-Based Zero-Knowledge Proofs with Straight-Line Extractability. APKC '25 // Proceedings of the 12th ACM ASIA Public-Key Cryptography Workshop. Режим доступу: <https://dl.acm.org/doi/10.1145/3709015.3728673>

Надійшла до редколегії 12.10.2025

Відомості про автора:

Мордвінов Руслан Ігорович — кандидат технічних наук, Україна; email: rmordvinov@gmail.com; ORCID: <https://orcid.org/0000-0003-1229-2840>

*В.І. ЗАБОЛОТНИЙ, канд. техн. наук, Ю.М. ГОЛОБОРОДЬКО, канд. техн. наук,
Д.М. ЗАБОЛОТНИЙ, Д.О. АБРОСИМОВ*

КІЛЬКІСНА МОДЕЛЬ ЗАСОБІВ ПАСИВНОГО ПРИХОВУВАННЯ МОВНОЇ ІНФОРМАЦІЇ НЕЛІНІЙНИМИ АТЕНЮАТОРАМИ

Вступ

Захист інформації на об'єктах інформаційної діяльності (ОІД) – це комплекс організаційних, правових та технічних заходів забезпечення безпечного функціонування організацій, підприємств всіх форм власності. У цій діяльності достатньо високу увагу привертає захист допоміжних технічних засобів (ДТЗ), які можуть створювати технічні канали витоку інформації (ТКВІ). Зокрема ТКВІ можуть створюватися низькочастотними полями, які виникають під час озвучування інформації, роботи технічних засобів прийому, обробки, зберігання й передачі інформації (ТЗПІ) та ДТЗ; під час впливу на ТЗПІ та ДТЗ електричних, магнітних та акустичних полів; під час виникнення паразитної високочастотної (ВЧ) генерації; під час проходження інформативних (небезпечних) сигналів у колі електроживлення; під час взаємного впливу кіл; під час проходження інформативних (небезпечних) сигналів у колі заземлення; під час паразитної модуляції високочастотного сигналу тощо [1, 2].

У статті розглянуто застосування нелінійних фільтрів для захисту ДТЗ від розвідки інформації на прикладі використання явища акустoeлектричного перетворення у визивних схемах телефонних апаратів. Детально проаналізовано принцип роботи нелінійних фільтрів, їхні характеристики та схеми застосування, а також надано метод оцінки їх кількісних показників. Ця інформація буде корисна для фахівців, які займаються захистом ОІД, а також для всіх, хто цікавиться питаннями безпеки даних від витоку.

Теоретичні положення

Нелінійні фільтри призначені для автоматичного захисту встановлених на об'єктах інформаційної діяльності ДТЗ у випадках, коли:

- провідники (лінії зв'язку, управління) від ДТЗ виходять за межі контрольованої території;
- напруги робочих сигналів ДТЗ перевищують величину в одиниці В, а небезпечні сигнали ІЗОД менші величин десятих В;
- робочі сигнали (управляючі сигнали) для ДТЗ короточасні і надходять із-за меж контрольованої зони (КЗ) ОІД.

Прикладами застосування нелінійних фільтрів можуть бути:

- захист дзвонкової ланки телефонного апарату;
- захист визивного дзвоника у приміщенні;
- захист вторинних годинників, які встановлюють у виділених приміщеннях;
- захист від наведень на комунікації сигналізацій лініями зв'язку у виділених приміщеннях тощо.

Основою нелінійного фільтру є пара зустрічно-паралельно ввімкнутих площинних напівпровідникових діодів. Призначення такого пристрою – задане суттєве зменшення рівня слабого небезпечного сигналу ІЗОД і практично безослаблене пропускання службового сигналу ДТЗ, який ІЗОД не несе. Інколи такі фільтри мають назву – амплітудні, в сенсі пригнічення слабких сигналів за ознакою їх амплітуди.

Слід відзначити, що до теперішнього часу аналітичні моделі співвідношень, які описують функціонування нелінійних фільтрів для захисту інформації, відсутні, в основному використовуються емпіричні дані обґрунтування роботи таких схем.

Характеристика площинного діода

Вольтамперна характеристика (ВАХ) $I(U)$ площинного діода може бути задовільно апроксимована виразом [3]:

$$I = I_0 \left(\exp \frac{U}{\varphi_T} - 1 \right), \quad (1)$$

де I – струм, який проходить через p - n перехід діода; I_0 – тепловий струм (зворотній струм насичення) діода; U – напруга на p - n переході діода; φ_T – температурний потенціал p - n переходу діода.

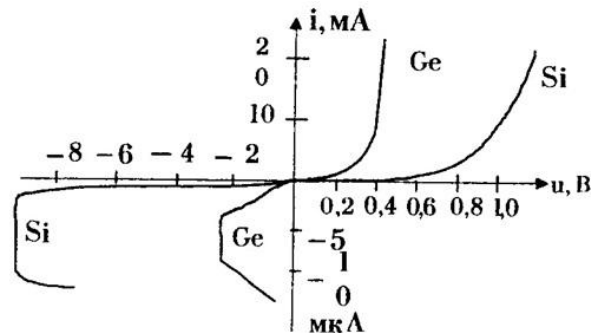


Рис. 1. Вольтамперні характеристики $I(U)$ площинних діодів, виконаних з різних матеріалів.
Масштаби гілок ВАХ різні для наочності представлення

Тепловий струм I_0 (або другий термін – зворотній струм насичення діода) суттєво залежить від матеріалу напівпровідника. Типові значення I_0 для площинних германієвих діодів середньої потужності складає величину близько 1 – 3 мкА, а для кремнієвих 1 – 10 нА, тобто відрізняються на кілька порядків.

Тепловий потенціал φ_T p - n -переходів для “кімнатних” температур складає величину близько 25 мВ як для германієвих, так і для кремнієвих діодів.

Відношення U/I характеризує опір діода R . Визначити залежність R від прикладеної напруги можна з виразу (1):

$$R = \frac{U}{I} = \frac{U}{I_0 \left(\exp \frac{U}{\varphi_T} - 1 \right)}. \quad (2)$$

При $U \rightarrow 0$ величина опору $R(U \rightarrow 0)$ має величину φ_T/I_0 . Видно, що опір кремнієвих діодів значно вище, ніж германієвих при малих напругах на p - n переході.

Характеристика ланцюжка зустрічно-паралельно увімкнених діодів

Пара зустрічно-паралельно увімкнених діодів складає типовий ланцюжок захисту нелінійного фільтру. Опір R_a такого ланцюжка можна визначити за відомою формулою паралельного з’єднання опорів [4]. Формулу (2) треба використовувати, враховуючи знак прикладеної напруги до кожного з p - n переходів діодів:

$$R_a = \frac{R^{\Pi} \cdot R^H}{R^{\Pi} + R^H},$$

де R^{Π}, R^H – вираз (2) з позитивним (Π) і негативним (H) знаком перед величиною U у формулі (2).

Тоді, після підстановок та перетворень можна одержати вираз (3) для опору R_a :

$$R_a = \frac{\frac{U}{I_0 \left(\exp \frac{U}{\varphi_T} - 1 \right)} \cdot \frac{-U}{I_0 \left(\exp \frac{-U}{\varphi_T} - 1 \right)}}{\frac{U}{I_0 \left(\exp \frac{U}{\varphi_T} - 1 \right)} + \frac{-U}{I_0 \left(\exp \frac{-U}{\varphi_T} - 1 \right)}} = \frac{U}{I_0} \cdot \frac{1}{\exp \frac{U}{\varphi_T} - \exp \frac{-U}{\varphi_T}}. \quad (3)$$

Легко показати, що при $U \rightarrow 0$ $R_a \rightarrow \varphi_T / 2I_0$.

Функція $R_a(U)$ парна. З ростом $|U|$ опір R_a зменшується. Граничне значення опору R_a при $|U| \rightarrow \infty$ зменшується до нуля.

Таким чином, ланцюжок зустрічно-паралельно увімкнутих діодів має великий опір для малих за амплітудою сигналів і низький – для великих. Кремнієві діоди мають суттєво більше значення опору (приблизно на три порядки) при малих сигналах чим германієві (рис. 2, 3)

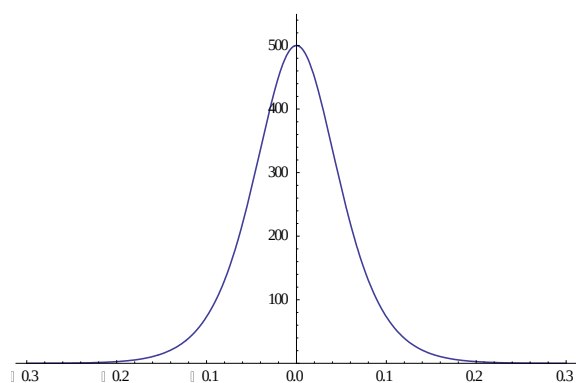


Рис. 2. Графік опору $R_a(U[B])$ германієвих діодів, Ом

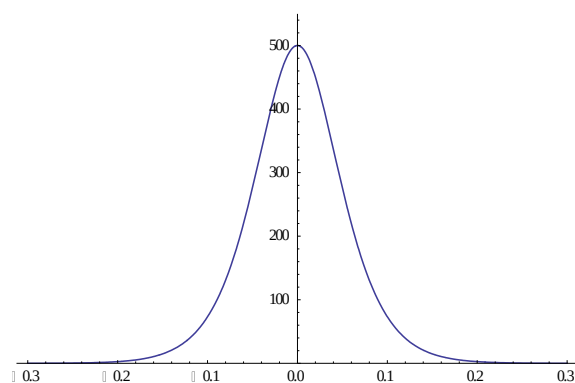


Рис. 3. Графік опору $R_a([B])$ кремнієвих діодів, кОм

Типова схема застосування ланцюжка зустрічно-паралельно увімкнутих діодів

Ланцюжок зустрічно-паралельно увімкнутих діодів ставлять у розрив (рис. 4) одного або, що краще, двох провідників, які виходять за межі контрольованої зони (території) ОІД.

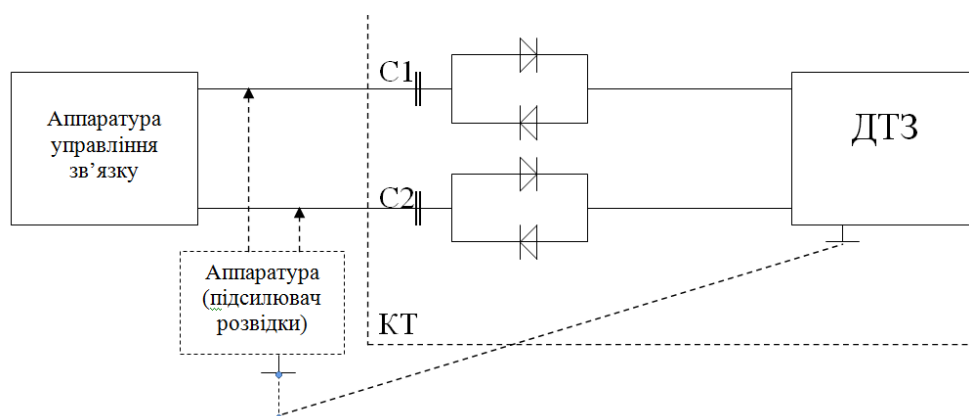


Рис. 4. Типова схема застосування ланцюжка зустрічно-паралельно увімкнутих діодів для захисту від витоків сигналів ІЗОД невеликих амплітуд, по відношенню до значно більших сигналів керування

Для боротьби із навмисним зниженням опору діодів, шляхом подачі постійного струму у лінію зв'язку, необхідно у схему вмикати конденсатори $C1, C2$.

Оцінка кількісних показників нелінійного фільтра

Оцінювати ефективність роботи нелінійних фільтрів можна за допомогою чинних НД ТЗІ, випущених ДССЗІ України [5–7]. Еквівалентна схема захищеного ДТЗ з підключеною до лінії зв'язку (керування) апаратурою розвідки наведена на рис. 5. Для спрощення аналізу розглядається лише один ланцюжок захисту у одному із провідників. Два ланцюжка, які вмикаються послідовно у кожний із провідників, подвоюють рівень захисту сигналу ІзОД. Подальше спрощення аналізу дає виключення із схеми конденсаторів C_1 , C_2 . Їх наявність при досить великій ємності практично не впливає на результати дії, але приводить до громіздких аналітичних виразів у комплексній формі.

Опір R_3 призначений для запобігання веденню розвідки підсилювачем з дуже високим вхідним опором при від'єднанні телефонної лінії зразу за межею КЗ (точки xx на схемі рис. 5).

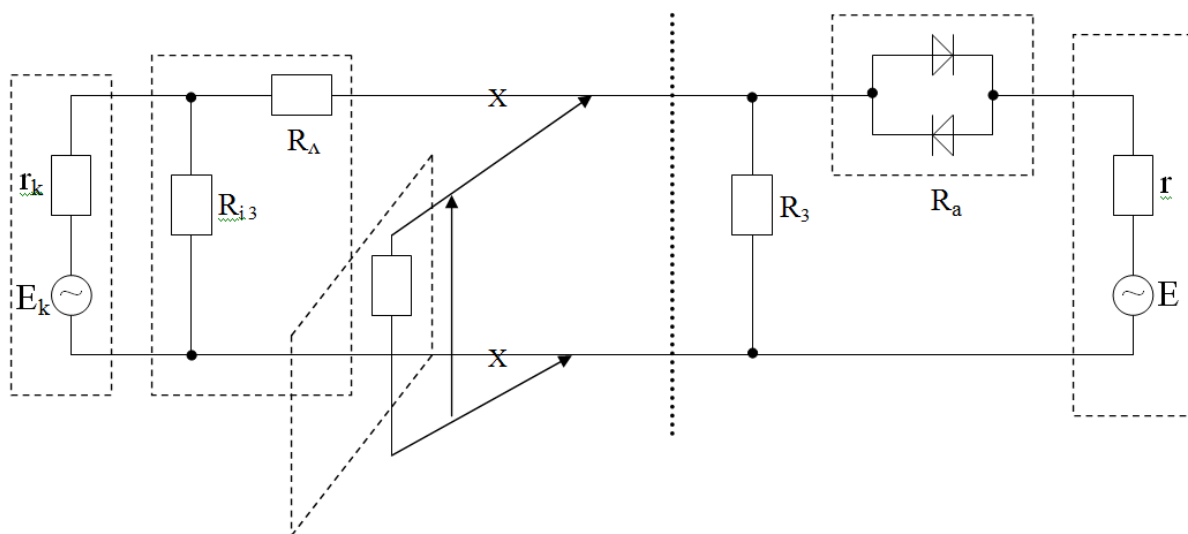


Рис. 5. Еквівалентна схема захищеного ДТЗ з підключеною до лінії зв'язку апаратурою розвідки.

Тут позначені R_L – опір лінії до АТС; R_{i3} – опір ізоляції лінії зв'язку до АТС, яку оператор розвідки може від'єднувати під час ведення розвідки

Подалі спростити еквівалентну схему рис. 5 можливо за рахунок перетворення еквівалентних схем джерела сигналу і лінії зв'язку (керування) у єдиний двополюсник за відомими правилами (рис. 6) [4]

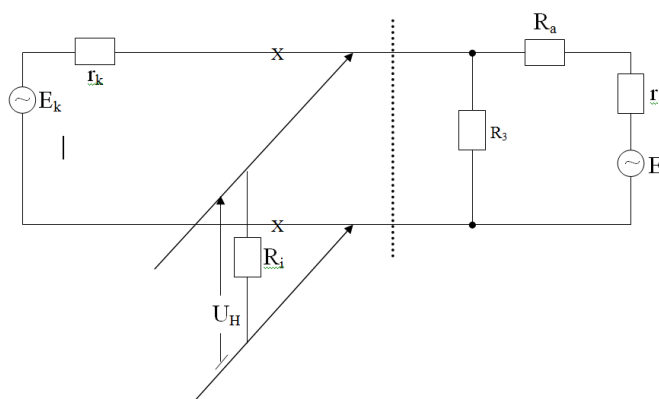


Рис. 6. Спрощена еквівалентна схема захищеного ДТЗ з підключеною до лінії зв'язку апаратурою розвідки

Еквівалентна схема рис. 6 дає змогу скласти рівняння для небезпечного сигналу

$$U_H = \frac{r_k \parallel R_i \parallel R_3}{r + R_a + r_k \parallel R_i \parallel R_3} E, \quad (4),$$

де $\parallel$ – знак паралельного підключення опорів; r_k – еквівалентний внутрішній опір мережі керування; R_i – вхідний опір апаратури розвідки; R_3 – захисний опір; R_a – нелінійний опір ланцюжка захисту; r – внутрішній опір ДТЗ; E – е.р.с. джерела небезпечного сигналу ДТЗ; E – е.р.с. еквівалентного джерела сигналу керування.

Останній вираз можна записати як коефіцієнт захисту:

$$k_3 = \frac{r_k \parallel R_i \parallel R_3}{r_k \parallel R_i \parallel R_3 + r + R_a},$$

що залежить від величини R_a , яка у свою чергу залежить від величини прикладеної до діодів напруги.

Оператор розвідки може за межами КЗ відключати лінію керування ($r_k \rightarrow \infty$), мати у своєму розпорядженні розвідапаратуру з великим вхідним опором ($R_i \rightarrow \infty$). В цьому випадку $r_k \parallel R_i \parallel R_3 = R_3$.

Тоді поточне значення коефіцієнту захисту k_3 , яке використовується для побудови графіків при певних обмеженнях (параметрах) з аргументом рівня сигналу необхідно використовувати вираз

$$k_3(r_k = \infty; r_i = \infty) = \frac{R_3}{R_3 + r + R_a} = \frac{1}{1 + \frac{r}{R_3} + \frac{R_a}{R_3}} \quad (5)$$

Відсутність опору R_3 ($R_3 \rightarrow \infty$) приводить до $k_3 \approx 1$, оскільки $R_a < \infty$. Таким чином, наявність R_3 у схемі захисту обов'язкова.

Величину R_3 потрібно вибирати як можна меншою, але її дуже мала величина не повинна погіршувати роботу схеми керування ДТЗ.

Підходом до вибору величини опору R_3 може бути, наприклад, величина потужності, яка на ній втрачається. Хай це буде 0,1 потужності, яка керує ДТЗ.

Тоді можна записати $P_{R3} = P_r / 10$, де P_{R3} і P_r – згадані відповідні потужності. Вище відмічено, що при великих амплітудах сигналу керування $R_a \rightarrow 0$.

Означене дає рівняння $U^2 / R_3 = U^2 / 10r$, звідки легко одержати, що $R_3 \geq 10r$.

Наведене дає можливість представити дві різні еквівалентні схеми. По-перше, еквівалентна схема дії ланцюжка захисту (рис. 7).

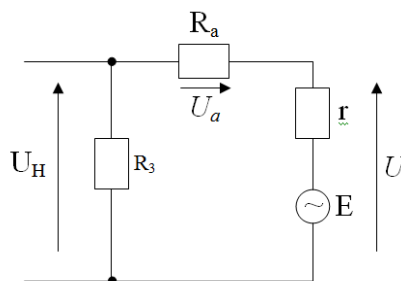


Рис. 7. Еквівалентна схема дії ланцюжка захисту

По-друге, еквівалентна схема дії ДТЗ у робочому режимі при подачі робочого сигналу зі сторони входу до КЗ (рис. 8).

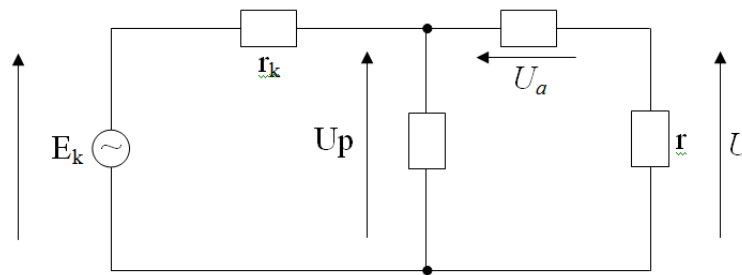


Рис. 8. Еквівалентна схема дії ДТЗ у робочому режимі подачі сигналу визову E_k

Наведені еквівалентні схеми дають можливість оцінити величини R_a у обох випадках в залежності від значень E , E_k , r_k , r і вибраного R_3 .

Аналітична оцінка кількісних показників нелінійного фільтра при проєктуванні елементів захисту інформації, що планується до захисту

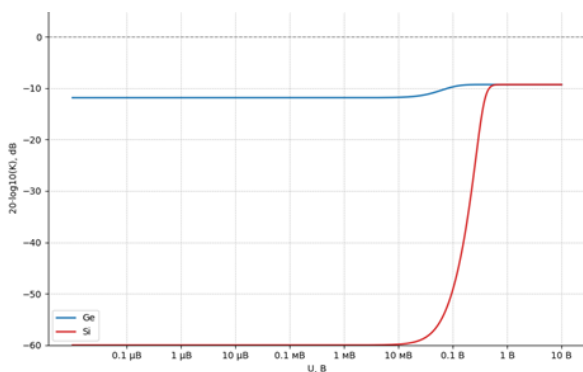
Сучасний розвиток чисельних методів оцінки показників захисту дозволяє розробнику або оцінювачу ефективності запропонованих заходів захисту проводити розрахунок величини коефіцієнта передачі в різних умовах ведення розвідки, зазначених вище.

Особливість створення та дослідження моделі роботи нелінійного фільтра полягає в застосуванні ітераційних методів розв'язування алгебраїчних і трансцендентних рівнянь при обчисленні параметрів коефіцієнта захисту для побудови. Програма побудови графіків виконана мовою програмування Python.

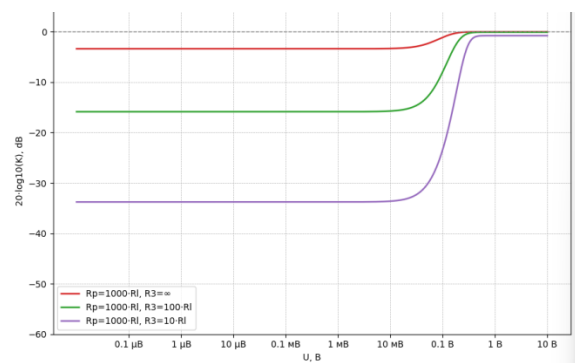
Графіки, що ілюструють та підтверджують одержані результати, наведено на рис. 9.

Підтверджено обґрунтованість використання в нелінійному фільтрі тільки кремнієвих діодів, які забезпечують коефіцієнт захисту не менше 60 дБ у діапазоні амплітуд небезпечно-го сигналу практично до 7 мкВ. В той же час нелінійний фільтр при під'єднанні до АТС може ослаблювати робочий сигнал виклику на 9 дБ, що є прийнятною величиною (рис. 9, а). Падіння рівня сигналу на 9 дБ обумовлюється впливом опору лінії зв'язку від АТС до ОІД.

Графіки (рис. 9, б) ілюструють різке зменшення захисних властивостей нелінійного фільтра при від'єднанні оператором розвідки телефонної лінії від АТС за рахунок перерозподілу падіння напруги небезпечно-го сигналу на підсилювачі розвідки та фільтри захисту. Причому збільшення вхідного опору підсилювачі розвідки збільшує рівень небезпечно-го сигналу (лінії зверху вниз). Одночасно зменшення величини захисного опору (від ∞ через $100R_L$ до $10R_L$) покращує ступінь захисту небезпечно-го сигналу (лінії зверху вниз).



а – на германієвих та кремнієвих діодах



б – на кремнієвих діодах в різних режимах ведення розвідки

Рис. 9. Графіки коефіцієнтів передачі нелінійних фільтрів, що ілюструють результати аналітичної оцінки кількісних показників виконаних досліджень

Висновки

У результаті аналізу показано, що нелінійні фільтри є ефективним засобом для захисту ДТЗ від витоку інформації. Їхні характеристики, такі як високий опір для малих сигналів і низький опір для великих, дозволяють пригнічувати небезпечні сигнали, не впливаючи на роботу ДТЗ.

Запропонований аналітичний метод оцінки коефіцієнту захисту дозволяє проєктувати характеристики нелінійних фільтрів з заданими характеристиками.

Показано, що протидія оператору апаратури розвідки по підвищенню можливості перехоплення сигналів ІзОД шляхом від'єднання лінії управління може бути компенсована шляхом увімкнення захисного опору в межах контрольованої зони. Величина цього опору може бути визначена, виходячи із електричних параметрів елементів кіл фільтра, характеристик джерела небезпечних сигналів, вхідного опору підсилювача розвідки та опорів лінії зв'язку.

Зазначене не відмінює необхідність оцінювати відповідність досягнутого рівня захисту інформації встановленому вимогами нормативних документів, згаданим у статті методикам випробувань шляхом атестації комплексів ТЗІ на ОІД.

Подальші дослідження можуть бути спрямовані на оптимізацію характеристик нелінійних фільтрів, застосування для них нової елементної бази та схемно-технічних рішень, нових сфер застосування нелінійних фільтрів і їх адаптації до сучасних об'єктів інформаційної діяльності.

Список літератури:

1. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації : навч. посіб. / С.О. Іванченко, О.В. Гавриленко, О.А. Липський, А.С. Шевцов. Київ : ІСЗІ НТУУ «КПІ», 2016. 104 с.
2. Тимчасові рекомендації з технічного захисту інформації від витоку каналами побічних електромагнітних випромінювань та наводок ТР ТЗІ - ПЕМВН-95.
3. Основи електроніки : навч. посіб. / А. С. Васюра, Г. Д. Дорощенко, В. П. Кожем'яко, Г. Л. Лисенко. Вінниця : ВНТУ, 2018. 197 с.
4. Загальна електротехніка і основи електроніки : навч. посіб. / В.М. Співак, А.М. Гуржий, А.Т. Нельга, О.С. Ітякін. Київ : КПІ, 2020. 266 с.
5. НД ТЗІ 2.3-002-2001 Технічний захист мовної інформації в симетричних абонентських аналогових телефонних лініях. Засоби пасивного приховування мовної інформації. Нелінійні атенюатори та загороджувальні фільтри. Методика випробувань, наказ ДСТСЗІ СБУ від 06.04.2001 № 11.
6. НД ТЗІ 2.3-003-2001 Технічний захист мовної інформації в симетричних абонентських аналогових телефонних лініях. Засоби пасивного приховування мовної інформації. Генератори спеціальних сигналів. Методика випробувань, наказ ДСТСЗІ СБУ від 06.04.2001 № 11.
7. НД ТЗІ 4.7-001-2001 Технічний захист мовної інформації в симетричних абонентських аналогових телефонних лініях. Засоби визначення наявності та віддаленості місця контактного підключення засобів технічної розвідки. Рекомендації щодо розроблення методів випробувань, наказ ДСТСЗІ СБУ від 06.04.2001 № 11с.
8. Цегелик Г. Г. Чисельні методи : підручник. Львів : Львів. нац. ун-т ім. І. Франка, 2004. 408 с.

Надійшла до редколегії 12.10.2025

Відомості про авторів:

Заболотний Володимир Ілліч – кандидат технічних наук, професор кафедри безпеки інформаційних технологій; Харківський національний університет радіоелектроніки; Україна; email: volodymyr.zabolotnyi@nure.ua ORCID: <https://orcid.org/0000-0003-3258-8489>

Голобородько Юрій Миколайович – кандидат технічних наук, доцент кафедри безпеки інформаційних технологій; Харківський національний університет радіоелектроніки; Україна; email: yurii.holoborodko@nure.ua, ORCID: <https://orcid.org/0009-0007-4040-9467>

Заболотний Дмитро Миколайович – АТ «ІТ», начальник відділу комплексів ТЗІ; Україна; email: dmytro.zabolotnyi@nure.ua, ORCID: <https://orcid.org/0009-0008-5891-4426>

Абросімов Даніїл Олегович – бакалавр кафедри безпеки інформаційних технологій; Харківський національний університет радіоелектроніки; Україна; email: daniil.abrosimov@nure.ua, ORCID: <https://orcid.org/0009-0004-3002-2507>

*П.В. ШУЛІК, канд. техн. наук, Д.С. БАЛАГУРА, канд. техн. наук,
В.В. ПРОСОЛОВ, Д.О. В'ЮХІН*

СТВОРЕННЯ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ НА БАЗІ OPEN PORTABLE TRUSTED EXECUTION ENVIRONMENT (OP-TEE), KVM/QEMU ТА INTEL TRUST DOMAIN EXTENSIONS

Вступ

За останні 10–15 років технології захисту інформації в мобільних пристроях та мікроконтролерах дуже просунулись завдяки розвитку бездротового Інтернету та систем Інтернету речей (IoT). Тобто, невеликі малопотужні пристрої стали частиною великої мережі – Інтернет. Але їх низькі обчислювальні потужності привели до неспроможності ефективного захисту несанкціонованого доступу до інформації. Таким чином це призвело до значного поштовху в розробці апаратно-програмних технологій захисту інформації для таких пристроїв.

Переважна більшість таких пристроїв базується на процесорах Advanced RISC Machines (ARM) одноіменної компанії. Тому ARM прийшлося зайнятися розробкою підсистем захисту інформації для своїх архітектур та розробити технологію ARM TrustZone [1, 2]. Технологія була представлена ще у 2002 р., але до більш-менш поширеного використання дійшло тільки після 2009 р. Основна ідея ARM TrustZone заключається в розподілі обчислень на звичайні та сек'юрні та ізоляції доступу зі звичайного середовища (операційної системи та звичайних додатків) до сек'юрних даних та обчислень. Це робиться завдяки апаратно-програмним механізмам. На рівні апаратних механізмів периферія поділяється на елементи для роботи з захищеною та звичайною інформацією – наприклад, розподіл оперативної пам'яті та флеш пам'яті. В ARM TrustZone також вводиться захищений режим роботи ARM ядра. У ньому виконується робота з секретною інформацією, яка не повинна бути доступною для основної операційної системи та її додатків.

З боку програмних механізмів існує багато різних підходів ізоляції доступу на рівні окремих додатків та на рівні ізольованих операційних систем. В сучасних операційних системах для захисту інформації існує підхід з використанням двох операційних систем, де система поділяється на два світи: звичайний (non secure world) – де працює звичайне програмне забезпечення, та захищений світ (secure world), в якому ведеться робота з конфіденційною інформацією. Звичайний світ не має доступу до захищеного світу, тоді як останній може з'єднуватись при бажанні з різними пристроями. Цей підхід стосується не тільки процесора, але і пам'яті, транзакції на шинах, переривань, периферійних пристроїв в рамках системи, в тому числі, програмного забезпечення.

Як приклад програмної підтримки такого підходу можна навести open source фреймворк OP-TEE (Open Portable Trusted Execution Environment) [3]. Це відкритий фреймворк TEE для платформ ARM, що реалізує захищене середовище виконання на базі TrustZone та сумісний зі специфікаціями GlobalPlatform. Типова архітектура програмного забезпечення OP-TEE показана на рис. 1.

У звичайному світі працює основна операційна система, наприклад Linux або Android та звичайні додатки. Коли потрібно запустити якусь задачу, яка працює з конфіденційними даними, наприклад, аутентифікація, шифрування даних, банківські операції та інше, то йде запит від звичайного до сек'юрного світу. Для цього використовується API, який надається сек'юрним світом. Звернення до API виконується через Kernel module (або драйвер) та Monitor. Monitor розташований в сек'юрному світі та виступає арбітром, який обробляє запити від звичайного світу та повертає відповіді. В сек'юрному світі на рівні User space працюють додатки, які запускаються у відповідь на API запити.

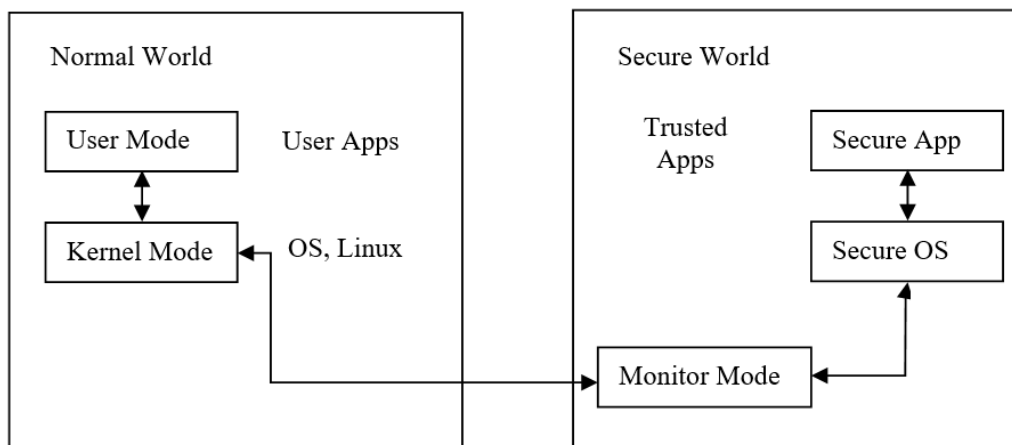


Рис. 1. Типова архітектура поділу світів OP-TEE

Спочатку OP-TEE була створена безпосередньо для підтримки ARM TrustZone для процесорів ARM Cortex A, де використовуються Unix-подібні операційні системи. Але OP-TEE поширюється дуже активно останні декілька років для роботи вбудованих та мобільних пристроїв і набрала популярності. Такий стан справ викликає інтерес до використання OP-TEE з боку виробників серверних рішень, де системи в основному базуються на процесорах Intel-x86. Підтримка такого підходу з боку Intel-x86 платформ є проблематичною, тому що Intel не має подібних ARM TrustZone рішень. Але Intel-x86 має розвинену апаратну підтримку віртуалізації, де для організації secure world може використовуватися окрема віртуальна машина.

Апаратна віртуалізація Intel-x86 (або VT-d/VT-x) [4, 5] – це технологія, що дозволяє запуск віртуальних машин в ізольованому режимі, де пам'ять, дисковий простір, периферія можуть бути розподілені та ізольовані між віртуальними машинами, тобто одна віртуальна машина не буде мати доступу до ресурсів іншої віртуальної машини.

Intel постійно удосконалює апаратні механізми для підтримки сек'юрних рішень та реалізації концепції поділу світів. Однією із останніх розробок від Intel є технологія Trust Domain Extensions (Intel TDX), яка додає нові апаратні елементи для ізоляції доступу до ресурсів віртуальних машин.

Метою даного дослідження є створення системи захисту інформації на основі інтеграції OP-TEE фреймворка з Intel-X86 платформами з використанням технології Intel TDX та VT-d/VT-x.

Предметом дослідження є програмні засоби інтеграції OP-TEE фреймворка з Intel-x86 VT-d/VT-x з використанням Intel TDX.

Суть інтеграції OP-TEE складається в заміщенні технології TrustZone віртуальними машинами та технологіями процесорів Intel-x86 VT-d/VT-x, де апаратні ресурси розподіляються між віртуальними операційними системами, і забезпечують ізоляцію ресурсів та інформації між операційними системами [6, 7]. В свою чергу Intel TDX додала нові елементи для підтримки ізоляції між віртуальними машинами. Перший елемент називається Total Memory Encryption (Intel TME), він забезпечує можливість шифрування пам'яті кожної віртуальної машини. Другий елемент – це новий режим праці процесора, який називається Secure-Arbitration Mode (SEAM) і в концепції повторює режим роботи non-secure/secure процесора ARM.

Технологія Intel TDX

Intel Trust Domain Extensions [8] була запропонована у травні 2021 р. для реалізації довіреного середовища, в якому віртуальні машини (так звані «довірчі домени» або TD) апаратно ізольовані від монітора віртуальної машини хоста (VMM), гіпервізора та іншого програмного забезпечення на хості. Ця апаратна ізоляція призначена для запобігання загроз суб'єктів

з адміністративним доступом або фізичним доступом до віртуальної машини хоста від шкоди аспектам конфіденційності та цілісності віртуальної машини.

Intel TDX включає апаратне середовище довіреного виконання (TEE), яке полегшує розгортання довірчих доменів (TD), які є апаратно ізольованими віртуальними машинами (VM), призначеними для захисту конфіденційних даних і додатків від несанкціонованого доступу. На рис. 2 показана архітектура Intel TDX, де показано, що все сек'юрне програмне забезпечення розташовано в TD. З хардверного боку основні компоненти підтримки адаптовані для підтримки TD. Так, наприклад, преривання в Advanced Programmable Interrupt Controller (APIC) розподіленні на trusted/untrusted та доданий контроль доступу в State Save Area для блокування доступу до станів, які належать до TD та аналогічного контролю page tables та VM control structures.

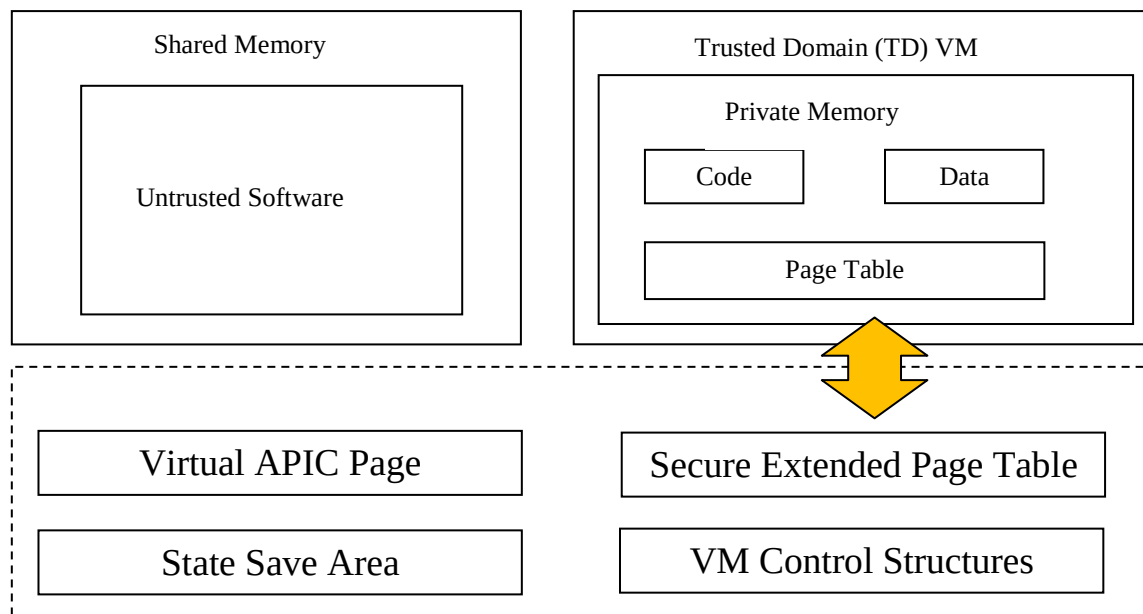


Рис. 2. Архітектура Intel TDX

Intel TDX включає також програмний модуль, який працює в новому режимі CPU, називається Secure Arbitration Mode (SEAM) та за концепцією дуже нагадує режим роботи secure-mode ARM TrustZone. Програмний модуль запускається на кожен менеджер віртуальних машин або virtual machine manager (VMM) і підтримує TD entry на кожен віртуальну машину. Модуль розміщується в зарезервованому просторі пам'яті, визначеному регістром діапазону SEAM (SEAMRR).

На рис. 3 показано обмін запитами між VMM та TD модулем.

Додана нова SEAMCALL інструкція в VMM для переводу CPU в режим операції SEAM-VMX-root та запуску TDX модуля. TDX модуль забезпечення інтерфейс для VMM для створення, видалення та виконання TD. Модуль Intel TDX виступає в якості надійного посередника, який допомагає впроваджувати політику безпеки, дії та необхідний доступ до даних для TD. Як частина створення TD, VMM надає сторінки пам'яті для TD-коду, даних та структур метаданих, пов'язаних з TD, таких як структура керування віртуальною машиною

Модуль Intel TDX призначений для виконання входу VM в SEAM-VMX, некореневої операції з використанням інструкцій VMRESUME і VMLAUNCH-VMX для виконання TD.

Intel TDX використовує шифрування пам'яті за допомогою Intel Total Memory Encryption (TME) [10], який шифрує всю пам'ять платформи одним ключем і надає можливість задати використання конкретного ключа для кожного TD.

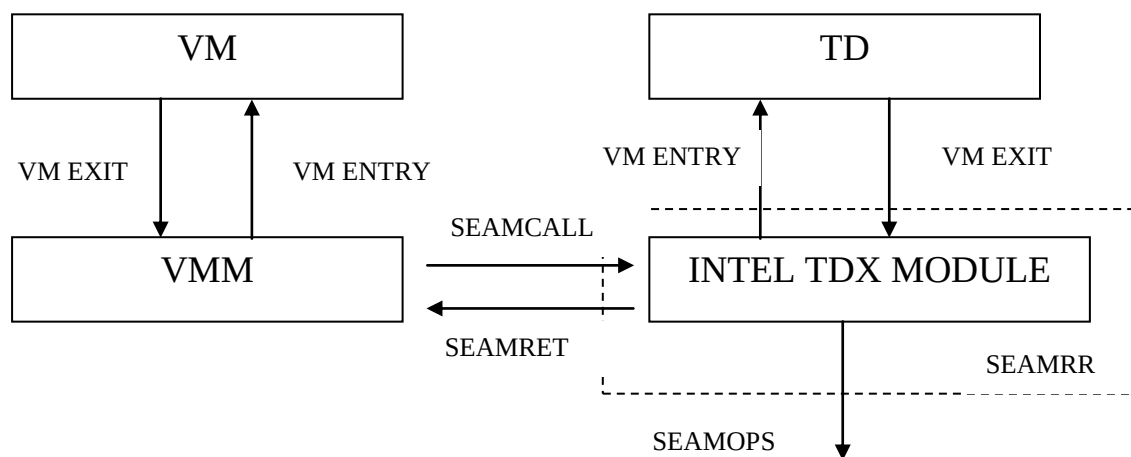


Рис. 3. Потоки в SEAM модулі

Режим Multi-Key TME (МК-TME) розширює TME для підтримки декількох ключів шифрування.

Операційна система (ОС) може використовувати можливості МК-TME в рідному або віртуалізованому середовищі. Якщо МК-TME сконфігуровано належним чином, то МК-TME доступна для кожної гостьової ОС у віртуалізованому середовищі, тому МК-TME може використовуватися як рідною, так і гостьовою ОС, як показано на рис. 4.

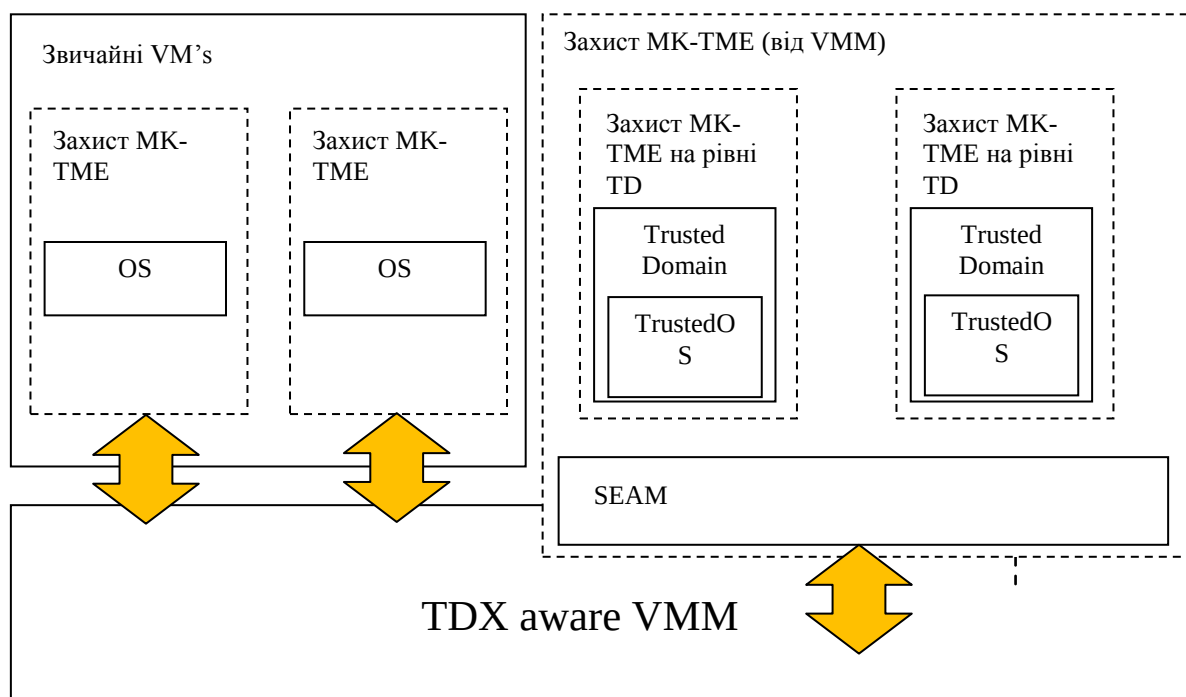


Рис. 4. Архітектура МК-TME

Таким чином, технологія Intel Trust Domain Extensions (Intel TDX) включає описані вище апаратно-програмні розширення до стандартної VT-d/VT-x та МК-TME, які разом утворюють новий вид середовища для віртуальної машини (virtual machine guest), яке називається Trust Domain (TD). TD виконується в CPU у режимі, який захищає конфіденційність змісту пам'яті та стану додатків TD в CPU від іншого програмного забезпечення (інших VM's) та від VMM.

Основні відмінності між стандартною технологією Virtual Machine Extension (VMX) та Intel TDX відмічені в табл. 1.

Порівняння технологій Virtual Machine Extension (VMX) та Intel TDX

Технологія	Доступ до віртуальної машини	Переключення між станами CPU. Операції State Save & Restore	Управління
VMX (VT-d/VT)	VMM має повний доступ	VMM SW виконує VMX переключення (наприклад реєстри загального призначення)	VMM має багатий набір елементів керування для взаємодії з VM для того, щоб скасувати привілеї VM
TDX	VMM не має повного доступу, TD може надати доступ, якщо забажає	керуються модулем Intel TDX в режимі безпечного арбітражу (SEAM)	VMM має обмежений набір контролю для управління ресурсами

Архітектура на базі Intel TDX з запуском OP-TEE в окремій TD

Запропоноване в роботі рішення (див. рис. 5) базується на ізоляції OP-TEE в окремій TD. Рішення базується тільки на використанні в якості хостової операційної OS Linux або Android. Тому у якості системи віртуалізації використовується Kernel-based Virtual Machine (KVM).

Для стандартної реалізації OP-TEE з відкритим кодом існує реалізація QEMU для платформ ARM TrustZone, яка легко інтегрується і запускається в середовищі KVM. Таким чином ми можемо запустити OP-TEE/QEMU/KVM як TD.

Для комунікації між клієнтськими додатками (Client Application's) операційної системи хоста в OP-TEE був доданий VIRTIO драйвер. На стороні хоста, оскільки optee-драйвер працює в ядрі Linux, надсилання та отримання повідомлень перекривається модулем vhost-vsock, як показано на рис. 5.

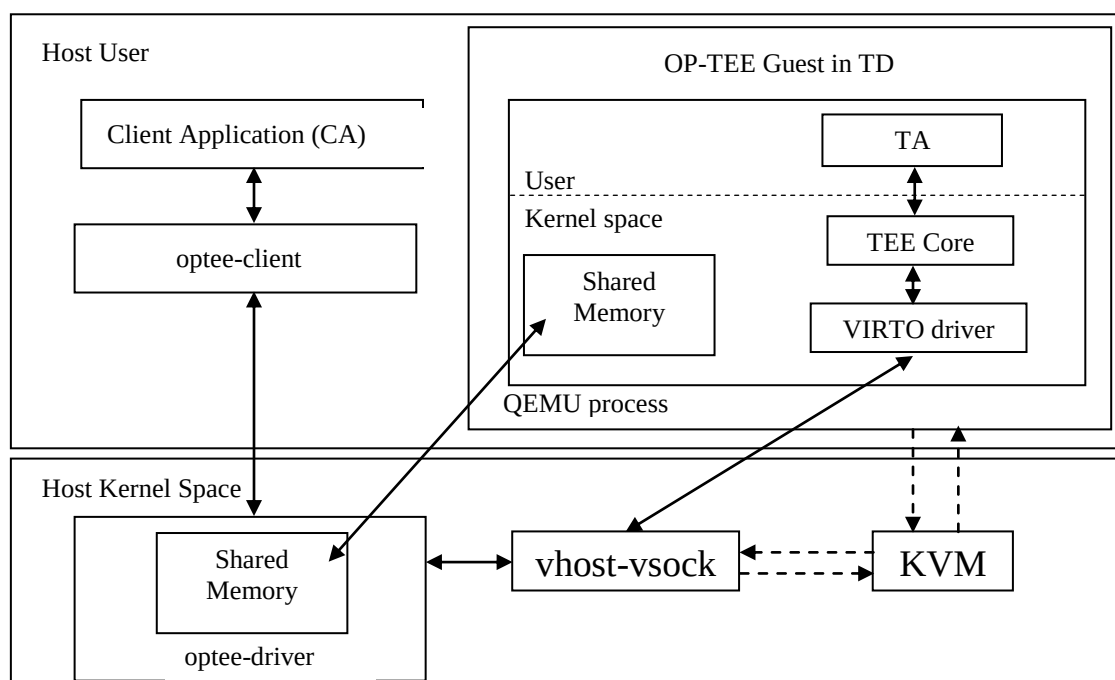


Рис. 5. Архітектура OP-TEE в контексті технології Intel TDX

Для передачі великих обсягів інформації між Normal та Secure World використовується shared memory. У KVM немає спеціальної конфігурації Extended Page Tables (EPT) для забезпечення спільного використання пам'яті між хостом та OP-TEE. Для вирішення цієї проблеми виділяються два блоки пам'яті з однаковим розміром в optee-driver і OP-TEE відповідно. Копія пам'яті на основі повідомлень VIRTIO синхронізується між цими двома блоками «спільної» пам'яті.

Інтеграція OP-TEE для Intel x86 з використанням Intel TDX була виконана з використанням таких компонентів: Intel Xeon Bronze 3508U Processor; Normal World OS: Ubuntu LTS 24.04.1; OP-TEE 4.3.0.

Висновки

Запропонований варіант інтеграції фреймворку OP-TEE на Intel x86 з використанням Intel Trust Domain Extensions. Така архітектура дозволяє будувати системи високого рівня захисту (банківські/фінансові та інші), які повністю захищені від несанкціонованого доступу до даних. OP-TEE фреймворк забезпечує захист на програмному рівні, ізолюючи працю з конфіденційними даними в окрему операційну систему (Secure World OS) з обмеженим доступом. Trust Domain Extensions забезпечує захист даних на апаратному рівні завдяки розміщенню Secure World OS в повністю зашифрованій пам'яті.

OP-TEE фреймворк первинно розроблений для ARM платформ, але запропоноване рішення дозволяє використовувати OP-TEE для захисту конфіденційних даних на Intel x86 платформах без будь-яких змін у коді.

Запропонований варіант дає більше модульності та забезпечує більш легке портування на інші платформи та легке оновлення компонентів. Наприклад, Secure World VM може оновлюватися окремо від Normal World VM.

Список літератури:

1. ARM Security Technology, Building a Secure System using TrustZone, ARM, Technology Copyright © 2005-2009 ARM Limited. All rights reserved. PRD29-GENC-009492C.
2. TrustZone Explained: Architectural Features and Use Cases.
3. GlobalPlatform // TEE System Architecture Version 1.2 (Nov 2018), GPD SPE 009.
4. Intel® Processor and Intel® Core™ i3 N-Series, Datasheet. Vol. 1 of 2. <https://edc.intel.com/content/www/us/en/design/products/platforms/processor-and-core-i3-n-series-datasheet-volume-1-of-2/001/intel-virtualization-technology-intel-vt-for-intel-64-and-intel-architecture-int/>
5. Intel Virtualization Technology for Directed I/O Architecture Specification, March 2023, Revision 4.1
6. Arshad Nehal, Priyanka Ahlawat Securing IoT applications with OP-TEE from hardware level OS // 2019 3rd International conference on Electronics, Communication and Aerospace Technology (ICECA) 10.1109/ICECA.2019.8822040.
7. Kickstart Embedded. OP-TEE: What a Beginner Needs to Know. Sep. 13, 2022. [Online]. Available: <https://kickstartembedded.com/2022/09/13/op-tee-part-1-what-a-beginner-needs-to-know/>.
8. Intel Trust Domain Extensions, White Paper, 0720/RR/MESH/PDF 343961-003US, <https://cdrdv2.intel.com/v1/dl/getContent/690419>
9. Intel, "Intel Supervisor Mode Execution Protection (SMEP) Datasheet," [Online]. Available: <https://edc.intel.com/content/www/us/en/design/products/platforms/processor-and-core-i3-n-series-datasheet-volume-1-of-2/001/intel-supervisor-mode-execution-protection-smep/>.
10. Intel TDX Virtual Firmware Design Guide, Document Number: 344991-004US, Intel Corp, December 2023
11. Шулік П. В., Федюшин О.І. Організація довіреного середовища виконання з використанням QEMU та TRUST DOMAIN EXTENSIONS від INTEL // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління : тези доп. 15-ї міжнар. наук.-техн. конф., 24-25 квітня 2025р., м. Баку, м. Харків, м. Жиліна : [у 3 т.]. Т. 3. Харків : Impress, 2025. С. 97. Doi: <https://doi.org/10.32620/ICT.25.t3>.
12. Шулік П. В. Використання віртуальних машин для організації захисту інформації на платформах INTEL // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління : тези доп. 15-ї міжнар. наук.-техн. конф., 24-25 квітня 2025р., м. Баку, м. Харків, м. Жиліна : [у 3 т.]. Т. 3. Харків : Impress, 2025. С. 98. Doi: <https://doi.org/10.32620/ICT.25.t3>.

Надійшла до редколегії 07.10.2025

Відомості про авторів:

Шулік Павло Вікторович – канд. техн. наук, ст. викладач кафедри безпеки інформаційних технологій, факультет комп'ютерної інженерії та управління, Харківський національний університет радіоелектроніки; Україна; e-mail: pavlo.shulik@nure.ua; ORCID: <https://orcid.org/0009-0004-6200-2172>

Балагура Дмитро Сергійович – канд. техн. наук, доцент кафедри безпеки інформаційних технологій, факультет комп'ютерної інженерії та управління; Харківський національний університет радіоелектроніки; Україна; e-mail: dmytro.balahura@nure.ua; ORCID: <https://orcid.org/0000-0002-6327-6405>

Просолов Владислав Валерійович – аспірант кафедри безпеки інформаційних технологій; Харківський національний університет радіоелектроніки; Україна; e-mail: vladyslav.prosolov@nure.ua; ORCID: <https://orcid.org/0009-0002-1276-4828>

В'юхін Данііл Олександрович – ст. викладач кафедри безпеки інформаційних технологій, факультет комп'ютерної інженерії та управління; Харківський національний університет радіоелектроніки; Україна; e-mail: daniil.viukhin@nure.ua; ORCID: <https://orcid.org/0009-0009-8442-9587>

*С.Я. ГИЛЬГУРТ, д-р техн. наук, Л.В. КОВАЛЬЧУК, д-р техн. наук,
А.М. ДАВИДЕНКО, д-р техн. наук*

ОГЛЯД ПІДХОДІВ ДО ПОБУДОВИ ЗАХИЩЕНИХ ЗАВАДОСТІЙКИХ СИСТЕМ ПЕРЕДАЧІ ПОТОКОВОГО ВІДЕО З БПЛА¹

Вступ

Останнім часом набуває масового поширення як в цивільних застосуваннях, так і у військовій сфері такий підклас безпілотних літальних апаратів (БпЛА), як FPV-дрони (від англ. First Person View). На фронті вони використовуються для розвідки та коригування вогню, але найбільш дієво зарекомендували себе в якості баражуючих боєприпасів (так звані FPV-дрони-камікадзе), що вражають цілі методом самознищення. Їх переваги – низька вартість (кілька сот доларів за одиницю) та висока точність ураження завдяки прямому відеоконтролю оператором (тобто віртуальної присутності людини безпосередньо у місці подій) протягом всього польоту.

Ключова вразливість таких дронів – радіоканал керування та передачі відеозображення. Особливо важливим є відеосигнал, що передається радіоканалом з бортової відеокамери БпЛА на наземну базову станцію, перехоплення якого ворожою стороною наражає на небезпеку дронівода. Тому цей канал зв'язку має бути захищений засобами захисту інформації. На сьогодні відомо багато підходів, методів та алгоритмів крипостійкого шифрування. Але внаслідок своєї реурсоємності вони вносять суттєву затримку в тракт передачі даних, і для їх реалізації потрібні обчислювальні ресурси, якими складно забезпечити легкий та дешевий модуль, придатний для використання у одноразових FPV-дронах-камікадзе.

З іншого боку, такі алгоритми, як правило, критичні до спотворення інформації в каналі зв'язку: заміна лише одного біту у повідомленні може призводити до втрати цілого блоку даних, або навіть всього повідомлення. Але в бойових умовах на відеоканал здійснюється вплив з боку ворожих засобів радіоелектронної боротьби (РЕБ). Ефективні глушники мають обмежену зону дії, але здатні виводити з ладу зв'язок FPV-дронів на критичній відстані. Це робить актуальним друге завдання – підвищення завадостійкості каналу передачі відеоданих. Відомо багато методів завадостійкого кодування, які втім не вирішують задачу захисту інформації і можуть бути легко декодовані противником. Методи скремблювання, які традиційно використовуються для закриття аналогових каналів відеозв'язку, згідно з практичним досвідом використання FPV-дронів-камікадзе у бойових умовах, не забезпечують потрібного рівня захищеності відеоканалу, оскільки дозволяють противнику за допомогою нескладних пристроїв зламати такий захист протягом одиниць хвилин.

Отже виникає важливе та нетривіальне завдання створення систем передачі відеоданих, які дозволяли б захищати інформацію, одночасно забезпечуючи надійність зв'язку в умовах штучних завад. В якості першого кроку на шляху вирішення даного завдання потрібно проаналізувати наявну інформацію про відомі підходи та методи як до захисту інформації, так і до підвищення завадостійкості каналів зв'язку.

Метою дослідження є попередній огляд останніх досягнень в галузі захисту інформації та корекції помилок, які можуть бути використані в якості прототипів для створення захищених завадостійких систем передачі потокового відео, придатних до інтеграції в існуючі безпілотні платформи FPV-дронів-камікадзе.

Отримані результати дозволять просунутися у напрямі створення концепції захищеної завадостійкої системи передачі відеоданих з БпЛА на наземну станцію, яка в свою чергу

¹ Дослідження виконане за фінансової підтримки з боку Національного фонду досліджень України, проєкт 2025.6/0109 "Захищена завадостійка система передачі відеоінформації з безпілотного літального апарата", номер державної реєстрації 0125U003164.

дозволить підвищити ефективність застосування FPV-дронів-камікадзе як у військових застосуваннях, так і в цивільних сферах (безпечний зв'язок для рятувальних дронів, правоохоронних органів тощо).

Огляд публікацій

В роботі [1] експлуатація безпілотних літальних апаратів розглядається як нова сфера кіберпротистояння, аналізуються ризики перехоплення, зламу чи глушіння сигналів управління та передачі даних. На основі прикладів з реальних бойових дій в Україні автори досліджують як поєднання військових і цивільних БпЛА змінює характер конфліктів гібридного типу. Робота звертає увагу на проблеми ідентифікації джерел керування, захисту від електронних атак і контролю за використанням цивільних безпілотників, що створює нові виклики для безпеки. Окрему увагу приділено питанням кіберзахисту та протидії зловмисному використанню безпілотних технологій, що підкреслює зростаючу роль кіберпростору у воєнних операціях.

Відомо, що противник активно застосовує переносні та встановлені на техніці засоби РЕБ для створення радіоперешкод на частотах передачі відеосигналів з дронів [2]. При цьому дружні засоби радіоелектронної боротьби також впливають на зв'язок з БпЛА через те, що свої пункти керування знаходяться ближче, як правило, РЕБ ефективніший проти них, ніж проти ворога [3].

Радикально вирішити проблему дозволяє заміна радіоканалу на оптоволоконну лінію зв'язку [4]. Однак такий підхід має суттєві недоліки – обмеження радіусу дії довжиною кабелю, ускладнення маневреності та ризик втрати зв'язку внаслідок пошкодження волоконного кабелю. Тому радіозв'язок досі залишається основним рішенням для забезпечення керування та передачі відеосигналу, отже проблема закриття каналу та підвищення завадостійкості залишається гострою.

Відомі рішення, що використовують криптографічні алгоритми шифрування, такі, як AES-256, та самоналагоджуванні MESH-мережі та частотний хопінг для протидії глушінню і перехопленню сигналу [5, 6].

Щодо підвищення завадостійкості, деякі сучасні цифрові системи (DJI FPV, Autel, тощо) використовують модульовані протоколи (OFDM на 2.4/5 ГГц) та розширення спектру для підвищення завадостійкості. Використовується також частотне перестрибування (FHSS) і пряме розширення спектру для каналів управління та ортогональне частотне мультиплексування (COFDM) для передачі а відео, що забезпечує вищу стійкість до шумів і перешкод [7]. Розробляються також спеціалізовані завадостійкі радіомодеми для БпЛА, які здатні динамічно змінювати частоту та знаходити "вікна" в спектрі ворожих глушників.

Відомі й інші рішення, пов'язані з безпекою передачі відеосигналу та використання БпЛА [8–12.] Але всі згадані розробки є складними та дорогими рішеннями, використання яких є доцільним на потужних, наприклад, розвідувальних БпЛА. До того ж важливим недоліком будь-яких цифрових систем є відчутна затримка, що є неприйнятним недоліком при застосуванні на дронах-камікадзе. З іншого боку, аналогові системи відеозв'язку, які завдяки малій затримці та природній властивості зберігати "картинку" навіть при великому відсотку втраченого сигналу найбільш поширені зараз саме на FPV-дронах, особливо вразливі, оскільки зазвичай працюють на фіксованих частотах (5.8 ГГц) і не шифрують радіосигнал. А методи захисту аналогового каналу на основі скремблювання не забезпечують потрібного рівня захищеності.

Деякі особливості передачі потокового відео з БпЛА

В роботах [13, 14] сформульовано основні вимоги та обмеження, які накладаються в реальних бойових умовах на тракт передачі відеоданих з бортової відеокамери на станцію керування. Час затримки передачі інформації вздовж всього каналу повинен мати порядок 20–100 мс. При цьому вимоги до стійкості криптозахисту такої системи набагато менш жорсткі порівняно з традиційним використанням криптозахисту – час, потрібний зловмиснику

для злому системи захисту з використанням потужних обчислювальних засобів, має бути порядку одиниць годин. Фактично, йдеться про тимчасову стійкість системи передачі відеозображення. Як наслідок, алгоритми, які шифрують відеопотік даних з БпЛА, мають належати скоріш до класу так званих малоресурсних алгоритмів [15], які за рахунок можливості зниження крипостійкості дозволяють скоротити ресурсні витрати та підвищити пропускну здатність. Тому доцільно ретельно проаналізувати роботи, присвячені саме таким алгоритмам.

Нижче розглянуто відомі розробки, присвячені малоресурсним алгоритмам шифрування та деяким іншим суміжним питанням, пов'язаним з забезпеченням захищеного завадостійкого відеозв'язку з БпЛА.

Малоресурсні алгоритми шифрування

У роботі [16] розглянуто питання автентифікації в системах керування БпЛА. Автори пропонують використовувати для цього малоресурсний асиметричний алгоритм NIGHT і зазначають, що для шифрування може застосовуватись також схема Фейстеля. Водночас у публікації не наведено конкретного алгоритму, який би відповідав вимогам щодо швидкодії та обсягу пам'яті, необхідним для оброблення відеоданих. Результати цієї роботи не можуть бути використані безпосередньо для захисту відеоданих, оскільки така задача вимагає значно більшої швидкодії.

У роботі [17] досліджується використання алгоритму AES у режимі EAX (encrypt-then-authenticate-then-translate) для шифрування відео- та аудіопотоків, що передаються з БпЛА. Експериментальні результати продемонстрували хороші показники при обробленні аудіосигналів навіть за умов помилок, проте показали низьку ефективність при шифруванні відео. Це пояснюється недостатньою швидкістю алгоритму AES, оскільки цей алгоритм першочергово розроблявся для досягнення високої крипостійкості, а не продуктивності.

У публікації [18] представлено малоресурсний блоковий шифр Piccolo з довжиною блоку 64 біти та ключем 80 або 128 біт. Це узагальнена схема Фейстеля з чотирма 16-бітними гілками, яка виконує 25 або 31 раунд залежно від довжини ключа. За обсягом пам'яті Piccolo подібний до поширеного шифру PRESENT [19], проте його пропускну здатність сягає лише 21,54 байта на секунду, що є недостатнім для відеошифрування, де допустима затримка не повинна перевищувати 0,03 секунди. Навіть зі зменшенням кількості раундів цей алгоритм залишається занадто повільним для оброблення відео.

У роботі [20] розглянуто застосування AES для шифрування даних, що передаються з БпЛА. Автори зазначають, що цей алгоритм використовується в українських дронах PD-2 та Shark для захисту телеметрії (швидкість, висота, координати тощо). Проте обсяг таких даних набагато менший, ніж у відеопотоці, і їх не обов'язково передавати безперервно в реальному часі. Тому AES, який добре підходить для невеликих обсягів інформації, не може бути ефективно застосований до відеошифрування через недостатню швидкість.

У дослідженні [21] представлено алгоритм шифрування зображень дикої природи, що передаються з БпЛА, побудований на поєднанні одно- та двовимірних клітинних автоматів (1D MCA і 2D MCA) із побітовими операціями додавання та перемішування. Основна увага приділена оцінці стійкості алгоритму та механізму генерації ключів. Проте в роботі відсутні дані щодо швидкодії та вимог до пам'яті, тому придатність цього методу для шифрування відео в реальному часі залишається невизначеною.

Робота [22] описує загальний фреймворк криптографічного захисту для малих дронів, який, за твердженням авторів, є енергоефективним і перевершує стандартні методи за швидкістю. До нього входить інфраструктура відкритих ключів (PKI) та алгоритми на еліптичних кривих. Однак конкретних алгоритмів для шифрування відео або даних про їх продуктивність не наведено.

У публікації [23] представлено малоресурсний шифр HANK-1, побудований за узагальненою схемою Фейстеля з чотирма гілками та вісьмома раундами. Його рекомендовано використовувати в режимі CBC. Алгоритм потребує 64 Кбайт пам'яті та забезпечує швидкість 84,1468 Кбіт/с, що робить його потенційно придатним для систем з обмеженими ресур-

сами. Водночас через малу кількість раундів і відсутність аналітичних оцінок стійкості застосування HANK-1 пов'язане зі значними ризиками. Автори наводять певні евристичні міркування та застосовують статистичні тести з пакету NIST [24], не отримуючи якихось аналітичних оцінок крипостійкості.

У роботі [25] запропоновано ультрамалоресурсний шифр Sriram, орієнтований на використання в RFID-мітках і сенсорних мережах. Це блоковий шифр Фейстеля зі SP-мережею, 64-бітовим блоком і ключем 96 або 128 біт, який виконує 27 раундів. Проте автори не надають кількісних характеристик щодо пам'яті чи пропускну здатності, тому придатність Sriram для відеошифрування оцінити неможливо.

У роботі [26] представлено блоковий алгоритм CARX для БпЛА, але зазначається, що для шифрування відео краще підходить потоковий алгоритм ZUC-128 [27], який має швидкість генерації гами 33,74 Кбіт/с і швидкість шифрування 23,31 Кбіт/с. Попри це, без тестування в реальних умовах не можна гарантувати необхідну затримку, а значний час ініціалізації робить ZUC-128 непридатним для використання в реальному часі.

У роботі [28] описано сімейство малоресурсних блокових шифрів SHIPHER, що базуються на динамічних операціях у різних алгебраїчних системах, подібно до шифру IDEA [29]. Автори заявляють про кращі показники швидкодії та пам'яті порівняно з AES, але не надають підтверджуючих даних. Використання операцій, відмінних від XOR, імовірно знижує продуктивність, тому питання часової затримки залишається відкритим.

У публікації [30] обговорюються проблеми безпеки БпЛА в аграрному секторі, зокрема ризик викрадення через підробку сигналів керування. Як контрзахід пропонується використання шифру Вернама, однак питання ресурсомісткості та швидкодії не розглядаються. Зберігання або генерація достатньо довгої гами без повторень вимагає великих обсягів пам'яті, що робить цей підхід малопридатним для реального застосування.

Стійкість до радіоелектронної боротьби

Робота [31] присвячена оцінюванню енергетичної доступності каналів зв'язку безпілотних літальних апаратів у контексті протидії засобам радіоелектронної боротьби противника. У роботі здійснено порівняльний аналіз різних технологій радіозв'язку для БПЛА з точки зору їхньої стійкості до радіоперешкод і ефективності використання енергетичних ресурсів. Автори показують, що більшість технологій вразливі до радіопридушення, проте використання широкосмугових систем із завадостійким кодуванням може істотно підвищити їхню надійність. На основі аналітичних розрахунків запропоновано рекомендації щодо використання типів модуляції, які забезпечують компроміс між енергетичною ефективністю та завадостійкістю, що має практичне значення для побудови безпечних комунікаційних каналів у складних електронних умовах.

В роботі [32] запропоновано метод багатоканальної компенсації завад для захисту комунікацій автономних літальних апаратів від радіопридушення. Розроблений підхід дозволяє одночасно здійснювати синхронізацію за часом і частотою та ефективно усувати вплив перешкод без потреби в попередньому знанні характеристик каналу чи сигналу завад. Метод ґрунтується на використанні відомої преамбули передавача, що спрощує реалізацію в існуючих протоколах зв'язку. Результати експериментів на апаратній платформі показали, що навіть за умови, коли потужність завад у 40 дБ перевищує потужність корисного сигналу, запропонована система здатна успішно відновлювати передану інформацію, забезпечуючи надійний і захищений зв'язок у складних умовах радіоелектронної боротьби.

В роботі [33] запропоновано міжрівневу архітектуру для передавання потокового мультимедіа з безпілотних літальних апаратів, що враховує динамічні зміни їхнього положення та швидкості. Створена система Client-Server-Ground&User (C-S-G&U) реалізує алгоритм розподілу навантаження Splitting-Merging Stream (SMS), який забезпечує одночасну передачу даних кількома каналами для підвищення пропускну здатності та зменшення затримки. Додатково застосовано механізми прямого виправлення помилок (Forward Error Correction – FEC), шифрування та динамічної адаптації режимів передавання відповідно до поточних

умов мережі. Експериментальна реалізація показала стабільність роботи системи при змінних параметрах польоту, що підтверджує ефективність запропонованої архітектури для надійної та безпечної передачі відеопотоку з БПЛА.

В роботі [34] досліджено задачу безпечного розподілу ресурсів у когнітивних МІМО-мережах для внутрішніх приміщень із залученням безпілотних літальних апаратів. Автори інтегрують технології когнітивного радіо, МІМО та О-RAN для створення енергоефективних і стійких до радіопридушення систем зв'язку. Розроблений алгоритм підвищує стійкість системи до атак заглушення та зменшує загальні енергетичні витрати при збереженні пропускну здатності мережі.

Препроцесінг та стиснення інформації перед шифруванням

В роботі [35] пропонується метод попередньої обробки відеоданих із безпілотних апаратів на основі вдосконаленого алгоритму стиснення цифрових зображень. Запропонований підхід спрямований на зменшення обсягу даних без суттєвих втрат якості зображення перед подальшим шифруванням. Метод поєднує інваріантні перетворення та виділення фону, що дозволяє досягати високого рівня стиснення та підвищити ефективність подальших етапів криптографічної обробки. Мета такої попередньої обробки – зменшити обсяг даних на борту БПЛА перед шифруванням. Скорочення бітрейту знижує вимоги до ресурсноємності процедури шифрування, але припускає можливість втрати якості, що може ускладнити подальше використання відеозображення.

Додаткові питання автентифікації

Автори роботи [36] пропонують інноваційний підхід до захисту каналів зв'язку безпілотних літальних апаратів, який ґрунтується на використанні біометричних характеристик оператора, отриманих із сигналів електроенцефалограма (ЕЕГ). Метод передбачає генерування криптографічного ключа на основі коефіцієнтів Бета-хвиль, оброблених за допомогою поліномів Лежандра та кодів Боуза–Чоудхурі–Хоквінгема. Такий ключ використовується для шифрування комунікації між БПЛА та базовою станцією, забезпечуючи унікальність і неможливість підробки. У разі виявлення атаки система автоматично переводить дрон у безпечний режим повернення. Проведені експерименти довели працездатність концепції на комерційному БПЛА, що підтверджує потенціал біометричного підходу до захисту бездротових каналів зв'язку. Висунута авторами дослідження ідея цікава з точки зору підвищення безпеки зв'язку, але додає складнощів при практичній реалізації та використанні, особливо в польових/бойових умовах.

Швидкодія та використання ПЛІС / SoC

В роботі [37] докладно розглянуто моделювання потоку керуючих даних радіоканалу безпілотного літального апарата. Автори досліджують вплив криптографічних перетворень на динамічні характеристики каналу, зокрема затримки сигналів і можливі похибки під час польоту апарата. Експериментальні результати, отримані в умовах, наближених до реальних, демонструють, як криптографічні механізми впливають на часові параметри управління та точність реакції системи. Отримані результати зокрема свідчать про потребу в швидких засобах реалізації криптографічних алгоритмів.

Робота [38] демонструє переваги використання ПЛІС типу FPGA для реалізації шифрування/дешифрування, які дозволяють знизити як затримку обробки інформації, так і енергоспоживання порівняно з реалізаціями на мікропроцесорах та мікроконтролерах. Програмова логіка відкрила шлях до апаратного шифрування не лише телеметричних даних, але й також відеоданих. Апаратна реалізація дозволяє забезпечити потрібну пропускну здатність для повноформатного відео. Зворотній бік застосування ПЛІС – вища порівняно з традиційним програмуванням складність проектування, більша ціна FPGA-чіпів та певна спеціалізована "обв'язка" мікросхем програмованої логіки порівняно з відпрацьованими цифровими схемами на мікроконтролерах.

Запропонована в роботі [39] схема шифрування відео QuVench побудована на принципах квазігрупового перетворення, орієнтована на забезпечення безпечної передачі стиснено-

го відео в реальному часі. Реалізовано її на так званій системі-на-кристалі (System on the Chip – SoC), яка є об'єднанням в одному електронному пристрої реконфігурованої матриці, як в ПЛІС, та потужного апаратного мікропроцесорного ядра. У дослідженні підкреслюється важливість швидкої обробки відеоданих у пристроях із обмеженими ресурсами, зокрема в безпілотних апаратах. Використання SoC демонструє можливість досягнення майже миттєвого шифрування та дешифрування майже без затримки, мінімізуючи апаратні витрати.

Аналіз інформації

Аналіз літературних джерел дозволяє поділити дослідження у сфері захищеного відеозв'язку з БпЛА на кілька напрямів.

Першу групу становлять роботи, що стосуються шифрування зображень або невеликих обсягів даних, наприклад, такі як [16, 18, 21, 30]. Ці алгоритми призначені для автентифікації, захисту телеметрії чи одиничних кадрів і не відповідають вимогам систем реального часу. Хоча вони демонструють високу криптостійкість, їхня швидкодія та обчислювальні потреби є надмірними для FPV-дронів, що працюють у режимі низьких затримок.

Другу групу утворюють дослідження, такі як [20, 26, 28], в яких запропоновано високостійкі, проте ресурсомісткі рішення, орієнтовані на потужні розвідувальні або інші багаторазові платформи. Використання повновимірних блокових алгоритмів шифрування забезпечує надійність, але не задовольняє обмеженням щодо затримки та енергоспоживання. Подібні підходи практично непридатні для легких, дешевих одноразових FPV-дронів-камікадзе.

До третьої групи можна віднести праці, де розглядаються малоресурсні алгоритми, орієнтовані на енергоефективність та простоту реалізації, наприклад [23, 25]. Розглянуті в них алгоритми потенційно придатні для шифрування відеопотоку, однак їх криптостійкість не має теоретичного обґрунтування, а швидкодія не перевірена експериментально.

Решта робіт, такі як [17, 22, 31], описують експерименти з використанням традиційних алгоритмів шифрування, але демонструють суттєві затримки чи відсутність практичних результатів.

Щодо забезпечення завадостійкості каналів, у низці публікацій запропоновано застосування ширококутових технологій, когнітивного радіо, МІМО-архітектур, алгоритмів багатоканальної компенсації завад та адаптивних методів кодування [31–34]. Ці підходи показують ефективність у протидії засобам РЕБ, однак не враховують одночасної потреби у шифруванні відеопотоку з мінімальною затримкою.

В дослідженнях [37–39] показано, що апаратні рішення на базі програмованої логіки надає можливість скоротити час обробки та знизити енергоспоживання, що відкриває перспективу апаратних рішень.

Таким чином, аналіз свідчить про відсутність готового комплексного рішення, здатного одночасно забезпечити потрібний криптографічний захист і достатню стійкість до радіоперешкод в режимі реального часу. Це створює передумови для розробки нових методів, що поєднують малоресурсне шифрування та корекцію помилок, які можна реалізовувати у вигляді легких та дешевих апаратно-програмних бортових модулів для БпЛА.

Невирішеність даного питання обумовлена об'єктивними причинами. Це, насамперед, стрімкий розвиток безпілотних технологій, особливо – БпЛА типу FPV, які суттєво змінили картину сучасних бойових дій. В результаті посилилися вимоги до швидкісних, масогабаритних та вартісних характеристик бортового електронного обладнання. З іншого боку, набагато більш короткий період життя таких апаратів дозволяє покращити характеристики каналу передачі відеоданих за рахунок зниження стійкості алгоритмів шифрування. Саме з цього випливає необхідність при подальших дослідженнях приділити найбільшу увагу малоресурсним алгоритмам шифрування при одночасному підвищенні їх завадостійкості.

Висновки

Огляд літературних джерел підтвердив, що наявні методи шифрування відеоданих, які передаються з безпілотних літальних апаратів, або забезпечують високу криптостійкість за рахунок задіяння надмірних ресурсів, або не гарантують достатньої криптостійкості. При цьому сучасні засоби радіоелектронної боротьби створюють суттєві перешкоди для каналу

передачі даних, тому завдання шифрування відеопотоку необхідно розглядати спільно з проблемою завадостійкості.

Жодне з відомих рішень не задовольняє одночасно вимогам як до швидкодії, енергоспоживання та крипостійкості, так і до потрібної стійкості щодо радіоперешкод, щоб їх можна було безпосередньо використати для створення систем передачі відеосигналу з FPV-дронів-камікадзе.

Ефективним шляхом зменшення затримки та енергоспоживання є використання апаратних рішень на базі ПЛІС або систем-на-кристалі, які дозволяють реалізувати у реальному часі паралельну реалізацію алгоритмів обробки відеопотоку, здійснюючи одночасно шифрування та корекцію помилок.

Отримані результати свідчать про потребу у створенні нової концепції захищеної завадостійкої системи передачі поточкового відео з БПЛА, що базуватиметься на принципах тимчасової крипостійкості, адаптивної завадостійкості та апаратної оптимізації. Подальші дослідження мають бути спрямовані на моделювання таких систем, експериментальну перевірку їх ефективності та розробку прототипів для практичного використання на військових і цивільних безпілотних платформах.

Список літератури:

1. Hartmann K., Giles K. UAV exploitation: a new domain for cyber power. 2016 8th international conference on cyber conflict (CyCon), Tallinn, 31 May – 3 June 2016. Tallinn, 2016. P. 205–221. <https://doi.org/10.1109/CYCON.2016.7529436>.
2. Способи протидії FPV-дронам (з ворожого довідника «Тактика применения противником FPV-дронов и способы противодействия»). Статті компанії «FPV-дрони та аксесуари для аеророзвідки». "FPV-дрони та аксесуари для аеророзвідки" – контакти, товари, послуги, ціни. Режим доступу: <https://drone.in.ua/ua/a506352-sposobi-protidiyi-fpv.html>.
3. Гліб, Керівник інструкторського напрямку БПЛА фонду «Повернись живим». Чому дрони не падають під РЕБом. Режим доступу: <https://savelife.in.ua/materials/blogs/chomu-drony-ne-padayut-pid-rebom/>.
4. Focus: Why jamming isn't a solution against FPV anymore in Ukraine's offensive initiative. Defense News security global military army equipment industry. Режим доступу: <https://armyrecognition.com/news/aerospace-news/2024/focus-why-jamming-isnt-a-solution-against-fpv-anymore-in-ukraines-offensive-initiative>.
5. Litnarovych V. Himera, Skiftech & More: How ukraine's defense tech companies are breaking into the US market. UNITED24 Media. Режим доступу: <https://united24media.com/latest-news/himera-skiftech-more-how-ukraines-defense-tech-companies-are-breaking-into-the-us-market-6942>.
6. Secure Real-Time Multimedia Data Transmission from Low-Cost UAVs with A Lightweight AES Encryption / N. Cecchinato et al. // IEEE communications magazine. 2023. Vol. 61, no. 5. P. 160–165. <https://doi.org/10.1109/MCOM.001.2200611>.
7. Drone defense system : patent US10339818B2 United States : G08G 5 / 00, H04W 76 /10. No. 15 /358574 ; applied on 22.11.2016 ; published on 25.05.2017. <https://patentimages.storage.googleapis.com/96/9b/c4/04589f6c523d45/US10339818.pdf>.
8. UAV anti-jamming video transmissions with qoe guarantee: a reinforcement learning-based approach / L. Xiao et al. // IEEE transactions on communications. 2021. Vol. 69, no. 9. P. 5933–5947. <https://doi.org/10.1109/tcomm.2021.3087787>.
9. Psilias D., Milidonis A., Voyiatzis I. Secure video transmission system for UAV applications / ed. by M. G. Vassilakopoulos, N. N. Karanikolas. Association for Computing Machinery, 2021. <https://doi.org/10.1145/3503823.3503882>.
10. Samanth S., K V P., Balachandra M. Security in internet of drones: a comprehensive review // Cogent engineering. 2022. Vol. 9, no. 1. <https://doi.org/10.1080/23311916.2022.2029080>.
11. Encryption and decryption of media data : patent EP3695560B1 United States : H04L 9/40, H04L 9/06, H04L 9/08, H04W 4/44. No. 18796555.3 ; applied on 12.10.2018 ; published on 09.10.2024, Bulletin no. 2024/41. <https://data.epo.org/publication-server/rest/v1.2/publication-dates/2024-10-09/patents/EP3695560NWB1/document.pdf>.
12. Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions / S. Singh et al. // Journal of ambient intelligence and humanized computing. 2017. <https://doi.org/10.1007/s12652-017-0494-4>.
13. Гільгурт С. Аналіз вимог до системи передачі відеоінформації з FPV-дрона-камікадзе на наземну базову станцію // Проблеми інформатики та моделювання (ПІМ-2025) : Тези двадцять третьої міжнар. науково-техн. конф., м. Харків, 25–28 верес. 2025 р. Харків, 2025. С. 15. https://web.kpi.kharkov.ua/pim/?page_id=327.
14. Гільгурт С., Яблоков І. Застосування ПЛІС для захисту каналу передачі відеоінформації з БПЛА з використанням штучного інтелекту // Безпека сучасних інформаційно-комунікаційних систем : зб. доп. Міжнар. наук.-техн. конф. SMICS-2025, м. Львів, 16–18 жовт. 2025 р. Львів, 2025.

15. Survey on the authentication and key agreement of 6LoWPAN: open issues and future direction / F. F. Ashrif et al. // Journal of network and computer applications. 2024. Vol. 221. P. 103759. <https://doi.org/10.1016/j.jnca.2023.103759>.
16. Al-Ta'i Z. T. M., Ismael H. M. Authentication and encryption drone communication by using HIGHT lightweight algorithm // Turkish journal of computer and mathematics education. 2021. Vol. 12, no. 11. P. 5891–5908. https://www.researchgate.net/publication/392193717_Authentication_and_Encryption_Drone_Communication_by_Using_HIGHT_Lightweight_Algorithm.
17. A secure real-time multimedia streaming through robust and lightweight AES encryption in UAV networks for operational scenarios in military domain / N. Cecchinato et al. ; ed. by G. L. Foresti, C. Drioli. Elsevier B.V., 2022. Vol. 205. <https://doi.org/10.1016/j.procs.2022.09.006>.
18. Rahiyanath T. Y. A novel architecture for lightweight block cipher, piccolo // International journal of research in engineering and technology. 2015. Vol. 04, no. 09. P. 97–103. <https://doi.org/10.15623/ijret.2015.0409017>.
19. PRESENT: an ultra-lightweight block cipher / A. Bogdanov et al. Cryptographic hardware and embedded systems - CHES 2007. Berlin, Heidelberg, P. 450–466. https://doi.org/10.1007/978-3-540-74735-2_31.
20. Сафронов Т. AES-256: В Ukrspesystems розкрили деталі шифрування даних БПЛА Shark. MILITARNY. <https://militarnyi.com/uk/news/zahyst-danyh-vid-bpla-shark-posylyly-shyfruvannyam-aes-256/>.
21. Belazi A., Migallón H. Drone-Captured wildlife data encryption: A hybrid 1D–2D memory cellular automata scheme with chaotic mapping and SHA-256 // Mathematics. 2024. Vol. 12, no. 22. P. 3602. <https://doi.org/10.3390/math12223602>.
22. Ozmen M. O., Yavuz A. A. Dronecrypt – an efficient cryptographic framework for small aerial drones // MILCOM 2018 - IEEE military communications conference, Los Angeles, CA, 29–31 October 2018. 2018. <https://doi.org/10.1109/milcom.2018.8599784>.
23. HANK-1, A new efficient and secure block cipher algorithm for limited resources devices / H. Eldeeb et al. The international conference on electrical engineering, P. 1–12. <https://doi.org/10.21608/iceeng.2012.30662>.
24. Special Publication 800-22 Revision 1a. A statistical test suite for random and pseudorandom number generators for cryptographic applications. Official edition. 2010. <https://doi.org/10.6028/nist.sp.800-22r1a>.
25. Ramudu S., Shanthi G. Implementation of an ultra-lightweight block cipher // International journal & magazine of engineering, technology, management and research. 2015. Vol. 2, no. 2. P. 233–242. <http://www.ijmetmr.com/olfebruary2015/SriRamudu-GShanthi-39.pdf>.
26. LWED: Lightweight white-box encryption communication system for drones over CARX algorithm / Y. Yang et al. // Journal of king saud university - computer and information sciences. 2023. P. 101727. <https://doi.org/10.1016/j.jksuci.2023.101727>.
27. WBZUC: novel white-box ZUC-128 stream cipher / Y. Yatao et al. // The journal of china universities of posts and telecommunications. 2023. Vol. 11, no. 78. P. 96–106. <https://doi.org/10.19682/j.cnki.1005-8885.2022.0022>.
28. Hei X., Song B., Ling C. SHIPHER: a new family of light-weight block ciphers based on dynamic operators // ICC 2017 - 2017 IEEE international conference on communications, Paris, France, 21–25 May 2017. 2017. <https://doi.org/10.1109/icc.2017.7996731>.
29. Lai X., Massey J. L. A proposal for a new block encryption standard. Advances in Cryptology – EUROCRYPT '90. Berlin, Heidelberg, 1991. P. 389–404. https://doi.org/10.1007/3-540-46877-3_35.
30. A method of encrypting the traffic of quadcopters through an A nalog path during monitoring of agricultural ground objects / Y. Meleshko et al. // National interagency scientific and technical collection of works. design, production and exploitation of agricultural machines. 2021. No. 51. P. 216–226. <https://doi.org/10.32515/2414-3820.2021.51.216-226>.
31. Evaluating the uav's communication channels energy availability in the context of enemy electronic countermeasures / D. Bakhtiarov et al. // 2024 IEEE 7th international conference on actual problems of unmanned aerial vehicles development (APUAVD), Kyiv, Ukraine, 22–24 October 2024. 2024. P. 159–164. <https://doi.org/10.1109/apuavd64488.2024.10765900>.
32. Jamming-Resistant AAV communications: a multichannel-aided approach / B. Wang et al. // IEEE wireless communications letters. 2025. Vol. 14, no. 7. P. 1939–1943. <https://doi.org/10.1109/LWC.2025.3559501>.
33. Liu Z., Jiang Y. Cross-Layer design for uav-based streaming media transmission // IEEE transactions on circuits and systems for video technology. 2022. Vol. 32, no. 7. P. 4710–4723. <https://doi.org/10.1109/TCSVT.2021.3125864>.
34. Bany Salameh H., Al-Obiedollah H., Aloqaily M. Secure batch-based resource allocation for green cognitive MIMO indoor flying networks // IEEE transactions on green communications and networking. 2024. Vol. 8, no. 3. P. 1090–1098. <https://doi.org/10.1109/TGCN.2024.3387899>.
35. Advanced method for compressing digital images as a part of video stream to pre-processing of UAV data before encryption / Z. Hu et al. // Springer Science and Business Media Deutschland GmbH, 2023. Vol. 181. https://doi.org/10.1007/978-3-031-36118-0_33.
36. Singandhupe A., La H. M., Feil-Seifer D. Reliable security algorithm for drones using individual characteristics from an EEG signal // IEEE access. 2018. Vol. 6. P. 22976–22986. <https://doi.org/10.1109/ACCESS.2018.2827362>.

37. Bakhtiarov D., Konakhovych G., Lavrynenko O. Protected system of radio control of unmanned aerial vehicle // Institute of Electrical and Electronics Engineers Inc., 2016. <https://doi.org/10.1109/MSNMC.2016.7783141>.
38. Secure video and telemetry FPGA architecture for uavs / D. Psilias et al. // Institute of Electrical and Electronics Engineers Inc., 2024. <https://doi.org/10.1109/SEEDA-CECNSM63478.2024.00021>.
39. Real-Time compressed video encryption: based on quasigroup on system on chip (SOC) / D. Haridas et al. // SN computer science. 2021. Vol. 2, no. 5. <https://doi.org/10.1007/s42979-021-00793-4>.

Надійшла до редколегії 17.09.2025

Відомості про авторів:

Гільгурт Сергій Якович – д-р техн. наук, Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, ст. наук. співробітник, зав. відділу математичного та економетричного моделювання; Україна; e-mail: hilgurt@ukr.net; ORCID: <https://orcid.org/0000-0003-1647-1790>

Ковальчук Людмила Василівна – д-р техн. наук, професор, Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, пров. наук. співробітник; Україна; e-mail: lusi.kovalchuk@gmail.com; ORCID: <https://orcid.org/0000-0003-2874-7950>

Давиденко Анатолій Миколайович – д-р техн. наук, професор, Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, пров. наук. співробітник; Україна; e-mail: davidenkoan@gmail.com; ORCID: <https://orcid.org/0000-0001-6466-1690>

*І.В. ОЛЕШКО, канд. техн. наук, В.І.ЛУЦЕНКО, О.Є. ПЕТРЕНКО, канд. техн. наук,
О.А. МЕЛЬНИКОВА, канд. техн. наук*

ОЦІНКА ЕФЕКТИВНОСТІ АТАК З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ НА СИСТЕМИ БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ ЗА ВІДБИТКАМИ ПАЛЬЦІВ

Вступ

У сучасному цифровому середовищі, де обсяг онлайн-транзакцій, мобільних сервісів та віддалених комунікацій невідомо зростає, питання надійної автентифікації користувачів набуває особливої ваги. Традиційні методи захисту, зокрема паролі та PIN-коди, дедалі частіше демонструють свою вразливість перед кіберзагрозами, що стимулює пошук більш стійких та зручних рішень. На цьому тлі біометрична автентифікація стає одним із ключових напрямів підвищення безпеки інформаційних систем. Її популярність зумовлена високою точністю, складністю підроблення та простотою використання. Одним з найпоширеніших методів біометричної автентифікації є автентифікація за відбитками пальців.

Зі стрімким розвитком технологій штучного інтелекту виникають принципово нові кібератаки для біометричних систем автентифікації. Завдяки можливостям ШІ, зокрема машинному навчанню, зломисники мають змогу моделювати та відтворювати біометричні дані з метою обходу систем біометричної автентифікації.

Метою статті є оцінка ефективності розповсюджених атак з використанням штучного інтелекту на системи біометричної автентифікації за відбитками пальців. Наші дослідження можуть бути корисними при розробці та тестуванні нових та існуючих біометричних систем автентифікації, для впровадження захисту критичної інфраструктури та фізичного доступу, а також для аудиту і стандартизації безпеки.

Огляд літературних джерел

Системи біометричної автентифікації на основі відбитків пальців є однією з найпоширеніших технологій в комерційних і мобільних додатках, що підтверджується зростанням ринку та широкою інтеграцією в доступні рішення [1]. Одночасно в літературі фіксується, що найбільш розповсюдженим видом загроз для цих систем залишаються спуфінг-атаки, коли зломисник намагається видати цифрову копію відбитка за істинне зображення для обходу сенсорів [2].

Сучасні дослідження показують, що розвиток генеративних моделей і методів глибокого навчання створюють нові загрози для систем біометричної автентифікації, зокрема шляхом генерації синтетичних образів, які можуть сприйматися системами біометричної автентифікації, як істинні [3]. Генеративні змагальні мережі або ж GAN є класом методів машинного навчання, який складається з двох нейронних мереж, генератора і дискримінатора. Ці мережі змагаються між собою в рамках теорії ігор [4]. Метою GAN є створення моделі, яка здатна синтезувати зразки, схожі на реальні дані з навчального набору. Згенерована інформація оцінюється і переглядається дискримінатором, який намагається відрізнити синтетичні дані від реальних. Генератор постійно покращує якість своїх вихідних даних так, щоб дискримінатор не міг їх відрізнити від справжніх [5]. Дослідження показують, що атаки на основі штучного інтелекту часто комбінують різні стратегії та підходи, що підвищує їхню стійкість у реальних сценаріях [6].

Таким чином, оцінка ефективності атак на основі штучного інтелекту є ключовою передумовою безпечного функціонування сучасних біометричних систем та їх подальшого розвитку.

1. Система біометричної автентифікації за відбитками пальців

Відбитки пальців являють собою унікальні генетичні риси, притаманні людині від народження. Зазвичай вони різняться між собою завдяки особливостям візерунків, що складаються з гребенів і западин. Саме ці деталі відіграють вирішальну роль у процесі ідентифікації відбитків. Для розпізнавання переважно використовуються точки роздвоєння гребенів та

кінцеві точки [7]. Зазвичай алгоритми розпізнавання базуються на збігу дрібниць, аналізу ключових точок, напрямів гребенів та загальної геометрії візерунку, перетворюючи ці характеристики у числові вектори. Дрібниці відбитків пальців мають особливості, зображені на рис. 1.

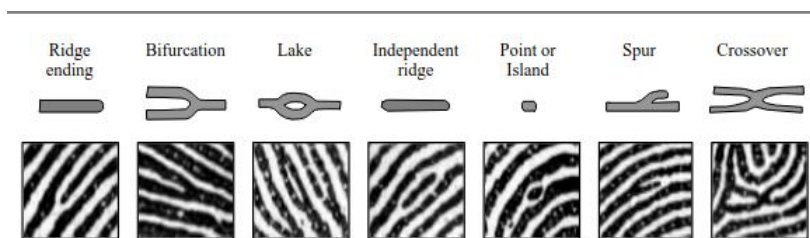


Рис. 1. Дрібниці відбитків пальців

Коефіцієнт подібності сам по собі не обов'язково вказує на те, чи належать два зображення відбитків пальців одній і тій самій людині. Натомість він показує, наскільки складно зіставити два відбитки. Хоча шаблони з високими показниками подібності найімовірніше належать одному й тому ж пальцю, це не завжди так. У системах розпізнавання за відбитками пальців можна обчислити три типи оцінок подібності на основі дрібниць [7]: локальна попарна оцінка, що вимірює відмінності для кожної пари дрібниць; глобальна оцінка, що аналізує співвідношення кількості співпалих дрібниць до їх загальної кількості; та гібридні оцінки, які поєднують інформацію на локальному і глобальному рівні.

Кожна дрібниця може бути описана кількома атрибутами, включаючи її розташування на зображенні, орієнтацію та тип. Найпоширеніші алгоритми зіставлення розглядають кожну дрібницю як триплет $m = \{x, y, \theta\}$, що вказує координати розташування мінуції $\{x, y\}$ та кут мінуції θ :

$$T = \{m_1, m_2, \dots, m_m\}, m_i = \{x_i, y_i, \theta_i\}, \quad i = 1 \dots m$$

$$I = \{m'_1, m'_2, \dots, m'_n\}, m'_j = \{x_j, y_j, \theta_j\}, \quad j = 1 \dots n$$

Дрібниця у зображенні I та дрібниця у шаблоні T вважаються відповідними, якщо просторова відстань між ними менша за задану допустиму величину (формула (1)), а різниця напрямків між ними менша за кутову допустиму величину (формула (2)). Згідно з цими формулами при обчисленні різниці кутів враховується їхня циклічність. Допустимі межі необхідні для компенсації неминучих помилок, що виникають під час виділення ознак, а також для врахування можливих деформацій пальця:

$$sd(m'_j, m_i) = \sqrt{(x'_j - x_i)^2 + (y'_j - y_i)^2} \leq r_0 \quad (1)$$

$$dd(m'_j, m_i) = \min(|(\theta'_j - \theta_i)|, 360^\circ - |(\theta'_j - \theta_i)|) \leq \theta_0 \quad (2)$$

Вирівнювання двох відбитків пальців є обов'язковим етапом [7], спрямованим на максимізацію кількості співставлених дрібниць. Коректне вирівнювання потребує визначення параметрів зміщення (по осях x та y) та обертання (кут θ). Для опису процедури вирівнювання вводять функції, зокрема $\text{map}()$, яка відображає дрібницю з відбитка I у нову позицію, та індикаторну функцію $\text{mm}()$, що повертає 1, коли мінуції відповідають критеріям зіставлення (1) та (2), і 0 в іншому випадку.

З урахуванням введених функцій, задачу зіставлення можна сформулювати наступним чином:

$$\max_{\Delta x, \Delta y, \theta, P} \sum_{i=1}^m \text{mm}(\text{map}_{\Delta x, \Delta y, \theta}(m'_{P(i)}, m_i)) \quad (3)$$

де $P(i)$ – невідома функція, яка визначає пару між I та T мініатюрами.

Формалізована задача вирівнювання полягає у визначенні параметрів геометричного перетворення, що максимізують кількість відповідностей між дрібницями порівнюваних відбитків.

Схожість між двома шаблонами дрібниць розраховується по формулі [8]

$$r_0 = \frac{N_M^2}{N_Q * N_R} \quad (4)$$

2. Атаки з використанням штучного інтелекту на системи біометричної автентифікації за відбитками пальців

Спуфінг відбитків пальців є однією з найпоширеніших атак на біометричні системи. Із появою генеративних моделей, зокрема GAN, ця проблема стала ще гострішою, оскільки з'явилася можливість створювати високоякісні синтетичні відбитки пальців, не маючи доступу до оригіналів. Однією з таких моделей є SpoofGAN, запропонована у 2022 р. [9]. Процес генерації зображення в ній складається з трьох етапів: спочатку відбувається синтез базового відбитка (бінарного зображення структури гребенів) з використанням латентного вектора $z_{id} \in \mathbb{R}^{256}$; далі йде створення різних відбитків шляхом застосування реалістичних трансформацій до базового зображення; на завершальному етапі відбувається накладання текстур за допомогою другої нейронної мережі для імітації реалістичної шкіри. На рис. 2 зображено структуру GAN моделі SpoofGAN з трьома основними етапами.

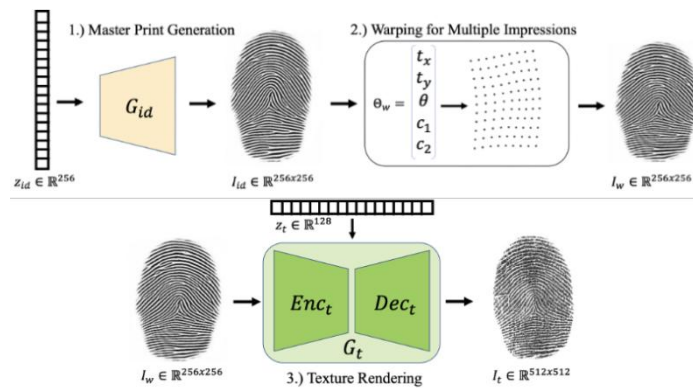


Рис. 2. Архітектура GAN моделі SpoofGAN

Більш новітній підхід, FingerFaker, запропонований у 2023 р., використовує концепцію псевдонабору дрібниць. Це дозволяє генерувати синтетичні відбитки без доступу до даних користувача [10]. Атака починається з випадкової ініціалізації популяції псевдодрібниць, яка обробляється генетичними операторами. Попередньо навчений генератор створює фальшиві відбитки, які надсилаються в систему розпізнавання. Якщо атака не вдається, FingerFaker використовує показники якості та результати порівняння для вибору наступного покоління псевдонаборів і повторює процес.

Алгоритм Фенга і Джейн реалізовано шляхом розбиття цільового простору на квадратні блоки 8×8 пікселів. Для кожного блоку прогнозується локальна орієнтація гребенів на основі напрямків найближчих дрібниць (використовується до восьми дрібниць, по одній з кожного з восьми секторів навколо блоку) [11]. Щоб врахувати періодичність, кути напрямків дрібниць a_k подвоюються. Потім орієнтація обчислюється через зважене агрегування тригонометричних компонентів, де w_k є ваговою функцією, що визначає вплив дрібниці k :

$$u = \sum_{k=1}^K \cos(2a_k) w_k \quad (7)$$

$$u = \sum_{k=1}^K \cos(2a_k) w_k \quad (8)$$

Фінальна орієнтація блоку $O(m, n)$ обчислюється як:

$$O(m, n) = \frac{1}{2} \arctan \left(\frac{v}{u} \right) \quad (9)$$

Блок-схема алгоритму реконструкції відбитків пальців Фенга і Джейн зображена на рис. 3.

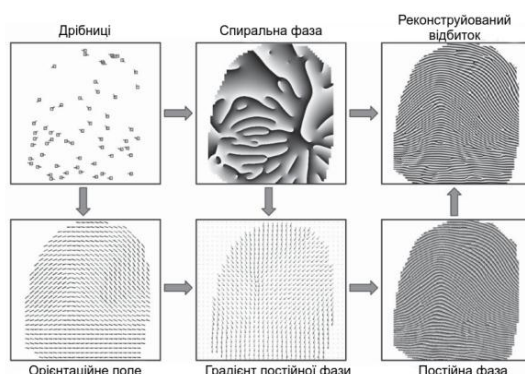


Рис. 3. Блок-схема алгоритму реконструкції відбитків пальців Фенга і Джейн

Методу відновлення відбитку пальця також представили Бузагло та Келлер у 2022 р. Було запропоновано використовувати енкодер дрібниці до вектора, де $x \in \mathbb{R}^{h \times w \times 3}$ – зразок відбитку пальця, а $S_x = \{\theta_{ij}, T_{ij}\}$ – набір дрібниць отриманих з x в точці $\{i, j\}$, θ_{ij} є напрямом і T_{ij} є класом дрібниці. Модель відновлення має на меті реконструювати x зображення за заданим набором S_x . Основною задачею на початку є перетворення набору дрібниць у мапу дрібниць $M_x \in \mathbb{R}^{h \times w \times 3}$. Після цього мапа дрібниць кодується у латентний вектор $w \in \mathbb{R}^{512}$ та подається до генератора GAN моделі, яка реконструює відбиток пальця [12].

У табл. 1 наведено порівняння розглянутих методів атак з використанням штучного інтелекту на системи біометричної автентифікації за відбитками пальців.

Таблиця 1

Назва методу	Тип атаки	Переваги	Недоліки та обмеження	Можливість цільового спрямування
SpoofGAN	Синтетична генерація	Висока точність генерації, не потребує фізичного доступу до оригіналу	Вимагає значних обчислювальних ресурсів, генерує випадкові особистості	Відсутня
FingerFaker	Синтетична генерація	Не потребує доступу до даних жертви	Висока ресурсомісткість навчання, складність налаштування	Відсутня
Метод Фенга і Джейна	Реконструкція з шаблону	Використовує лише стандартні дані дрібниць із шаблонів	Обмежена реалістичність без додаткових даних про текстуру	Наявна
Метод Бузагло та Келлер	Реконструкція з шаблону	Висока точність реконструкції завдяки використанню GAN	Залежність результату від якості класифікації вхідних дрібниць	Наявна

На основі порівняння визначено, що хоча методи синтетичної генерації демонструють високу точність у створенні загальних біометричних образів, вони не становлять прямої загрози для конкретних облікових записів без додаткових механізмів підбору. Найбільшу небезпеку для персоналізованої безпеки становлять методи реконструкції, які дозволяють зловмиснику відновити унікальний папілярний візерунок конкретної особи з компрометованого шаблону.

3. Експериментальне дослідження атаки методом реконструкції відбитку пальця

3.1. Налаштування експерименту

Для проведення експериментального дослідження необхідна система з наступними характеристиками:

- операційна система Ubuntu 20.04 і вище;
- процесор Intel Core i5 або AMD Ryzen 5 з тактовою частотою від 2.5 ГГц;
- оперативна пам'ять обсягом не менше 8 ГБ;
- відеокарта з підтримкою CUDA та обсягом пам'яті не менше 4 ГБ з рекомендацією використання NVIDIA RTX серії;
- вільне місце на жорсткому диску обсягом не менше 30 ГБ для зберігання моделей та проміжних результатів;
- клавіатура та миша для взаємодії з інтерфейсом програми.

Центральним елементом архітектури є генератор відбитків пальців, побудований на основі StyleGAN2, який попередньо натренований на наборі даних NIST SD14.

Практична реалізація виконана мовою Python 3.8. Для нормального функціонування програми необхідно встановити PyTorch версії 1.8 або вище для роботи з нейронними мережами, OpenCV – для обробки зображень, NumPy – для роботи з багатовимірними масивами, SciPy – для математичних операцій.

Детектор дрібниць MINDTCT, розроблений NIST, необхідний для отримання характеристик дрібниць з оригінальних зображень відбитків 512x512 у форматах PNG або JPG.

Архітектура з використанням CUDA потрібна для ефективної паралельної обробки на GPU.

3.2. Проведення експерименту

Обраний для дослідження метод реконструкції відбитків базується на праці Бузагло та Келлера. Загальна архітектура є конвеєром, що складається з чотирьох основних компонентів: модуль обробки дрібниць, блок алгоритмічного перетворення, енкодер на основі ResNet50 та генератор StyleGAN2. Загальна схема обраного методу зображена на рис. 4.

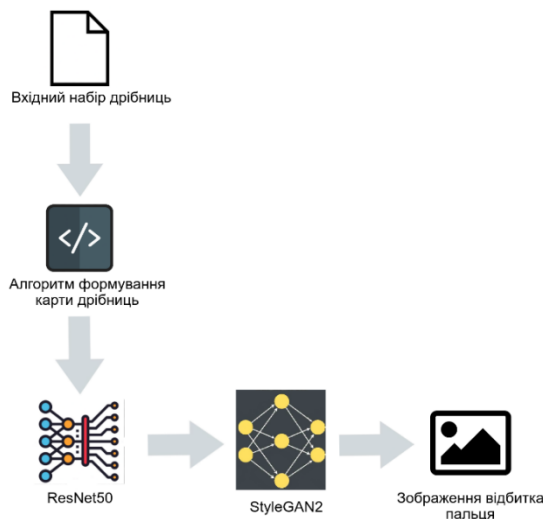


Рис. 4. Загальна архітектура обраного методу реконструкції

Процес реконструкції починається з обробки дрібниць: на початковому етапі дискретний набір мінуцій перетворюється у структуроване просторове представлення. Спеціалізований алгоритмічний блок перетворює цей набір у тривимірний тензор розміром $h * w * 3$, де h та w відповідають висоті та ширині цільового зображення відповідно.

Отримана карта дрібниць M_x піддається операції згортки з Гауссовим ядром $G(\sigma)$ для стабілізації характеристик та зменшення шуму. Цей крок є критично важливим для забезпечення стабільності навчання нейронних мереж на наступних етапах обробки.

Модуль енкодера виконує перетворення оброблених просторових даних у компактне латентне представлення. В якості архітектурної основи енкодера використовується згорткова нейронна мережа ResNet50. Енкодер E приймає на вхід згладжену карту дрібниць розмірністю $h * w * 3$ та формує латентний вектор w фіксованої розмірності 512.

Завершальний етап реалізується генератором StyleGAN2 (G). Ця модель перетворює латентний код w у послідовність стильових векторів, які модулюють процес синтезу на різних рівнях деталізації, що дозволяє досягти високої якості реконструйованих зображень.

Результатом роботи генератора є зображення відбитка пальця I у градаціях сірого $I \in \mathbb{R}^{h*w}$, де I представляє реконструйоване зображення відбитка пальця з роздільною здатністю $h * w$. Структура реалізованого методу реконструкції відбитку пальця зображена на рис. 5.

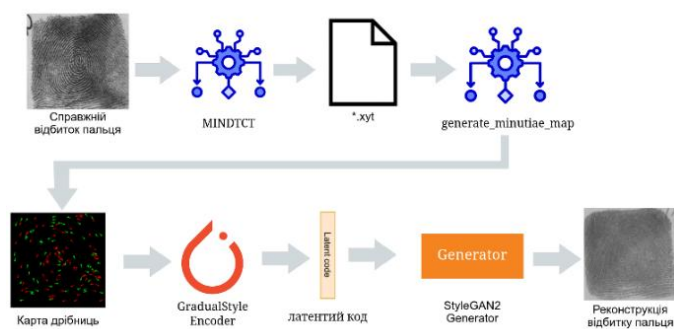


Рис. 5. Структура реалізованого методу реконструкції відбитку пальця

3.3. Оцінка ефективності

Для оцінки ефективності реалізованого методу було створено програмну реалізацію для аналізу атак. Цей сценарій передбачає, що зломисник реконструює відбитки з викрадених шаблонів і використовує їх проти тієї ж системи, з якої вони були вкрадені.

Для порівняння відбитків було інтегровано алгоритм BOZORTH3, розроблений NIST [13]. Цей алгоритм порівнює локальні структури дрібниць і працює з файлами формату .xvt.

Для проведення експериментального дослідження було використано 466 genuine відбитків пальця та зроблено 99235 impostor порівнянь. Genuine відбитки представляли справжні зразки користувачів системи, тоді як impostor порівняння включали спроби несанкціонованого доступу з використанням реконструйованих відбитків.

В основі оцінки ефективності використовується значення порогу, що є числовим значенням схожості, яке система використовує для прийняття рішення про надання доступу. Для визначення порогового значення було побудовано гістограму згідно з рис. 6. На ній зображено розподіл оцінок відповідностей для легітимних користувачів та зломисників. По горизонтальній осі відкладено числові значення оцінок схожості, а вертикальна вісь відображає частоту появи таких значень під час експерименту. Червоним кольором позначено розподіл для спроб несанкціонованого доступу. Основна маса цих значень зосереджена в області низьких показників, що свідчить про ефективне відсіювання системою більшості атак. Зеленим кольором виділено розподіл для легітимних користувачів з реконструйованих зображень, що зміщений у бік високих показників. У місці перетину цих двох графіків знаходиться порогове значення. Високий відсоток успішності атаки підтверджує, що реконструйовані відбитки долають цей бар'єр і змішуються в зону довіри, через що система помилково ідентифікує їх як легітимні.

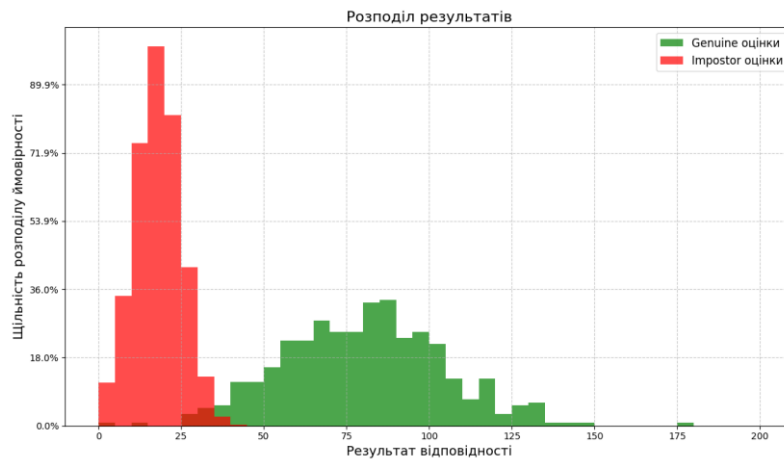


Рис. 6. Розподіл результатів відповідності відбитків пальців

Для визначення оптимального порогу обчислюється коефіцієнт хибного прийняття в діапазоні від 0 до 300 з кроком 5 $FAR(t) = \frac{\text{impostor} \geq t}{\text{total_impostor}}$, де $\text{impostor} \geq t$ є кількістю оцінок для зловмисних відбитків, які перевищують або дорівнюють порогу t , total_impostor показує загальну кількість порівнянь зловмисних відбитків. Для заданого цільового значення знаходиться оптимальний поріг за критерієм $\text{Оптимальний поріг} = \text{argmin}|FAR(t) - FAR_target|$, де FAR_target заздалегідь задані цільові рівні безпеки системи (1 %, 0.1 %, 0.01 %).

Точність верифікації показує відсоток успішних атак як частку реконструйованих відбитків, які змогли подолати відповідний поріг системи $\text{Точність} = \left(\frac{\text{кількість genuine оцінок} \geq \text{Поріг}}{\text{Загальна кількість спроб атаки}} \right) * 100$.

Результати оцінки ефективності атаки наведені в табл. 2.

Таблиця 2

FAR, %	Поріг	Точність, %
1	33	98.52
0.1	39	97.66
0.01	43	96.68

Аналіз результатів демонструє, що при зниженні допустимого рівня хибних прийняття з 1 до 0.01 %, поріг прийняття рішень зростає з 33 до 43 балів, що призводить до зменшення точності верифікації з 98.52 до 96.68 %.

В роботі проведено порівняльний аналіз успішності атаки реалізованим методом та інших розповсюджених атак на основі штучного інтелекту на системи біометричної автентифікації за відбитками пальців. Результати такого аналізу наведені у табл. 3.

Таблиця 3

Метод	Тип атаки	Успішність атаки, %	FAR, %
SpoofGAN	Синтетична генерація	99.87	FAR = 0.01
FingerFaker	Синтетична генерація	94.22	FAR = 0.01
Feng & Jain	Реконструкція	93.62	FAR = 0.01
Реалізований метод	Реконструкція	96.68	FAR = 0.01

З табл. 3 можна зробити висновок, що метод, заснований на праці Бузагло та Келлера дозволяє досягти точності розпізнавання за підробленим зразком 96.68 %. Це перевищує

показники методу реконструкції Фенга та методу синтетичної генерації. І, хоча метод SpoofGAN демонструє найвищу точність розпізнавання, реалізований підхід підтверджує критичну небезпеку, оскільки забезпечує високу ймовірність злому конкретного облікового запису.

Висновки

Проаналізовано існуючі біометричні системи автентифікації та встановлено, що автентифікація за відбитком пальця є однією з найпоширеніших технологій. Атаки на основі штучного інтелекту створюють нові виклики та необхідність впровадження додаткових механізмів захисту для біометричних систем.

Розглянуто систему біометричної автентифікації за відбитками пальців та надані основні формули для знаходження подібності двох зображень.

Зроблено порівняльний аналіз методів атак із використанням GAN, зокрема порівняно синтетичну генерацію SpoofGAN, FingerFaker та методи реконструкції відбитків з шаблонів дрібниць на основі алгоритмів Фенга і Джейна, а також Бузагло і Келлера. Встановлено, що підхід Бузагло і Келлер є одним з найперспективніших.

Проведено експериментальне дослідження атаки методом реконструкції відбитку пальця. Результати експерименту підтвердили вразливість біометричних систем автентифікації до атак реконструкції. Навіть при налаштуваннях системи безпеки, де FAR = 0.01 %, реконструйовані відбитки продемонстрували високу ефективність обходу біометричної системи автентифікації, досягнувши точності розпізнавання у 96.68 %.

Проведено порівняння оцінок ефективності розповсюджених методів атак на основі штучного інтелекту на біометричні системи автентифікації за відбитками пальців. Встановлено, що метод Бузагло і Келлера демонструє одну з найвищих ефективностей серед розглянутих підходів. Точність верифікації за цим методом варіює з 98.52 до 96.68 % в залежності від налаштувань системи.

Вважаємо, що актуальними та необхідними є подальші дослідження у сфері проведення атак на основі штучного інтелекту на системи біометричної автентифікації. Це дозволить створювати ефективні методи протидії таким атакам та підвищити рівень надійності біометричних систем автентифікації загалом.

Список літератури:

1. Методи і технології біометричної ідентифікації за результатами літературних джерел / Л. Г. Коваль та ін. // Вчені записки ТНУ ім. В.І. Вернадського. Серія: технічні науки. 2019. Т. 30 (69) Ч. 1 № 2. С. 104–111.
2. Security vulnerabilities against fingerprint biometric systems: book chapter / Sushanta Kumar Das and other // Recent Advances in Computational Intelligence Applications for Biometrics and Biomedical Devices. 2025. Chapter 4. P. 35–43.
3. Generating MasterPrints for Dictionary Attacks via Latent Variable Evolution / P. Bontrager, et al. // Conference: 2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS) IEEE BTAS. 2018. P. 1–9. DOI:10.1109/BTAS.2018.8698539.
4. Goodfellow I, Pouget-Abadie J, Mirza M, Xu B, Warde-Farley D, Ozair S, Courville A, Bengio Y. Generative adversarial networks. Commun // ACM, 2020. vol. 63, no. 11. P.139–144.
5. Ateniese G. Hacking smart machines with smarter ones: How to extract meaningful data from machine learning classifiers / G. Ateniese, G. Felici, L. V. Mancini 1 et al. // International Journal of Security and Networks. 2010. Vol. 10, Issue 3. P. 137–150.
6. Combined Adversarial Attacks for Breaking Fingerprint Presentation Attack Detectors / S. Zedda // EUSIPCO 2025: conference paper, Thu, 11 Sep. 2025, Italy, Bellini. P. 1352–1356.
7. Yu Y, Niu Q, Li X, Xue J, Liu W, Lin D. A Review of Fingerprint Sensors: Mechanism, Characteristics, and Applications. Micromachines (Basel). 2023 Jun 14;14(6):1253. doi: 10.3390/mi14061253. PMID: 37374839; PMCID: PMC10305017..
8. Maltoni D., Maio D., Jain A.K., Prabhakar S. Handbook of Fingerprint Recognition. 2nd ed. London : Springer-Verlag London Limited, 2009. 475 p.
9. S. A. Grosz, A. K. Jain. SpoofGAN: Synthetic Fingerprint Spoof Images // IEEE Transactions on Information Forensics and Security. 2023. vol. 18. P. 730–743. doi: 10.1109/TIFS.2022.3227762.

10. Shen Y., Ma Z., Lin F., Yan H., Ba Z., Lu L., Xu W., Ren K. FingerFaker: Spoofing Attack on COTS Fingerprint Recognition Without Victim's Knowledge // Proceedings of the 21st ACM Conference on Embedded Networked Sensor Systems (SenSys '23). New York : Association for Computing Machinery, 2024. P. 167–180.
11. K. Cao, A. K. Jain. Learning fingerprint reconstruction: From minutiae to image // IEEE Trans. on Information Forensics and Security. 2015. Vol. 10, no. 1. P. 104–117.
12. Bouzaglo R., & Keller Y. Synthesis and reconstruction of fingerprints using generative adversarial networks. arXiv preprint arXiv:2201.06164, 2022.
13. NIST Biometric Image Software (NBIS). nist.gov. URL: <https://www.nist.gov/services-resources/software/nist-biometric-image-software-nbis/>.

Надійшла до редколегії 20.10.2025

Відомості про авторів:

Олешко Інна Вікторівна – канд. техн. наук, Харківський національний університет радіоелектроніки, доцент кафедри безпеки інформаційних технологій, Україна; e-mail: inna.oleshko@nure.ua; ORCID: <https://orcid.org/0000-0002-8021-0467>

Луценко Владислав Ігорович – Харківський національний університет радіоелектроніки, бакалавр; Україна; e-mail: vladyslav.lutsenko1@nure.ua; ORCID: <https://orcid.org/0009-0007-0102-461X>

Петренко Ольга Євгенівна, канд. техн. наук, Харківський національний університет радіоелектроніки, доцент кафедри безпеки інформаційних технологій, Україна; e-mail: olha.petrnko@nure.ua; ORCID: <https://orcid.org/0000-0002-7862-5399>

Мельникова Оксана Анатоліївна – канд. техн. наук, Харківський національний університет радіоелектроніки, доцент кафедри безпеки інформаційних технологій, Україна; email: oksana.melnykova@nure.ua; ORCID: <https://orcid.org/0000-0001-8843-9648>

*О.І. ФЕДЮШИН, канд. техн. наук, П.В. ШУЛІК, канд. техн. наук, В.В. ПРОСОЛОВ,
Д.О. В'ЮХІН, О.В. ЧЕЧУЙ, канд. техн. наук*

ВИКОРИСТАННЯ МЕТОДІВ ГЛИБОКОГО НАВЧАННЯ ДЛЯ ВІЗУАЛІЗАЦІЇ ТА ВИЯВЛЕННЯ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Вступ

Шкідливе програмне забезпечення (Malware) залишається однією з найбільш стійких та серйозних загроз у сфері кібербезпеки. Воно постійно еволюціонує, атакуючи широкий спектр цифрових систем починаючи від традиційних настільних і мобільних платформ до новітніх пристроїв Інтернету речей [1]. Обсяги та складність сучасних кібератак невпинно зростають, що створює значні виклики для існуючих захисних механізмів.

Традиційні підходи до виявлення шкідливого програмного забезпечення (ШПЗ), які здебільшого покладаються на сигнатурний аналіз, демонструють дедалі нижчу ефективність. Їхня проблема полягає у нездатності виявляти нові та невідомі загрози. Сучасні зловмисники широко використовують техніки обфускації (заплутування коду), а також поліморфні та метаморфні механізми [2]. Ці методи дозволяють шкідливому ПЗ змінювати свою структуру у кожній новій ітерації, зберігаючи при цьому свою шкідливу поведінку. Як наслідок, сигнатурний аналіз, що шукає точні збіги у коді, стає практично марним проти нових загроз.

З великим обсягом даних, які генеруються кожної секунди, важливо мати ефективні методи для автоматичного виявлення шкідливих програм серед цього потоку інформації. Глибоке навчання (Deep Learning, DL) [3] може допомогти автоматизувати процес виявлення шкідливих програм та відфільтрувати їх з великої кількості даних. Моделі DL здатні вивчати складні, приховані закономірності у даних, що дозволяє їм ідентифікувати шкідливу поведінку навіть у раніше невідомих зразках.

Одним з найбільш перспективних напрямків став підхід, що поєднує кібербезпеку та комп'ютерний зір [1]. Суть методу полягає у візуалізації шкідливого ПЗ: бінарний код виконувального файлу (наприклад, PE-файлу) конвертується у графічне зображення, наприклад, у відтінках сірого [2]. Це дозволяє трактувати задачу класифікації шкідливого ПЗ як задачу класифікації зображень. Такий підхід відкриває можливість застосування потужних архітектур згорткових нейронних мереж (CNN), які домінують у сфері аналізу візуальних даних. Дослідники активно порівнюють ефективність різних архітектур CNN, а також новітніх моделей, таких як Vision Transformers (ViT) [4], та розробляють гібридні системи, що поєднують аналіз зображень (статичні ознаки) з аналізом поведінкових патернів, наприклад, послідовностей викликів API (динамічні ознаки) [5].

Незважаючи на значний прогрес, питання вибору оптимальної архітектури CNN для задачі класифікації візуалізованого шкідливого ПЗ залишається відкритим, оскільки різні моделі мають різну обчислювальну складність та ефективність у виявленні тонких текстурних відмінностей у зображеннях.

Метою даного дослідження є проведення детального порівняльного аналізу ефективності низки поширених архітектур згорткових нейронних мереж (зокрема, DenseNet169, EfficientNetB0, InceptionV3, MobileNetV2, ResNetV2, VGG16 та XceptionNet) для задачі класифікації сімейств ШПЗ на основі його попередньої візуалізації.

Об'єктом дослідження є процес класифікації ШПЗ на основі методів глибокого навчання та візуалізації даних.

Предметом дослідження є порівняльний аналіз ефективності та результативності (точність, повнота, F1-score) обраних архітектур згорткових нейронних мереж при класифікації зображень шкідливого ПЗ.

В якості концептуальної основи для дослідження запропоновано обрати методи та моделі з використанням Transfer Learning. Це дозволяє виявляти атаки на ранніх стадіях. На їх основі побудована класифікаційна модель та проведено її тестування.

Використання нейронних мереж та методів комп'ютерного зору для аналізу Malware

Зловмисники постійно вдосконалюють свої атаки, і PE-файли залишаються одними з основних векторів розповсюдження шкідливого програмного забезпечення. Розуміння та аналіз цих файлів є важливим для виявлення і нових загроз.

Формат PE використовується в операційних системах Windows для збереження виконуваних файлів і бібліотек. Зловмисники часто маскують свої віруси і троянці, змінюючи PE-файли, і дослідження цього формату дозволяє виявляти такі зміни. Частіше за все аналіз включає в себе аналіз імпортів, секцій, реєстрації, підписів і багато іншого і може використовувати різні методи, наприклад, такі як статичний аналіз, динамічний аналіз, емуляція та дешифрування шкідливого коду. Ці методи дозволяють отримувати більше інформації про загрози. У розробників зловмисного програмного забезпечення стало звичайною практикою використовувати кілька методів обфускації за допомогою метаморфічних та поліморфних методів для створення варіантів існуючого сімейства зловмисних програм, щоб уникнути їх швидкого виявлення. Ці методи дозволяють змінювати бінарний код шкідливого ПЗ при кожному новому зараженні, роблячи неможливим його виявлення за допомогою заздалегідь відомих, статичних сигнатур (хеш-сум).

Одна із технік, яка запропонована сучасними дослідниками для детектування Malware, полягає у візуалізації бінарного коду виконуваних файлів (PE, ELF тощо), і подальшому його аналізі на основі нейронних мереж. Процес візуалізації зазвичай включає наступні кроки: зчитування байтів, трансформацію у 2D уявлення і формування кінцевого зображення. При цьому бінарний файл читається як одновимірний потік байтів (значення від 0 до 255), потім перетворюється на двовимірну матрицю пікселів. Фінальна матриця зберігається як зображення у відтінках сірого (grayscale), де кожне значення байта відповідає яскравості пікселя.

Ця трансформація виявилася надзвичайно ефективною, оскільки програми, що належать до однієї родини шкідливого ПЗ, часто мають схожі структури коду. Навіть після обфускації, ці структури призводять до схожих візуальних текстур та патернів на зображеннях, які людське око може не розпізнати, але які легко "влловлюються" нейронними мережами.

Після перетворення файлів у зображення задача виявлення шкідливого ПЗ стає задачею класифікації зображень. Тут на перше місце виходять згорткові нейронні мережі, які є золотим стандартом у комп'ютерному зорі.

Архітектура CNN характеризується наявністю згорткових шарів, шарів об'єднання та повністю зв'язаних шарів (рис. 1).

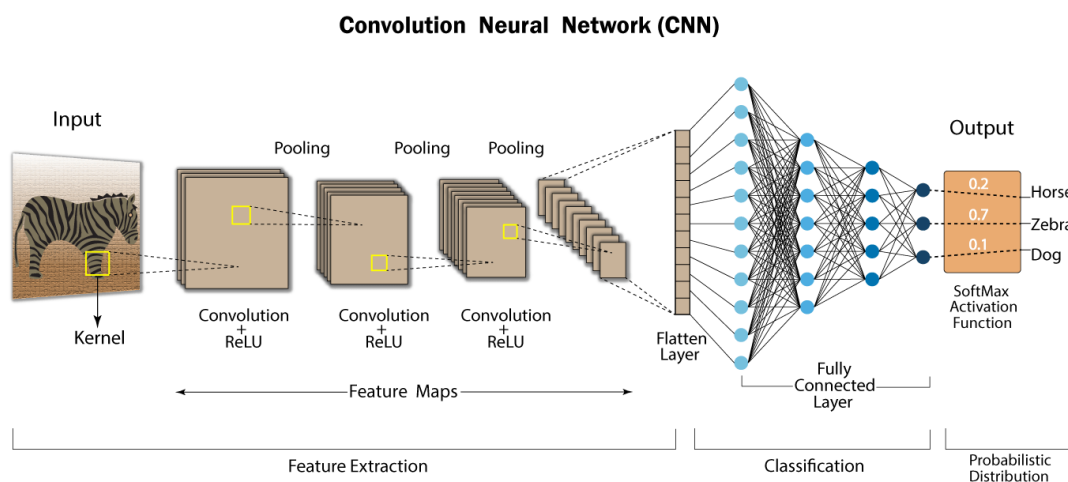


Рис. 1. Базова архітектура CNN

Ключові переваги CNN у цій задачі: автоматичне виділення ознак, ієрархічне навчання, стійкість до зсувів, універсальність. На відміну від традиційного машинного навчання CNN не потребують ручного "конструювання ознак" (feature engineering). Їхні згорткові фільтри автоматично навчаються виявляти релевантні візуальні патерни (текстури), що відповідають шкідливим фрагментам коду. Глибокі шари мережі вчаться розпізнавати все складніші патерни, комбінуючи простіші, виявлені на попередніх шарах. Завдяки механізмам згортки моделі стійкі до того, де саме у файлі (і, відповідно, на зображенні) знаходиться шкідливий патерн. Універсальність полягає в тому, що цей метод не залежить від конкретної архітектури процесора чи операційної системи, оскільки він аналізує лише сирий бінарний потік.

Навчання глибоких CNN (таких як, VGG, ResNet, Inception, XceptionNet) "з нуля" вимагає величезних наборів даних та обчислювальних потужностей. У сфері кібербезпеки домінуючим підходом стало використання трансферного навчання [4].

Підхід полягає у використанні моделей, що вже були навчені на мільйонах загальних зображень (наприклад, з набору даних ImageNet). Виявляється, що базові фільтри, які ці моделі вивчили (детектори кутів, градієнтів, текстур), є універсальними. Вони ефективно "бачать" текстури і в зображеннях шкідливого ПЗ, що дозволяє: 1) використати потужні, перевірені архітектури; 2) значно скоротити час навчання та обсяг даних; 3) досягти дуже високих показників точності (часто понад 98–99 %).

Найпоширенішим втіленням трансферного навчання в контексті глибинного навчання є наступний робочий процес (рис. 2):

- взяття шарів з попередньо навченої моделі;
- їх замороження, щоб уникнути знищення будь-якої інформації, яка в них міститься, під час майбутніх тренувань;
- додавання нових тренувальних шарів поверх заморожених шарів. Вони навчаються перетворювати старі функції на прогнози на новому наборі даних;
- навчання нових шарів на вашому наборі даних.

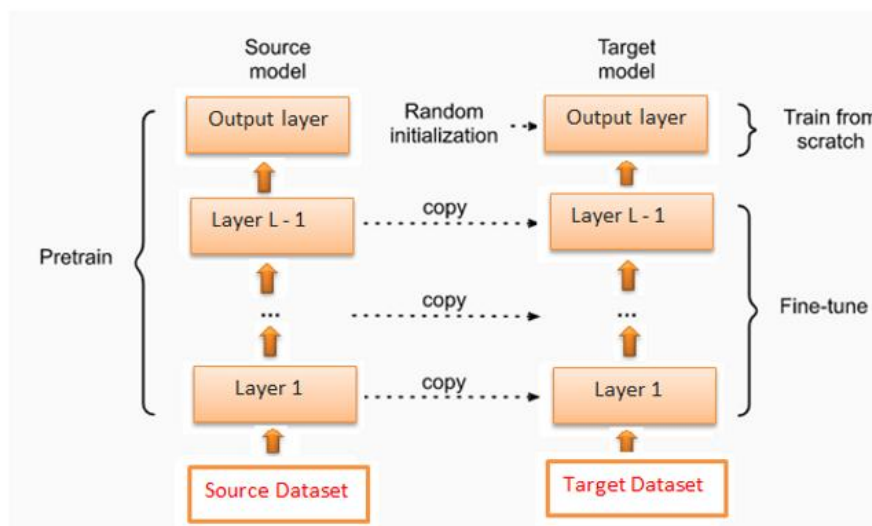


Рис. 2. Ілюстрація процесу Transfer Learning

Останнім необов'язковим кроком є тонке налаштування, яке складається з розморожування всієї моделі, отриманої вище (або її частини), і повторного навчання на нових даних із дуже низькою швидкістю навчання. Як результат – можна досягти значних покращень шляхом поступової адаптації попередньо навчених функцій до нових даних.

Найбільшим викликом для всіх методів глибокого навчання є їхня непрозорість. Модель може з 99 % точністю сказати, що файл є шкідливим, але не може пояснити чому. Це створює попит на методи пояснювального штучного інтелекту (Explainable AI, XAI), такі як

Grad-CAM, які можуть візуалізувати, на які "частини" зображення програмного коду модель звернула увагу при ухваленні рішення [3].

Для оцінки ефективності детектування елементів ШПЗ було обрано та проаналізовано сім відомих архітектур згорткових нейронних мереж: DenseNet169, EfficientNetB0, InceptionV3, MobileNetV2, ResNetV2, VGG16 та XceptionNet. Для кожної архітектури базові згорткові шари були "заморожені" (або частково розморожені), а верхні шари класифікатора були замінені новими, адаптованими до кількості класів у нашому наборі даних.

DenseNet169 [6] – це архітектура згорткової нейронної мережі, яка належить до сімейства щільно зв'язаних згорткових мереж (DenseNets).

Ключовою інновацією DenseNet є щільна схема з'єднання. На відміну від традиційних згорткових нейронних мереж, де кожен шар пов'язаний лише з сусідніми шарами, DenseNet з'єднує кожен шар із кожним іншим у прямому зв'язку. Цей щільний зв'язок досягається шляхом об'єднання карт функцій усіх попередніх шарів як входів до поточного шару. Ця конструкція має кілька переваг, включаючи покращене повторне використання функцій, градієнтний потік і ефективність параметрів.

Мережа VGG16 [7] складається з малих згорткових фільтрів. VGG16 має три повністю зв'язані шари та 13 згорткових шарів. У неї проста, глибока архітектура. Слугує чудовим базовим рівнем (baseline). Вхідними даними для будь-якої мережевої конфігурації вважається зображення фіксованого розміру 224 x 224 із трьома каналами – R, G і B. Єдина виконана попередня обробка – нормалізація значень RGB для кожного пікселя. Це досягається шляхом віднімання середнього значення від кожного пікселя.

ResNetV2 [8] використовує "залишкові з'єднання" (residual connections), що дозволяє навчати надзвичайно глибокі мережі без втрати градієнта. Ідеально для виявлення дуже складних, ледь помітних патернів.

InceptionV3/XceptionNet [9] мають як ключову ідею "багатомасштабний аналіз" (рис. 3). Вони одночасно застосовують фільтри різного розміру (1x1, 3x3, 5x5), що дозволяє їм бачити і дрібні, і великі патерни одночасно. Це може бути критично важливим, оскільки шкідливий код може бути як короткою інструкцією (дрібний патерн), так і цілим вбудованим блоком (великий патерн).

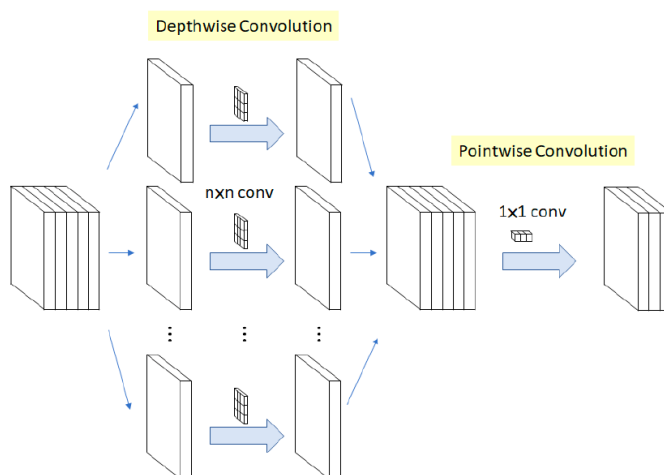


Рис. 3. Архітектура XceptionNet

MobileNetV2/EfficientNetB0 являють собою "ефективні" архітектури. Вони розроблені для досягнення максимальної точності при мінімальних обчислювальних витратах. Їх аналіз важливий для практичного застосування, бо така модель могла б працювати навіть на мобільному пристрої або в антивірусному сканері реального часу без значного навантаження на систему.

Експериментальні дослідження та метрики оцінки

З метою оцінки ефективності виявлення різними CNN ШПЗ через бінарні файли було обрано набір даних зловмисного програмного забезпечення MaleVis [10]. Він містить 14226 зображень зловмисного програмного забезпечення, що охоплює 25 класів, а також 1 клас звичайного програмного забезпечення. З набору даних було використано всі 26 класів і 7280 зображень додатково відібрано з цих класів з метою навчання. Для цілей тестування (5126 зображень) та валідації (1820 зображень) було відібрано 6946 зображень із всіх класів. Зображення в наборі даних MaleVis були отримані шляхом вилучення бінарних зображень із файлів шкідливих програм у 3-канальному форматі RGB. Потім розміри зображень змінювалися до роздільної здатності квадратів 224x224.

Ключовим етапом дослідження, що передував навчанню моделей, було перетворення виконуваних PE-файлів у графічні зображення. Для цього завдання було обрано Python-скрипт Bin2png [11], здатний без втрат конвертувати бінарні дані у формат PNG.

Процес генерації зображень мав два етапи:

1) Конвертація. За допомогою адаптованого скрипту вся колекція бінарних файлів з набору даних була перетворена на PNG-зображення. На цьому етапі встановлювалася фіксована ширина (224 або 300 пікселів), що призводило до генерації зображень з різною висотою, яка залежала від розміру вихідного файлу.

2) Масштабування (стандартизація). Оскільки архітектури згорткових нейронних мереж вимагають на вході зображення фіксованого розміру, усі отримані PNG-файли були стандартизовані. Їх було приведено до квадратних розмірів 224x224 та 300x300 пікселів.

Для мінімізації втрат інформації та артефактів під час масштабування обрано метод інтерполяції Ланцоша. Цей метод, реалізований у бібліотеці OpenCV, аналізує розширений набір пікселів (8x8) і забезпечує високу якість зображення у порівнянні з простішими методами (наприклад, білінійною інтерполяцією).

Для навчання та оцінки моделей було використано пропорції поділу оригінального набору даних Malevis. Загальний набір даних був розділений на дві основні частини: 1) тестувальний набір: 36 % від усіх даних; 2) набір для навчання та валідації: 64 % від усіх даних. Особливістю даної роботи було те, що оригінальний 64 %-й набір був додатково розділений для створення окремого валідаційного набору. Цей набір є критично необхідним для моніторингу перенавчання моделі в процесі тренування.

Поділ 64 %-го набору проводився у пропорції 4:1 (тобто, 80 % даних для навчання та 20 % – для валідації). Таким чином, фінальний розподіл усього набору даних виглядає так: 1) тренувальний набір: 51.2 % (80 % від 64 %); 2) валідаційний набір: 12.8 % (20 % від 64 %); 3) тестувальний набір: 36 % (збережено з оригінального поділу).

Такий підхід дозволив одночасно виділити дані для валідації, не порушуючи при цьому цілісність оригінального тестового набору, що забезпечує об'єктивність та порівнянність результатів.

В табл. 1 представлено дані щодо класів зловмисного ПЗ і їх кількості (в тому числі відношення кількості тренувальних і тестувальних даних). На рис. 4 наведено приклади зображень представників різних видів зловмисного ПЗ.

В якості додаткових інструментів для роботи з датасетом, навчання моделей та оцінки метрик ефективності було обрано TensorFlow, Matplotlib та Seaborn. TensorFlow надає повний набір інструментів, бібліотек і ресурсів спільноти, які полегшують дослідникам і розробникам впровадження та розгортання моделей машинного навчання. Matplotlib та Seaborn будуть використані для візуалізації даних та статистичної обробки.

Після підготовки набору даних (конвертації файлів у зображення та їх стандартизації) ми розробили єдиний алгоритм для навчання кожної з обраних нейронних мереж. Цей процес, проілюстрований на блок-схемі (рис. 5), використовує поширений та ефективний підхід трансферного навчання (transfer learning).

Таблиця 1

Номер	Назва	Клас	Тренувальні/Тестувальні/ Валідаційні дані
1	Adposhel	Adware	280/144/70
2	Agent-fyi	Trojan	280/120/70
3	Akorfn	Ransomware	280/146/70
4	Allaple	Worm	280/128/70
5	Amonetize	Adware	280/147/70
6	Androm	Backdoor	280/150/70
7	AutoRun-PU	Worm	280/146/70
8	BrowseFox	Adware	280/143/70
9	CVEap	Ransomware	280/149/70
10	Dinwod!rfn	Trojan	280/149/70
11	DoejoCrypt	Ransomware	280/135/70
12	Elex	Trojan	280/150/70
13	Expiro-H	Virus	280/151/70
14	Fasong	Worm	280/150/70
15	Hlux!IK	Worm	280/150/70
16	Injector	Trojan	280/145/70
17	InstallCore.C	Adware	280/150/70
18	MultiPlug	Adware	280/149/70
19	Neoreklami	Adware	280/150/70
20	Neshta	Virus	280/147/70
21	Goodware	Not a Malware	280/1482/70
22	Salaty	Virus	280/149/70
23	Snarasite.D!tr	Trojan	280/150/70
24	Stantinko	Backdoor	280/150/70
25	VBKrypt	Trojan	280/150/70
26	Vilssel	Trojan	280/146/70

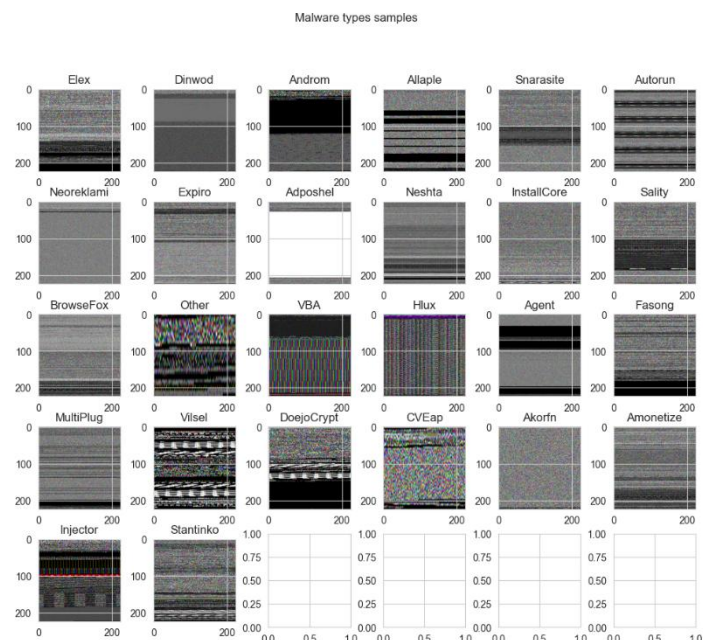


Рис. 4. Приклад графічних представлень кожного з класів ШПЗ в датасеті

Ми не будували нейронну мережу "з нуля", а брали потужні, вже навчені моделі (як VGG16, ResNet та ін.) і "перекваліфіковували" їх для нашого конкретного завдання розпізнавання зображень шкідливого ПЗ.

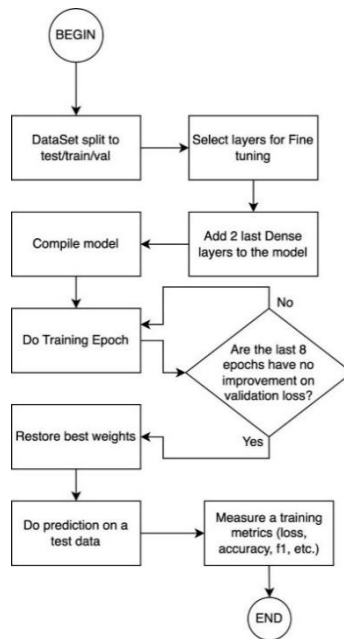


Рис. 5. Блок-схема алгоритму тренування нейронної мережі

Основні кроки проведення експерименту [12].

К р о к 1. Підготовка даних. Весь наш набір зображень був розділений на дві ключові групи:

- набір для навчання та валідації (64 %). Ці дані використовувалися для самого процесу "навчання". Модель використовувала їх, щоб знайти закономірності (тренування), а ми періодично перевіряли її успішність на частині цих даних (валідація);
- тестовий набір (36 %). Ці дані модель ніколи не бачила під час навчання. Вони були "відкладені" для фінального, об'єктивного тестування.

К р о к 2. Адаптація архітектури (трансферне навчання). Для кожної з моделей ми виконали "тонке налаштування":

1) "Заморозка" шарів. Ми припустили, що перші шари нейронної мережі (наприклад, перші 100) вже чудово навчені розпізнавати базові речі (лінії, кути, прості текстури) завдяки їх навчанню на мільйонах інших зображень. Ми "заморозили" їхні ваги, заборонивши їм змінюватися.

2) "Розморозка" шарів. Ми дозволили до-навчання лише для більш глибоких шарів (усіх, що йдуть після 100-го). Це дало змогу мережі адаптувати свої знання про складні патерни до специфіки наших зображень ШПЗ.

3) Встановлення нового "класифікатора". Ми "відрізали" оригінальний вихідний шар моделі (який міг розпізнавати, наприклад, 1000 класів типу "кіт", "собака", "автомобіль") і додали замість нього два нових щільно зв'язаних (Dense) шари:

- прихований шар (1000 нейронів) як проміжний, що допомагає моделі агрегувати вивчені ознаки;
- вихідний шар (26 нейронів) як кінцевий шар, де кожен нейрон відповідає одному з 26 класів шкідливого ПЗ у нашому датасеті.

К р о к 3. Процес тренування та компіляції.

Після адаптації модель була скомпільована (підготовлена до навчання) та запущена. Ключовою особливістю був механізм "ранньої зупинки" (Early Stopping), який допоміг нам заощадити час та уникнути перенавчання (ситуації, коли модель просто "зазубрює" тренувальні дані, але погано працює на нових).

Ось як він працював:

- модель тренувалася циклами (епохами);

- встановили "терпіння" (patience) у 8 епох;
- після кожної епохи модель перевіряла свою ефективність (значення функції втрат) на валідаційних даних;
- якщо протягом 8 епох поспіль модель не показувала покращення (не встановлювала новий "рекорд" ефективності), навчання автоматично зупинялося;
- після зупинки система автоматично відновлювала ваги моделі з тієї епохи, яка була найкращою.

Встановлено максимальну межу у 80 епох, але завдяки цьому розумному механізму жодній з наших моделей не знадобилося більше 25 епох, щоб досягти свого піку ефективності.

К р о к 4. Фінальна оцінка.

Після того, як навчання було завершено і ми отримали найкращу версію кожної моделі, настав час тестування. Ми взяли тестовий набір (36 % даних, які модель ніколи не бачила) і попросили моделі зробити на ньому прогнози.

Далі порівняли ці прогнози з реальними, правильними відповідями і розрахували матрицю невідповідностей (візуальну таблицю, що показує, які класи модель плутала між собою) і ключові метрики Precision, Recall та F1-Score, щоб об'єктивно оцінити точність кожної моделі.

Після навчання всіх 7 нейронних мереж ми оцінили їхню ефективність. Для цього ми використали стандартні метрики: Accuracy (загальна точність), Precision (точність прогнозів), Recall (повнота виявлення) та F1-Score (збалансований показник).

Щоб отримати узагальнені бали (табл. 2) ми використали «зважений» підхід. Це означає, що точність у класі, де було 1000 тестових файлів, мала більшу «вагу» для загальної оцінки, ніж у класі, де було лише 100 файлів. Це робить оцінку більш справедливою та об'єктивною, особливо коли класи нерівномірні.

Таблиця 2

Нейронна мережа	Precision	Recall	F1	Accuracy
XceptionNet	0.89	0.86	0.86	0.86
EfficientNetB0	0.90	0.85	0.86	0.85
MobileNetV2	0.90	0.85	0.86	0.85
DenseNet169	0.90	0.86	0.86	0.86
InceptionV3	0.89	0.83	0.85	0.83
VGG16	0.88	0.82	0.82	0.82
ResNet50V2	0.88	0.83	0.83	0.83

Як видно з табл. 2, усі моделі показали досить високі та схожі результати. По показнику Precision найкращий бал (0.90) у EfficientNetB0, MobileNetV2 та DenseNet169. Це означає, що якщо ці моделі казали "Це вірус!", вони мали рацію у 90 % випадків. По показниках Recall та Accuracy найкращий бал (0.86) у XceptionNet та DenseNet169. Це означає, що вони змогли правильно детектувати та класифікувати 86 % усіх файлів у тестовій вибірці.

За суто чистими балами DenseNet169 та XceptionNet виглядають лідерами. Але висока точність не основний показник. Нам також важлива ефективність моделі. DenseNet169 "легша" бо має 14 мільйонів параметрів (умовних "налаштувань"), тоді як XceptionNet має 27 мільйонів. Але під час нашого експерименту ми "до-навчали" 69 шарів у DenseNet169, і лише 32 – у XceptionNet. Через це один цикл (епоха) навчання у DenseNet169 тривав у 1.5 рази довше. Найважливіше, що XceptionNet досягла свого найкращого результату всього за 7 епох, тоді як DenseNet169 знадобилося 13 епох.

Висновок: хоча обидві моделі точні, XceptionNet виявилася більш перспективною. Вона вчиться набагато швидше і вимагає менше циклів навчання для досягнення пікової ефективності. Ми детально проаналізували, де саме помилялася наша найкраща модель XceptionNet.

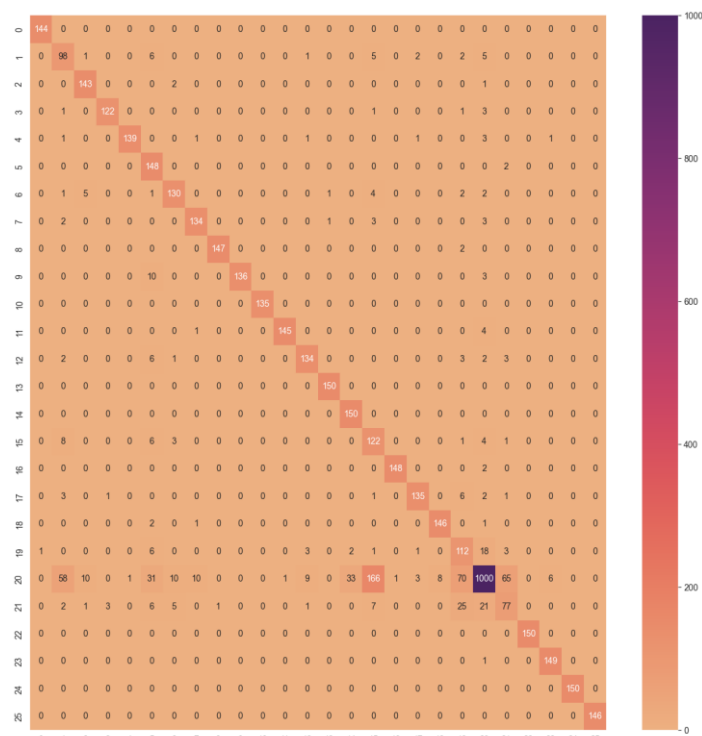


Рис. 6. Матриця невідповідностей для XceptionNet

Матриця невідповідностей (рис. 6) показала кілька цікавих речей. Найбільше помилок модель робила з класом "Goodware" (безпечні файли). Вона часто плутала їх з вірусами. Це очікувано, оскільки у нас було в 10 разів більше безпечних файлів, ніж будь-якого іншого класу шкідливого ПЗ. Найпроблемніший вірус "Injector" (Клас 16). Модель найчастіше плутала цей тип трояна з безпечними файлами. Це може свідчити про те, що його візуальні патерни дуже "хаотичні" або схожі на звичайні програми. Деякі класи, наприклад, "Snarasite.D!tr", "DoejoCrypt" та "Vilsel", модель розпізнавала зі 100 % точністю. Їхні візуальні патерни виявилися дуже унікальними та легко впізнаваними.

Висновки

Традиційні антивіруси здебільшого покладаються на сигнатурний аналіз. Вони шукають у файлах унікальні "цифрові відбитки" (сигнатури) вже відомих вірусів. Цей підхід став на практиці мало ефективним через масове використання зловмисниками технік поліморфізму та обфускації. Після перетворення бінарних файлів у зображення задача виявлення шкідливого ПЗ може бути перекваліфікована в задачу класифікації зображень.

У ході дослідження успішно вирішено актуальну задачу класифікації шкідливого програмного забезпечення за допомогою методів глибокого навчання, застосованих до візуальних представлень виконуваних PE-файлів.

Було сформовано збалансований набір даних, що включав різні сімейства шкідливого ПЗ та "чисті" файли (Goodware) і проведено порівняльний експериментальний аналіз семи поширених архітектур згорткових нейронних мереж, які навчалися за методологією трансферного навчання. Ключовим етапом роботи стала конвертація цих файлів у зображення у відтінках сірого за допомогою адаптованого скрипту Bin2png.

Експерименти засвідчили, що класифікація шкідливого ПЗ за його графічним образом є високоточним підходом, який не поступається іншим сучасним методам статичного аналізу. Моделі XceptionNet та DenseNet169 продемонстрували найкращі узагальнені показники, досягнувши ідентичної фінальної точності (Accuracy) у 86 %. Попри однакову точність глибший аналіз показав, що XceptionNet є більш перспективною. Вона досягла свого пікового результату всього за 7 епох навчання, тоді як DenseNet169 знадобилося 13. Це свідчить про

вищу ефективність та швидкість адаптації архітектури XceptionNet до даної специфічної задачі. Практичне значення роботи полягає в тому, що розроблений підхід може бути інтегрований у сучасні антивірусні програмні комплекси. Він здатен слугувати потужним модулем статичного аналізу для виявлення нових та поліморфних загроз, які ефективно обходять традиційні сигнатурні сканери.

Список літератури:

1. Brosolo M. et al. Security through the Eyes of AI: How Visualization is Shaping Malware Detection. (2025). arXiv:2505.07574v4. Available: <https://doi.org/10.48550/arXiv.2505.07574>.
2. Shah Nawaz M. et al. Dynamic Malware Classification of Windows PE Files using CNNs and Greyscale Images Derived from Runtime API Call Argument Conversion. arXiv:2505.24231v1. (2025). Available: <https://doi.org/10.48550/arXiv.2505.24231>.
3. Bensaoud A. et al. A Survey of Malware Detection Using Deep Learning. (2024). arXiv:2407.19153v1. Available: <https://doi.org/10.48550/arXiv.2407.19153>.
4. Ashawa M., Owoh N., Hosseinzadeh S., & Osamor J. Enhanced Image-Based Malware Classification Using Transformer-Based Convolutional Neural Networks (CNNs) // Electronics. 2024. Vol. 13(20). P. 4081. Available: <https://doi.org/10.3390/electronics13204081>.
5. Kim H. & Kim M. Malware Detection and Classification System Based on CNN-BiLSTM // Electronics. 2024. Vol. 13. P. 2539. Available: <https://doi.org/10.3390/electronics13132539>.
6. Huang G., Liu Z., Van Der Maaten L. and Weinberger K. Q. Densely Connected Convolutional Networks // 2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Honolulu, HI, USA, 2017. P. 2261–2269. Available: doi: 10.1109/CVPR.2017.243.
7. Simonyan K., & Zisserman A. Very Deep Convolutional Networks for Large-Scale Image Recognition // Proceedings of the 3rd International Conference on Learning Representations (ICLR). (2015). Available: <https://doi.org/10.48550/arXiv.1409.1556>.
8. He K., Zhang X., Ren S., & Sun J. Identity Mappings in Deep Residual Networks // Proceedings of the European Conference on Computer Vision (ECCV). (2016). Available: <https://doi.org/10.48550/arXiv.1603.05027>.
9. Chollet F. Xception: Deep Learning with Depthwise Separable Convolutions // 2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Honolulu, HI, USA. 2017. P. 1800–1807. [Online]. Available: doi: 10.1109/CVPR.2017.195.
10. MaleVis Dataset Home Page. Режим доступу: <https://web.cs.hacettepe.edu.tr/~selman/malevis/>.
11. GitHub – ESultanik/bin2png: A simple cross-platform script for encoding any binary file into a lossless PNG. GitHub. Режим доступу: <https://github.com/ESultanik/bin2png>.
12. Федюшин О. І., Хижняк К. М. CNN та їх використання для класифікації MALWARE // Матеріали Одинадцятої міжнар. наук.-техн. конф. «Проблеми інформатизації», Харків, 16–17 листопада 2023 р. С. 49.

Надійшла до редколегії 04.10.2025

Відомості про авторів:

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

Шулік Павло Вікторович – канд. техн. наук, Харківський національний університет радіоелектроніки, ст. викладач кафедри безпеки інформаційних технологій, факультет комп'ютерної інженерії та управління, Україна; e-mail: pavlo.shulik@nure.ua; ORCID: <https://orcid.org/0009-0004-6200-2172>

Просолов Владислав Валерійович – Харківський національний університет радіоелектроніки, аспірант кафедри безпеки інформаційних технологій, Україна; e-mail: vladyslav.prosolov@nure.ua; ORCID: <https://orcid.org/0009-0002-1276-4828>

В'юхін Даніїл Олександрович – Харківський національний університет радіоелектроніки, ст. викладач кафедри безпеки інформаційних технологій, факультет комп'ютерної інженерії та управління, Україна; e-mail: daniil.viukhin@nure.ua; ORCID: <https://orcid.org/0009-0009-8442-9587>

Чечуй Олександр Вікторович – канд. техн. наук, доцент, Харківський національний університет Повітряних Сил імені Івана Кожедуба, доцент кафедри радіоелектронних систем пунктів управління Повітряних Сил, Україна; e-mail: alche1972@ukr.net; ORCID: <https://orcid.org/0000-0002-7584-4457>

А.А. ТЕЛЬНОВА, Т.О. ГРИНЕНКО, канд. техн. наук, О.П. НАРЄЖНИЙ, канд. техн. наук

АНАЛІЗ СТІЙКОСТІ АЛГОРИТМІВ ПОСТКВАНТОВОГО ЦИФРОВОГО ПІДПISY FULEECA, WAVE, BISCUIT TA RYDE

Вступ

Алгоритми постквантового цифрового підпису (PQDS, Post-Quantum Digital Signature) розробляються як альтернатива класичним схемам, що здатна забезпечити криптографічну безпеку навіть за умови наявності квантових обчислювальних потужностей. Процес розробки та впровадження криптографічних алгоритмів цифрового підпису в умовах загрози квантових атак є актуальним питанням. У світовій практиці цим питанням займається Національний інститут стандартів і технологій (NIST). У грудні 2016 р. NIST ініціював відкритий конкурс на стандартизацію постквантових алгоритмів з відкритим ключем – Post-Quantum Cryptography Standardization Process (PQC) [1]. Метою цього конкурсу стало визначення алгоритмів, які могли б замінити існуючі стандарти у світі, де квантові комп'ютери становитимуть реальну загрозу. У вересні 2022 р. NIST оголосив четвертий раунд конкурсу на додаткові пропозиції щодо цифрових підписів, які будуть розглянуті в рамках процесу стандартизації PQC. NIST був зацікавлений, в першу чергу, в додаткових схемах підпису загального призначення, які не базуються на структурованих алгебраїчних решітках, однак також був відкритий і для отримання додаткових пропозицій на основі структурованих алгебраїчних решіток, які б значно перевершували CRYSTALS-Dilithium і FALCON у відповідних критеріях і забезпечували суттєві властивості безпеки [1].

Огляд літературних джерел свідчить про зростаючу увагу світової наукової спільноти до проблематики постквантової криптографії, особливо в аспекті цифрових підписів. У роботах Лео Дюкаса, Томаса Преста, Джеффрі Гоффстейна та інших розглядаються фундаментальні принципи побудови постквантових алгоритмів, заснованих на алгебраїчних решітках, кодах, багатосторонніх рівняннях та геш-функціях. Значну частину публікацій присвячено аналізу алгоритмів, які вийшли до фінальних етапів конкурсу NIST, таких як CRYSTALS-Dilithium, FALCON, SPHINCS+, тоді як розгляд менш відомих, але потенційно перспективних схем – Wave, RYDE, FuLeeca, Biscuit – часто обмежується суто математичними аспектами або первинними криптоаналітичними результатами.

Водночас систематизованих досліджень, які б поєднували криптостійкість, ефективність, реалізаційну придатність і технічні характеристики зазначених алгоритмів у порівняльному форматі, наразі обмаль. У доступній літературі відчутною є нестача узагальнень щодо практичного впровадження цих рішень у реальні інформаційні системи з урахуванням апаратних та програмних обмежень. Отже, попри наявність ґрунтовної математичної бази, проблема вибору оптимального постквантового алгоритму цифрового підпису для конкретних умов залишається відкритою та актуальною.

Мета статті – аналіз та дослідження теоретичних і прикладних аспектів функціонування алгоритмів цифрового підпису FuLeeca, Biscuit, Wave та RYDE, що є учасниками конкурсу NIST; аналіз структури побудови, стійкості та вразливостей алгоритмів, з урахуванням актуальних криптоаналітичних досліджень, що стосуються кожного з алгоритмів.

1. Постквантові алгоритми цифрового підпису

До чинних стандартів і тих, які зараз перебувають у процесі розробки, можна віднести CRYSTALS-DILITHIUM і SPHINCS+, які в серпні 2024 р. увійшли до стандартів FIPS 204 і FIPS 205, а також FALCON, який має увійти до стандарту FIPS 206. Також варто віднести ETSI TR 103 619 – технічний звіт, що містить рекомендації щодо постквантової криптографії й ETSI TS 103 744 – технічні специфікації щодо постквантових алгоритмів для застосування в різних галузях.

Постквантові цифрові підписи базуються на складних математичних задачах, які вважаються стійкими до атак квантових комп'ютерів. Найбільш поширеними класами задач, що лежать в основі PQDS, є:

- криптосистеми на алгебраїчних решітках (Lattice-based Cryptography): криптосистеми використовують складні задачі на алгебраїчних решітках, наприклад, алгоритми NTRU, BLISS, Falcon та Dilithium;
- кодові криптосистеми (Code-based Cryptography): криптосистеми базуються на складності декодування випадкових лінійних кодів, наприклад, алгоритм McEliece та Niederreiter;
- багатосторонні криптосистеми (Multivariate Quadratic Equations): криптосистеми використовують складність розв'язування систем багатосторонніх квадратичних рівнянь, як-то проблема факторизації многочленів або задача ізогеній еліптичних кривих. До таких алгоритмів відносяться Rainbow та UOV (Unbalanced Oil and Vinegar);
- геш-стійкі криптосистеми (Hash-based Cryptography): криптосистеми, що використовують криптографічні геш-функції для побудови підписів, наприклад, алгоритми XMSS (eXtended Merkle Signature Scheme) та SPHINCS+;
- еліптичні криві: деякі методи залучають еліптичні криві для постквантових схем [2].

Після оголошення у вересні 2022 р. четвертого раунду конкурсу на додаткові пропозиції щодо цифрових підписів, які будуть розглянуті в рамках процесу стандартизації PQC, NIST отримав 50 заявок, 40 з яких були визнані повними та належними відповідно до вимог.

Серед 40 заявок, що були допущені до подальшого конкурсу, можна виділити наступні категорії згідно з проблемами, які лежать в основі алгоритмів:

- алгоритми на основі кодів: CROSS, Enhanced pqsigRM, FuLeeca, LESS, MEDS і Wave;
- алгоритми на основі ізогеній: SQIsign;
- алгоритми на основі алгебраїчних решіток: EagleSign, EHTv3 і EHTv4, HAETAE, HAWK, HuFu, Raccoon та SQUIRRELS;
- алгоритми на основі багатосторонніх обчислень (MPC): Biscuit, MIRA, MiRitH, MQOM, PERK, RYDE й SDitH;
- алгоритми на основі багатомірності: 3WISE, DME-Sign, HPPC, MAYO, PROV, QR-UOV, SNOVA, TUOV, UOV і VOX;
- алгоритми на основі симетричних підписів: AIMer, Ascon-Sign, FAEST, а також SPHINCS-alpha;
- інші алгоритми: ALTEQ, eMLE-Sig 2.0, KAZ-SIGN, Preon і Xifrat1-Sign.I.

Після більш ніж річної оцінки NIST, у жовтні 2024 р., NIST оголосив про відбір 14 кандидатів на цифровий підпис, які пройшли до другого раунду в процесі стандартизації постквантової криптографії.

Серед основних переваг постквантових алгоритмів цифрового підпису можна виділити:

- стійкість до квантових атак: розроблені для витримки атак квантових комп'ютерів;
- різноманіття підходів: вже зараз існує велика кількість різних методів забезпечення безпеки.

Водночас вже зараз помітні і деякі недоліки постквантових криптосистем, а саме:

- великі розміри ключів та підписів: деякі алгоритми, як наприклад кодові криптосистеми, вимагають великих розмірів ключів та підписів, що може бути незручним для зберігання та передачі;
- часові затримки: деякі алгоритми мають більший час обчислення у порівнянні з класичними алгоритмами.

Дослідження постквантової криптографії призводить не лише до подолання деяких викликів, але й до появи нових. Можна виділити такі основні питання для пошуку розв'язання:

- оптимізація продуктивності: криптографічні операції повинні бути достатньо швидкими для практичного використання, особливо на обмежених пристроях;

- розмір підпису: багато постквантових алгоритмів мають великі ключі та підписи, що може бути проблематичним для деяких застосувань;
- стійкість до фізичних атак: алгоритми повинні бути стійкими не лише до теоретичних атак квантових комп'ютерів, але й до практичних фізичних атак.

2. Аналіз структури побудови, стійкості та вразливостей FuLeeca, Biscuit, Wave та RYDE

У роботі досліджено чотири постквантові криптографічні алгоритми, що належать до двох принципово різних напрямів – кодових та багатосторонніх схем. Такий вибір зумовлений прагненням порівняти підходи з різною математичною природою, які демонструють високий потенціал у контексті постквантової криптографії та перебувають на різних етапах аналізу і впровадження.

2.1. Постквантовий алгоритм цифрового підпису Fuleeca

Алгоритм FuLeeca (Fujisaki-Lee Code-based Encryption with Error Correcting Codes and Approximation) є одним із представників постквантових криптографічних схем, що базуються на так званій лі-метриці – альтернативі більш поширеній гамінговій метриці. Використання цієї метрики дозволяє створювати компактніші ключі та зменшувати обчислювальні витрати, що робить FuLeeca привабливим кандидатом для застосувань у ресурсно обмежених середовищах. Як варіант шифрування на основі кодів, FuLeeca поєднує ідеї з використанням лінійних кодів, випадкових помилок та схем подовження, аби забезпечити як коректність, так і стійкість до відомих атак.

2.1.1. Математична задача, на якій базується стійкість алгоритму Fuleeca

FuLeeca базується на квазіциклічних метричних кодах Лі. Вага Лі секретних генераторів встановлюється на межі Лі-метрики Гілберта–Варшавова (GV). Це дозволяє розглядати секретний код як випадковий лінійний квазіциклічний код Лі-метрики, який досягає цієї межі з високою ймовірністю.

Квазіциклічні коди є спеціальним типом лінійних блокових кодів, що характеризуються тим, що кожен циклічний зсув коду є також кодовим словом. Вони мають високу структуру і регулярність, що дозволяє ефективно їх реалізовувати та декодувати.

Існує два основні методи побудови схем підпису на основі коду: перший застосовує перетворення Фіата–Шаміра до схеми ідентифікації з нульовим знанням на основі коду, а другий називається підходом Hash and Sign. Перший підхід зазвичай страждає від завеликих розмірів підпису через велику ймовірність шахрайства в схемі ідентифікації, а другий має невеликі розміри підпису за рахунок більшого розміру відкритого ключа. Постквантовий алгоритм цифрового підпису FuLeeca базується на підході Hash and Sign.

Першу схему на основі коду, що дотримується цього підходу, представили в 2001 р. Куртуа, Фініаш і Сендріє [3], яка отримала назву CFS. Ця класична схема підпису Hash and Sign є прямою адаптацією схеми шифрування з відкритим ключем McEliece. Схеми підпису на основі коду, засновані на квазіциклічних структурах з кодами низької щільності Геммінга, вразливі до атак зі статистичними ключами. Зловмисник може відновити розріджений секретний ключ, спостерігаючи за розподілом багатьох підписів і порівнюючи його з випадковим розподілом.

Використання метрики Лі перешкоджає вищевказаним атакам, оскільки навіть незважаючи на те, що вага Лі секретного базису низька, кількість ненульових записів може бути дуже високою для досить великих розмірів поля.

Здебільшого атаки на алгоритм Fuleeca вимагають розв'язання задачі знаходження кодового слова з заданою вагою Лі. Формально вона визначається наступним чином. Необхідно знайти $c \in \mathbb{F}_p^n$, таке, що

$$\begin{cases} cH^T = 0 \\ wt_L(c) = \omega \end{cases} \quad (1)$$

де $H \in \mathbb{F}_p^{(n-k) \times n}$ і $\omega \in \mathbb{N}$ [4].

Знаходження кодових слів заданої ваги еквівалентно задачі декодування [5]. Версія рішення цієї проблеми була доведена як NP-повна [6].

2.1.2. Стійкість алгоритму FuLeesa до атак

Схема підпису FuLeesa полягає в тому, що секретний ключ є квазіциклічною генераторною матрицею, де генератори мають вагу L_i відповідно до обмеження GV метрики L_i , а відкритий ключ є її систематичною формою. Відновлення початкової основи має таку ж складність, як і проблема пошуку кодових слів заданої ваги L_i , яка, як доведено, є NP-складною [6].

Відповідно до вимог NIST було зроблене припущення, що зловмисник має доступ до 264 підписів для вибраних повідомлень. Такі сценарії багаторазового використання вимагають доказу екзистенціальної неможливості підробки під час атаки на вибране повідомлення.

Розробниками було розглянуто атаки, що використовують витік через опубліковані пари геш-функції й підпису. Згадані атаки не можуть бути застосовані до FuLeesa, оскільки в метриці L_i вектори з низькою вагою L_i не обов'язково мають малу підтримку Геммінга. Поклавши вагу секретних генераторів на границю GV , можливо трактувати отриманий код як випадковий. Це перешкоджає Геммінг-метричним атакам, оскільки секретні генератори й підписи мають близьку до повної вагу Геммінга.

Встановлення достатньо високого порогу для кількості необхідних збігів підписів запобігає тому, що раніше опублікований підпис може бути безпосередньо використаний для підписання іншого повідомлення. Очевидним узагальненням цієї атаки повторного використання є створення лінійних комбінацій існуючих підписів для підробки нових підписів.

З переважною ймовірністю вага L_i результуючого вектору буде занадто великою, щоб бути прийнятою верифікатором. Отже, така атака, яка подібна до виконання алгоритму просіювання, відомого з решітчастої криптографії, вимагає складності, яка є експоненціальною по відношенню до параметрів коду. Зокрема, в роботах [7, 8] доведено, що знайти кодове слово з меншою вагою L_i в квазіциклічному коді значно простіше, якщо розмірність коду $n = 2$ є складеним числом. Фактично задача захисту зводиться до задачі знаходження кодового слова у квазіциклічному коді.

Щоб уникнути витоку інформації через опубліковані пари геш/підпис розробниками було інтегровано спеціальну процедуру в алгоритм підписання, яка отримала назву процедури концентрації. Доцільність цієї процедури була доведена розробниками наступним чином. Для двох різних закритих ключів вони порівняли ваги L_i та збіги значень відповідних підписів після застосування простого підпису (рис. 1).

На рис. 1 показано зв'язок між кодовим словом та цільовим вектором, який є гешем повідомлення. Оскільки алгоритм підпису ефективно співвідносить секретний ключ і геші, то виявляється можливим дізнатися принаймні деяку інформацію про секретний ключ на основі розподілу отриманих кодових слів.

Незважаючи на те, що конкретної атаки, що використовує цю поведінку, не наведено, результати показують, що деяка інформація про приватний ключ витікає й потенційно може бути використана для допомоги в процесі відновлення секретного ключа.

На рис. 2 показано розподіл значень логарифмічної ймовірності збігу та відносних ваг L_i для тих самих гешів, що й на рис. 1, але вже після завершення концентруючої частини алгоритму. Результати показують, що процедура концентрації значно зменшує витік, який можна спостерігати за відносною вагою L_i та логарифмічною ймовірністю збігу.

У 2023–2024 рр. FuLeesa став об'єктом кількох глибоких криптоаналітичних досліджень. 21 липня 2023 р. Феліцітас Хьорманн і Вессел ван Вурден опублікували можливу атаку на алгоритм FuLeesa, що не зламує всі системи на базі L_i -метрики, але є специфічною для схеми FuLeesa [9]. Вона засвідчила, що алгоритм вразливий до побічних атак, що базуються на витоку інформації (leakage-based learning). Зокрема, при атаці використовується вибір інформаційного вектору x , який використовується для отримання підпису $v=xG$. Оскільки цей вектор вибрано з малими записами, зловмисник може розглянути цілочисельну алгебраїчну

решітку $L(G)$. Крім того, вибір $G = (A \mid B)$ як квазіциклічного коду дозволяє зломиснику працювати в циркулянтній алгебраїчній решітці $L(A)$.

Після публікації атаки, командою розробників було розглянуто методи захисту, але жоден із них не продемонстрував позитивного результату, адже вони призводять до вразливості щодо атак підробки та до непрактичних розмірів відкритих ключів. Наразі розробники алгоритмів працюють над вдосконаленням схеми.

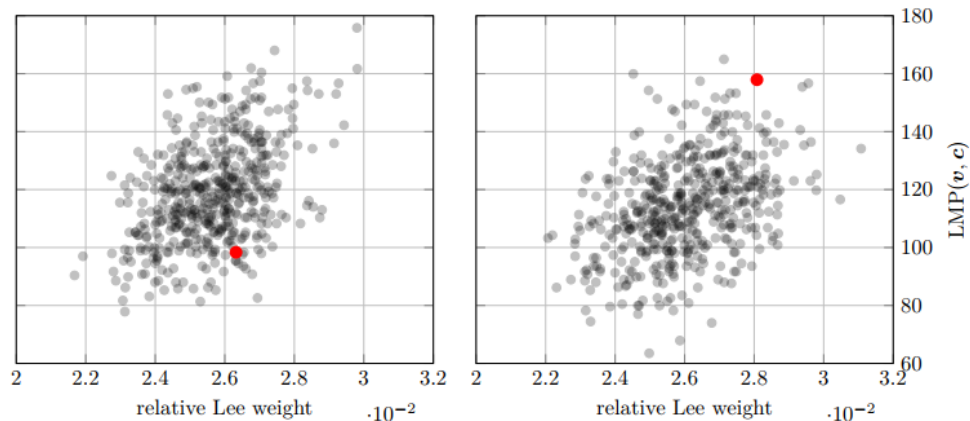


Рис. 1. Оцінка 500 підписів для імітованих гешів із використанням двох різних ключів після застосування «простого підпису»

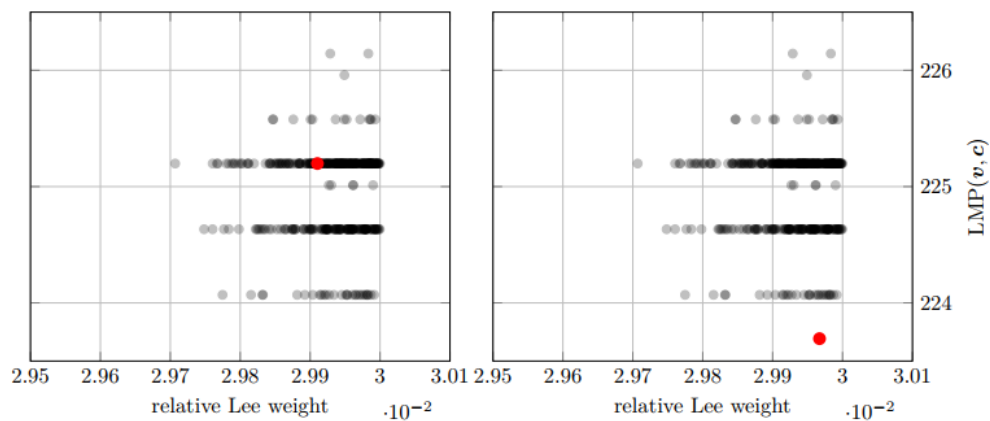


Рис. 2. Оцінка 500 підписів для імітованих гешів для двох різних ключів після застосування підпису й процедури концентрування

2.2. Постквантовий алгоритм цифрового підпису WAVE

Wave – постквантовий алгоритм цифрового підпису, який поєднує ідеї з теорії помилок виправних кодів і концепцію пасток (trapdoor) на основі спеціальних лінійних кодів. Він реалізує підхід Hash-and-Sign для поля $\mathbb{F}_3$ з використанням складної схеми кодування. Його безпека ґрунтується на NP-складній задачі декодування в геммінговій метриці та задачі розрізнення спеціальних кодів від випадкових. Завдяки коротким підписам і швидкій перевірці, Wave є потенційно придатним для використання у високопродуктивних системах з допустимим компромісом – великим розміром відкритого ключа [10].

2.2.1. Математична задача, на якій базується стійкість алгоритму Wave

Цифровий підпис Wave базується на NP-складній задачі декодування лінійних кодів у геммінговій метриці, зокрема її варіації – Decoding One Out of Many (DOOM). Суть цієї задачі полягає у знаходженні кодового слова фіксованої ваги, яке відповідає одному з багатьох синдромів, утворених шляхом гешування повідомлень [11]. Саме така постановка задачі виникає в схемах типу Hash-and-Sign, до яких належить алгоритм Wave.

Базовою задачею, що лежить в основі Wave, є Decoding Problem (DP). Вона формулюється наступним чином: нехай $H \in \mathbb{F}_3^{(n-k) \times n}$ – матриця перевірки на парність для деякого лінійного коду, а $s \in \mathbb{F}_3^{(n-k)}$ – синдром. Необхідно знайти вектор $e \in \mathbb{F}_3^n$ з геммінговою вагою $|e| = w$, такий що

$$eH^T = s. \quad (2)$$

Ця задача є NP-повною, навіть у випадку фіксованого алфавіту та випадкових матриць H . Саме на ній базується безпека більшості схем, що використовують лінійні коди, зокрема класичних схем McEliece і Niederreiter.

У схемі Wave зломисник стикається не з однією, а з великою кількістю потенційних синдромів, оскільки підпис формується шляхом підбору випадкового параметра salt, а далі гешування повідомлення разом із salt:

$$s = H(m||salt). \quad (3)$$

Таким чином, для атаки на підпис зломисник повинен знайти такий вектор e , що для деякого i

$$He^T = H(m_i||salt). \quad (4)$$

Це призводить до постановки задачі DOOM, яка формально формулюється так: для заданої матриці H та великої множини синдромів $\{s_1, s_2 \dots s_q\}$ знайти такий вектор e фіксованої ваги w [11], що для деякого i

$$He^T = s_i. \quad (5)$$

Задача DOOM вважається складнішою за звичайну задачу DP, оскільки вона передбачає вибір з множини випадкових цілей. Це унеможливило застосування специфічних декодерів, що працюють лише для обмежених класів синдромів, і забезпечує додаткову стійкість схеми навіть у моделі з доступом до вибраних повідомлень (chosen-message attack).

Щоб зробити задачу DP розв'язуваною лише для власника секретного ключа, у Wave використовується спеціальна пастка (trapdoor) – структурований код типу $(U||U + V)$, побудований над полем $\mathbb{F}_3$ [11]. Код має наступну конструкцію:

$$C = \{(u, u + v) : u \in U, v \in V\}, \quad (6)$$

де $U, V \subset \mathbb{F}_3^{n/2}$ – лінійні підкоди.

Далі код піддається перестановці координат π та додаванню маскуючих векторів b, c , що перешкоджає розпізнаванню структури зі сторони.

Секретний ключ – це опис кодів U і V , перестановки π та векторів маскування. Завдяки цій структурі, власник секретного ключа може ефективно декодувати синдроми шляхом розкладу на eV та eU , тоді як для зломисника задача залишається аналогом випадкового коду.

Розмірність коду та вага w у Wave підібрані так, щоб задача декодування залишалася за межами зони ефективного декодування. Існує відомий інтервал значень w , у якому ймовірність існування коду з помилками, що задовольняють умову (4), є низькою, і жоден відомий алгоритм (навіть ISD) не може вирішити задачу швидко. Wave працює за цим порогом, гарантуючи, що навіть оптимальні класичні чи квантові атаки не можуть зламати систему при дотриманні рекомендованих параметрів.

Оскільки схема підпису Wave реалізує парадигму Hash-and-Sign, вона критично залежить від геш-функції H . Саме вона трансформує повідомлення у синдром, що потрібно декодувати. Щоб уникнути ймовірності відсутності рішення, схема генерує випадкове значення salt і підбирає його доти, поки задача DOOM не має розв'язку для поточного $m||salt$.

Ця особливість підкреслює, що алгоритм фактично шукає серед багатьох DOOM-випадків – саме той, для якого існує придатне e , що вдається зробити лише знаючи внутрішню структуру пастки.

2.2.2. Стійкість алгоритму Wave до атак

Кодовий криптоалгоритм WAVE дотримується тієї самої схеми, що й FuLeesa, але базується на новій проблемі: декодуванні великих помилок ваги. Цією схемою вдалося запобігти всім вищезазначеним атакам (див. п. 2.1.2), і досі не було встановлено жодного успішного алгоритму криптоаналізу. Однак, стійкість до атак досягається за рахунок непрактично великих розмірів відкритих ключів.

Безпека алгоритму Wave має формальне обґрунтування і базується на складності задач Decoding One Out of Many (DOOM) та розрізнення структури відкритого ключа (DWK). Розробники алгоритму провели повний доказ стійкості в моделі Quantum Random Oracle Model (QROM), враховуючи можливість атак з боку квантових зломисників. Водночас у схемі враховано потенційні канали витоку інформації з підписів, які мінімізуються завдяки використанню технік rejection sampling та спеціальних розподілів.

Стійкість Wave доведено у моделі existential unforgeability under chosen message attacks (EUF-CMA). Це означає, що навіть за наявності доступу до оракула підпису, зломисник не зможе згенерувати підпис для нового повідомлення.

У доведенні безпеки Wave використовується зведення атаки на підпис до двох основних задач:

1. DOOM (n, k, w, q) – задача знаходження вектора e фіксованої ваги w , яке задовольняє хоча б одне з q рівнянь виду (5).

2. DWK (Distinguishing Wave Keys) – задача визначення, чи є задана матриця відкритого ключа переставленою пасткою ($U \parallel U+V$)-коду, чи випадковою.

Формально ймовірність успішної атаки оцінюється як

$$\Pr[\text{forge}] \leq 2 \cdot (\text{Adv}_{\text{DOOM}} + \text{Adv}_{\text{DWK}} + \frac{q_s^2}{2\lambda_0}), \quad (7)$$

де q_s – кількість запитів до оракула підпису, а λ_0 – довжина salt, яка завжди більше 256.

Відкритий ключ Wave – результат маскування структури коду ($U \parallel U + V$) шляхом перестановки π і додавання векторів b і c . Утворений код має вигляд

$$\pi(U \parallel (U+V)) + b + c. \quad (8)$$

Задача DWK передбачає, що зломисник намагається розпізнати, чи цей код має приховану структуру, тобто є переставленою версією ($U \parallel U + V$)-коду. Відомо, що жоден ефективний метод не здатен надійно вирішити цю задачу без знання перестановки π , особливо коли параметри n і k великі, як у Wave822, Wave1272 та Wave1906.

Щоб запобігти витоку інформації про секретний ключ через спостереження за великою кількістю підписів, у Wave реалізовано механізм відхилення зразків (rejection sampling) [11]. Підпис формується лише в разі, якщо згенерований вектор помилок e належить спеціальному розподілу D , який не залежить від ключа.

Зокрема, вектори e формуються з використанням двох внутрішніх розподілів: DV – для частини помилки, яка декодується V -кодом; DU – для помилки в U -коді.

Розподіл усіх підписів наближено до рівномірного на множині векторів фіксованої геммінгової ваги. В [11] показано, що Реньї-дивергенція між реальним і ідеальним розподілом підписів не перевищує 2^{-68} , тобто навіть за умови доступу до 2^{64} підписів, зломисник не отримає статистично значущої інформації про секретний ключ.

Найефективнішими на практиці є атаки типу ISD (Information Set Decoding) – комбінаторні атаки, які намагаються знайти підмножину координат, де розв'язок має особливу структуру. У Wave ці атаки застосовуються як до задачі DOOM, так і до DWK, але складність залишається експоненційною навіть для найменших параметрів (Wave-822). Наприклад: для класичної моделі: складність $\approx 2^{128}$; для квантової моделі з алгоритмом Гровера: $\approx 2^{64}$, однак необхідна кількість оперативної пам'яті і квантостійкість salt не дозволяють реалізувати такі атаки на практиці.

Навіть за умов обмеження salt-простору, підробити підпис без знання секретного коду залишається складним. Зловмиснику необхідно: вгадати salt, для якого є придатний синдром; знайти вектор e з відповідною геммінговою вагою, що задовольняє $He^T = s$; забезпечити, щоб результат підпису пройшов перевірку розподілу. Виконання цих трьох умов одночасно є високоскладним у обчислювальному сенсі, навіть за умов знання великої кількості валідних підписів.

У сукупності наведені властивості забезпечують високий рівень стійкості Wave як у класичній, так і в квантовій моделі атак. Жодна з відомих атак не дозволяє зламати навіть найменший параметр (Wave822) при адекватному рівні обчислювальних ресурсів, що робить цю схему однією з найперспективніших серед постквантових алгоритмів цифрового підпису.

2.3. Постквантовий алгоритм цифрового підпису Biscuit

Biscuit – сучасна криптографічна схема цифрового підпису, що базується на складності розв'язування систем багатосторонніх квадратичних рівнянь (MQ), яка вважається стійкою до атак з боку квантових комп'ютерів. Biscuit є однією з небагатьох MQ-схем нового покоління, яка поєднує компактність підпису, порівняно низькі вимоги до обчислювальних ресурсів та оригінальний підхід до обфускації структурних елементів схеми.

Алгоритм розроблено з урахуванням новітніх криптоаналітичних атак на попередні MQ-схеми (наприклад, Rainbow) і має за мету запропонувати підпис, що поєднує в собі гнучкість параметрів безпеки та придатність до використання в практичних сценаріях. У цьому підрозділі детально розглядається математична основа, криптографічна стійкість, продуктивність та вимоги до реалізації алгоритму Biscuit з метою визначення його потенціалу як надійного постквантового рішення.

2.3.1. Математична задача, на якій базується стійкість алгоритму Biscuit

Протокол багатосторонніх обчислень (MPC) – це протокол, який виконується набором з N учасників, які знають відкриту функцію f . Мета протоколу – обчислити зображення z :

$$z = f(x_1, \dots, x_N), \quad (9)$$

де значення x_i відоме тільки i -й стороні.

Протокол MPC вважається безпечним і коректним, якщо в кінці протоколу кожна сторона i знає z , і ніяка інформація про її секретне вхідне значення x_i не стає відомою іншим сторонам.

Алгоритм постквантового цифрового підпису Biscuit побудований на проблемі розв'язування багатосторонніх рівнянь, визначених як добуток двох афінних форм. Ця задача параметризується кортежем натуральних чисел (n, m, q) , який позначається як *PowAff2*.

Формально ця проблема визначається наступним чином [12]. Необхідно знайти вектор $(s_1, \dots, s_n) \in \mathbb{F}_q^n$, такий, що

$$f_1(s_1, \dots, s_n) = t_1, \dots, f_m(s_1, \dots, s_n) = t_1, \quad (10)$$

де

$$f_1(x_1, \dots, x_n) = A_{k,0}(x_1, \dots, x_n) + \prod_{j=1}^2 A_{k,j}(x_1, \dots, x_n), \quad (11)$$

для усіх $k \in [m]$, якщо $t = (t_1, \dots, t_m) \in \mathbb{F}_q^m$, афінне перетворення $A_{k,j}(x_1, \dots, x_n) \in \mathbb{F}_q[x_1, \dots, x_n]$, $k \in [m]$ і $0 \leq j \leq 2$ [12].

Задачу *PowAff2* можна розглядати як структурований варіант задачі розв'язування m -квадратних рівнянь у $\mathbb{F}_q[x_1, \dots, x_n]$, тобто багатовимірної квадратної задачі (MQq). Відомо, що ця задача є NP-важкою [13].

При $m=n$ і для достатньо великого поля доведено, що поліноми *PowAff2*, поведуться як звичайні квадратичні поліноми. Очікується, що це також матиме місце у випадку $m > n$ [14], що розглядається у Biscuit.

Варто зазначити, що формальне доведення цього питання еквівалентне розв'язанню гіпотези Фреберга, яка є давньою проблемою у комутативній алгебрі. Таким чином, розв'язати випадкові випадки задачі *PowAff2* було б так само важко, як і випадкові екземпляри задачі MQ_q розв'язування системи нелінійних квадратних рівнянь над скінченним полем $\mathbb{F}_q$ проти загальних алгоритмів.

Захищеність від загальних алгоритмів для задачі MQ_q не виключає можливості існування потенційно нових швидших алгоритмів, які враховують структуру рівнянь або знання афінних карт $A_{k,j}$. Втім, поліноміальні системи зі структурою задачі *PowAff2* були широко вивчені раніше в постквантовій криптографії й наразі відповідних загроз винайдено не було.

2.3.2. Стійкість алгоритма Biscuit до атак

На сьогодні існує значна кількість алгоритмів, що розв'язують проблему MQ_q [12]. Найактуальніші алгоритми включають:

1. Алгоритми для недовизначених систем. Система рівнянь називається недовизначеною, якщо вона має більше невідомих, ніж рівнянь, тобто в наших позначеннях $m < n$. Перший підхід полягає у фіксації значень $n - m$ невідомих і подальшому розв'язуванні відповідної квадратної системи рівнянь. Для систем, де m набагато менше, ніж n , були запропоновані покращені алгоритми, наприклад алгоритм, запропонований Патарінім, Куртуїзом та Губінім [15], алгоритм Thomae-Wolf [16] і його останню модифікацію, запропоновану Хірокі Фуруе, Шухей Накамура та Цуйюші Такагі [17].

2. Швидкий вичерпний пошук. Спосіб виконання полягає у вичерпному пошуку $\mathbb{F}_2^n$ шляхом нумерації простору розв'язку кодами Грея. Часова складність знаходження одного розв'язку задачі MQ_2 за допомогою цього алгоритму визначається як $4 \log(n)2^n$. Цей підхід можна поширити на будь-яке поле $\mathbb{F}_q$ за допомогою лексикографічного впорядкування замість кодів Грея, з часовою складністю задається $O(dq^n)$ [18].

3. Базисні алгоритми Гребнера – це спеціальний набір багаточленів, який має ті ж самі корені, що й початковий набір, але володіє додатковими властивостями. Цей базис дозволяє легко вирішувати багато задач, пов'язаних із системами багаточленів, таких як розв'язання систем нелінійних рівнянь і перетворення між різними представленнями алгебраїчних структур. Існує кілька алгоритмів для побудови базисів Гребнера, серед яких найвідомішими є алгоритм Бухбергера і F4 та F5 алгоритми. Це алгоритм, що дозволяє знайти базис Гребнера шляхом послідовного додавання і спрощення багаточленів, а також його покращені версії, які використовують матричні методи і різні оптимізації для прискорення обчислень [12].

4. Гібридні підходи. У серії робіт автори описують гібридні методи, які поєднують вичерпний пошук і обчислення, подібні до базису Гребнера; що призводить до асимптотично швидких алгоритмів, наприклад алгоритму Hybrid-(F4/F5) і Crossbed. Ефективність таких підходів пов'язана з вибором компромісу між цими двома методами.

5. Імовірнісні алгоритми. Лоскштанов та інші були першими, хто ввів імовірнісні алгоритми, які в гіршому випадку розв'язують MQ_q за час $O(q^{\delta n})$, для деякого $\delta < 1$, що залежить лише від q і ступеня системи, не покладаючись на жодне недоведене припущення.

Щоб полегшити аналіз безпеки на основі MQ_q , Р. Макарім, К. Санна та Дж. Вербел [19] запровадили програмний інструмент під назвою MQEstimator, який дозволяє отримати рівень безпеки для вирішення даного екземпляра MQ_q з урахуванням усіх можливих відомих атак.

Приблизну бітову складність можна оцінити як $(\log q)^\theta$, помножену на $\mathbb{F}_q$ -часову складність, з $\theta \in [1, 2]$. З іншого боку, складність бітового простору просто дорівнює $\log q$, помноженому на $\mathbb{F}_q$ -просторову складність.

Іншу загрозу складають засоби квантового криптоаналізу. Зазначимо найдоцільніші з них:

1. Квантовий вичерпний пошук. Перший квантовий алгоритм для MQ_2 належать П. Швейбу та Б. Вебштербауну [20]. Автори описали квантовий варіант вичерпного пошуку з

використанням алгоритму Гровера, як результат було отримано точні оцінки ресурсів для їхніх алгоритмів, які демонструють, що квантовий комп'ютер може розв'язувати m двійкових квадратних рівнянь у n двійкових змінних, використовуючи $O(m + n)$ кубітів і вимагаючи оцінки $O(mn^2 2^{n/2})$ квантових воріт. Автори також описують варіант із використанням меншої кількості кубітів, тобто $O(n + \log_2(m))$, але з удвічі більшою кількістю квантових воріт, ніж перший підхід.

2. GroverXL. Автори запропонували квантовану версію XL, розглянувши варіант FXL, який поєднує XL з вичерпним пошуком. Принцип GroverXL полягає в поєднанні FXL з алгоритмом Гровера. GroverXL вирішує MQ_q з часовою складністю $2^{(t+o(1))n}$ комп'ютера з mesh-з'єднанням області $2^{(a+o(1))n}$. Значення t і a можуть бути явно обчислені для заданих параметрів екземпляра MQ_q , що розглядається.

3. QuantumMQSolve. Пропонується й дещо інший підхід для поєднання квантових алгоритмів і базисів Гребнера. На сьогодні це найшвидший відомий квантовий алгоритм для вирішення MQ_q . Нехай:

$$m = \lceil \alpha n \rceil, \text{ де } \alpha \geq 1. \quad (12)$$

Для $q = 2$ QuantumMQSolve має середню складність:

$$O(2^{(\frac{1}{2}-0.0375\alpha)n}). \quad (13)$$

Зокрема, для $\alpha = 1$ складність визначається як $O(2^{0.462n})$.

Коли $n = m \rightarrow \infty, q \rightarrow \infty$ і $\log_2(q) \leq n$, QuantumMQSolve має середню складність:

$$O(2^{n(2.76 - \frac{1.26}{\log_2(\sqrt{q})})}). \quad (14)$$

Наведені нижче складності є асимптотичними та неточними для заданих параметрів (q, n, m) . Але вартість QuantumMQSolve також можна чітко обчислити шляхом мінімізації компромісу та використання більш точної форми складності.

4. Квантові алгоритми Гребнера. Новий підхід для розв'язання MQ_2 і більш загальний MQ_q полягає у використанні квантового алгоритму А. Харроу, А. Хасідіма та С. Ллойда (HLL) для вирішення лінійних систем. Квантовий вичерпний пошук майже завжди є швидшим, ніж підхід HLL для MQ_2 Чена та Гао. Автори також запропонували вдосконалений варіант алгоритму Чена і Гао для MQ_2 , складність якого експоненціальна у вазі Геммінга. Зокрема, ця версія перевершує квантовий вичерпний пошук, коли вага Геммінга рішення логарифмічна за кількістю змінних.

2.4. Постквантовий алгоритм цифрового підпису RYDE

Алгоритм RYDE (Rank-sYndrome-based Digital signaturE) – RYDE (Rank-sYndrome-based Digital signaturE) побудований на складності задачі декодування синдрому в ранговій метриці, що є NP-важкою і не має відомих квантових алгоритмів, здатних її ефективно розв'язати. На відміну від класичних кодових криптосистем у геммінговій метриці, використання рангової метрики дозволяє суттєво зменшити розміри ключів та підписів [21].

RYDE поєднує у своїй структурі кодові схеми з сучасними криптографічними техніками, такими як zero-knowledge докази та багатосторонні обчислення (MPC-in-the-head), що забезпечують високий рівень конфіденційності та автентичності. Цей підрозділ присвячено аналізу математичної основи, стійкості до криптоаналітичних атак, продуктивності та практичної реалізації алгоритму RYDE в умовах квантової загрози.

2.4.1. Математична задача, на якій базується стійкість алгоритму RYDE

Схема цифрового підпису RYDE побудована на NP-складній задачі декодування синдрому в ранговій метриці – Rank Syndrome Decoding (Rank-SD). Це одна з фундаментальних задач у кодовій криптографії, яка залишається важкою навіть за умови використання кванто-

вих обчислень. Її складність зростає експоненційно з параметрами, і саме це забезпечує криптографічну стійкість алгоритму.

Rank-SD є узагальненням задачі декодування синдрому, що широко використовується в класичних схемах McEliece або Niederreiter, але замість метрики Геммінга тут використовується рангова метрика. У ранговій метриці вага вектора визначається як ранг відповідної матриці, яка утворюється з координат вектора при розкладі над основним полем. Таким чином, вага рангу є мінімальною розмірністю підпростору, що містить усі координати вектора.

Формально задача Rank Syndrome Decoding визначається таким чином: дано випадкову матрицю $H \in \mathbb{F}_{q^m}^{(n-k) \times n}$, а також вектор y , що має рангову вагу не більше за деяке r :

$$y = Hx, x \in \mathbb{F}_{q^m}^n. \quad (15)$$

Необхідно знайти вектор x , знаючи H та y . Ця задача зберігає свою складність навіть у випадку випадкових кодів, і є доведено складною у сенсі NP-повноти [22].

В основі схеми RYDE лежить перетворення задачі знання рішення Rank-SD у доказ із нульовим розголошенням знань. Для цього використовується так званий підхід MPC-in-the-Head, при якому імітується багатосторонній протокол обчислень (MPC), де кожна «партія» володіє часткою секретного вектора x . За допомогою цього підходу будується інтерактивний доказ володіння рішенням до задачі Rank-SD, який згодом перетворюється на підпис завдяки трансформації Фіата-Шаміра.

Відмітною особливістю рангової метрики є значно менша кількість можливих векторів заданої ваги порівняно з метрикою Геммінга. Це дозволяє побудувати компактніші підписи без втрати стійкості. Крім того, проблема Rank-SD демонструє високу стійкість як до комбінаторних атак (перебору підтримки вектора), так і до алгебраїчних атак, таких як методи базисів Гребнера. Складність атак істотно зростає з параметрами та лишається високою навіть при застосуванні квантових алгоритмів (наприклад, Гровера).

Таким чином, безпека схеми підпису RYDE прямо залежить від складності задачі Rank Syndrome Decoding, що робить її перспективним кандидатом у сфері постквантової криптографії.

2.4.2. Стійкість алгоритму RYDE до атак

Схема цифрового підпису RYDE базується на задачі декодування синдрому в ранговій метриці (Rank-SD), що є NP-складною. Однак для повноти аналізу безпеки важливо розглянути не лише математичну складність базової задачі, а й стійкість алгоритму до конкретних типів атак, що можуть бути застосовані проти як Rank-SD, так і проти структури підпису як такого. У цьому підрозділі розглянуто основні напрями атак: комбінаторні, алгебраїчні, атаки на схему підпису на основі доказів з нульовим розголошенням знань, а також вплив квантових алгоритмів.

Найбільш класичними атаками на Rank-SD [22] є комбінаторні методи, які зводяться до перебору можливих підтримок (підпросторів) секретного вектора. Основна ідея полягає в тому, щоб вгадати підпростір $E \subset \mathbb{F}_{q^m}$, що містить підтримку вектора x , і потім перетворити рівняння (15) у систему лінійних рівнянь над полем $\mathbb{F}_q$.

Найвідомішим є алгоритм Chabaud-Stern, складність якого оцінюється як

$$O((nr + M)^3 \cdot q^{(m-r)(r-1)}), \quad (16)$$

де n – довжина вектора, r – ранг вектору, m – розмірність поля.

Через експоненційний множник $q^{(m-r)(r-1)}$ атака стає непридатною при достатньо великих параметрах, які використовуються в RYDE.

Інший метод – це GRS-алгоритм, що є адаптацією методу інформаційного множини для рангової метрики. Його ефективність залежить від ймовірності вгадати підпростір, що містить підтримку вектора, і складність також має експоненційну залежність від параметрів виду

$$O((n-k)^3 m^3 \cdot q^{r \cdot \lfloor \frac{(k+1)m}{n} \rfloor}). \quad (17)$$

У RYDE ці атаки не є ефективними, оскільки схема використовує параметри, близькі до межі Гілберта–Варшавова в ранговій метриці, що забезпечує мінімальну ймовірність вгадування підтримки.

Алгебраїчні атаки формулюють задачу Rank-SD як систему поліноміальних рівнянь і розв’язують її методами алгебраїчної геометрії (наприклад, базисами Гребнера). Найефективнішими на сьогодні є:

MaxMinors Modeling – метод, що формує систему рівнянь на основі мінорів добутку матриць;

Support Minors Modeling – розширення попереднього підходу, яке зменшує кількість змінних за рахунок фіксації частини підтримки.

Для обох моделей існує гібридний метод, який фіксує деякі змінні (припущення) та перебирає всі їх значення, зменшуючи розмір системи, але збільшуючи кількість запусків. У будь-якому разі ці підходи залишаються експоненційно складними при параметрах, рекомендованих для схеми RYDE.

У контексті постквантової безпеки важливо враховувати можливість застосування квантових алгоритмів:

- алгоритм Гровера дозволяє прискорити перебір до $O(2^{\frac{n}{2}})$ замість 2^n , що впливає на комбінаторні атаки;

- для алгебраїчних методів, зокрема тих, що базуються на базисах Гребнера, переваги квантових обчислень наразі не доведені, тобто ці атаки не покращуються на квантових комп’ютерах.

Розробники RYDE встановили параметри, що вдвічі перебільшують мінімально необхідні для стійкості до квантових атак. Наприклад, для рівня безпеки AES-128, складність атаки Rank-SD повинна бути щонайменше 2^{256} , що дозволяє квантове зниження до 2^{128} [21].

Схеми підпису, що базуються на доказах з нульовим розголошенням знань, також уразливі до так званих атак Калеса–Заверучі, які використовують факт повторного використання випадковостей у кількох сесіях доказу. Вони дозволяють зменшити складність підробки, якщо кількість раундів кількості раундів MPC-симуляції τ недостатня. Значення τ у схемі RYDE обране так, щоб атака Калеса–Заверучі не давала жодної практичної переваги. Крім того, алгоритм використовує гіперкубову структуру для подання MPC-партій, що дозволяє приховати інформацію при відкритті лише частини протоколу.

Як і для будь-якої схеми підпису, важливо враховувати можливість атак за багаторазовим використанням. У RYDE зловмисник потенційно може мати доступ до великої кількості пар повідомлення–підпис. Схема проєктувалась таким чином, щоб:

- кожен підпис був унікальним завдяки випадковим сольовим значенням;
- кількість інформації, яка розкривається в MPC-протоколі, контролюється через вибір параметра N (кількість партій);
- параметри обрані так, щоб статистичний аналіз підписів не давав змоги відновити частини секретного ключа.

Таким чином, схема RYDE демонструє високу стійкість до всіх відомих типів атак:

- NP-складна математична основа (Rank-SD);
- низька ймовірність вгадування підпростору підтримки;
- стійкість до атак на перетворення Фіата–Шаміра через налаштування τ і MPCitH;
- стійкість до квантових атак завдяки подвоєній оцінці параметрів.

У сукупності це робить RYDE одним із найбільш надійних алгоритмів цифрового підпису в умовах як класичних, так і квантових загроз.

Висновки

Постквантові алгоритми цифрового підпису є ключовим напрямом сучасної криптографії, які гарантують безпеку даних у майбутньому світі з квантовими комп'ютерами. Різноманіття підходів дозволяє обрати оптимальний алгоритм для конкретних умов використання, але також ставить перед викликами, пов'язаними з ефективністю та розміром ключів. Подальші дослідження в цій галузі є вкрай необхідними для забезпечення безпеки інформації у квантову еру.

Проведене дослідження алгоритмів цифрового підпису, стійких до квантового криптоаналізу, дозволило системно проаналізувати один із найактуальніших напрямів сучасної криптографії, що виник у відповідь на стрімкий розвиток квантових обчислювальних технологій. У ході роботи досліджено чотири алгоритми цифрового підпису, подані до четвертого раунду конкурсу NIST: FuLeesa, Biscuit, Wave та RYDE. Вибір саме цих алгоритмів пояснюється їхньою різною математичною природою, а також потенціалом для використання в сучасних ІТ-системах із різним рівнем ресурсних обмежень.

Дослідження алгоритму FuLeesa підтвердило його концептуальну ефективність у контексті постквантової криптографії, однак виявило критичні вразливості при наявності побічних каналів витоку інформації. Попри математичну надійність конструкції на рівні базової моделі, практична безпека значною мірою залежить від фізичного середовища реалізації. Атака FuLeakage демонструє можливість витягнення секретного ключа за допомогою машинного навчання, навіть без повного доступу до внутрішнього стану системи. Це свідчить про необхідність інтеграції контрзаходів на рівні реалізації, зокрема технік маскування або шумозахисту. Хоча FuLeesa не є універсально скомпрометованою схемою, її практичне використання потребує серйозного перегляду підходів до безпечної реалізації. Подальші дослідження повинні зосередитися на розробці захищених реалізацій та перевірці стійкості до широкого спектра побічних атак.

Алгоритм Wave є багатосторонньою схемою цифрового підпису, побудованою на кодах та використанні гаусового приховування. Його відмінною рисою є відсутність структури в матрицях приватного ключа, що потенційно підвищує стійкість до структурних атак. Проведений аналіз підтвердив коректність роботи алгоритму, а також теоретичну стійкість до атак, що використовують класичні та квантові обчислення. Попри публікації, в яких пропонувались потенційні атаки на Wave, жодна з них не продемонструвала практичного компрометування схеми за рекомендованих параметрів. Ключовим елементом забезпечення безпеки залишається правильна реалізація вибірки підписів із використанням rejection sampling. Саме ця процедура унеможливорює витoki інформації, що могли б бути використані для відновлення секретного ключа. Слід зауважити, що Wave не пройшов до фінальних етапів початкового конкурсу NIST через відкликання заявки з боку авторів, однак вартий розгляду як перспективний стійкий до квантового криптоаналізу алгоритм.

Аналіз алгоритму Biscuit показав, що ця MQ-схема є перспективним кандидатом для застосування в постквантових умовах, завдяки високій стійкості до квантового криптоаналізу та порівняно помірним вимогам до апаратного забезпечення. Алгоритм демонструє хорошу продуктивність при генерації ключів, підписанні та перевірці, а також забезпечує гнучке налаштування параметрів для досягнення різних рівнів безпеки. Особливою перевагою Biscuit є його захист від сучасних атак на структуру MQ-схем завдяки ефективним методам приховування внутрішніх параметрів. Водночас деякі обмеження, зокрема пов'язані з розміром відкритого ключа та необхідністю ретельної параметризації, залишають простір для подальших досліджень і оптимізацій. Загалом, Biscuit може розглядатися як реалістична альтернатива для реалізації квантово-стійких електронних підписів, особливо в контексті систем, що потребують високого рівня безпеки та підтримують багатосторонню криптографічну основу.

Дослідження алгоритму RYDE підтверджує його потенціал як криптографічної схеми, здатної забезпечити високий рівень безпеки в умовах епохи квантових обчислень. Алгоритм

демонструє достатні показники ефективності, зокрема – відносно невеликі розміри ключів і підписів, що є перевагою над деякими іншими PQDS-схемами. Застосування складної задачі декодування синдрому в ранговій метриці як основи стійкості робить RYDE несприйнятливим до широкого спектру як класичних, так і квантових атак. Крім того, використання концепції zero-knowledge і багатосторонніх обчислень у проєктуванні алгоритму підвищує довіру до його криптографічних властивостей. Разом з тим, складність реалізації MPC-підходу може створювати додаткові виклики при імплементації в обмежених середовищах. Проте загальний баланс між безпекою, продуктивністю та ефективністю дозволяє вважати RYDE одним із сильних кандидатів для стандартизації та подальшого впровадження в системи, що потребують високого рівня криптографічного захисту.

Список літератури:

1. Additional PQC Digital Signature Candidates Announced | Computer Security Resource Center. URL: <https://csrc.nist.gov/news/2023/additional-pqc-digital-signature-candidates>
2. Post-Quantum Cryptography: Digital Signature Schemes | Computer Security Resource Center. URL: <https://csrc.nist.gov/Projects/pqc-dig-sig/round-1-additional-signatures>
3. Nicolas T Courtois, Matthieu Finiasz, and Nicolas Sendrier. How to achieve a McEliece-based digital signature scheme. B Advances in Cryptology–ASIACRYPT 2001 // 7th International Conference on the Theory and Application of Cryptology and Information Security Gold Coast, Australia, December 9-13, 2001 Proceedings 7, pages 157-174. Springer, 2001.
4. Stefan Ritterhoff, Sebastian Bitzer, Patrick Karl, Georg Maringer, Thomas Schamberger, Jonas Schupp, Georg Sigl, Antonia Wachter-Zeh, Violetta Weger. FuLeeca Submission to the NIST Post-Quantum Cryptography Standardization Process Algorithm Specifications and Supporting Documentation // Technical University of Munich, Germany. 2023. URL: <https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/FuLeeca-spec-web.pdf>.
5. Anna-Lena Horlemann-Trautmann and Violetta Weger. Information set decoding in the Lee metric with applications to cryptography // Advances in Mathematics of Communications. 2001. 15(4).
6. Violetta Weger, Karan Khathuria, Anna-Lena Horlemann, Massimo Battaglioni, Paolo Santini, and Edoardo Persichetti. On the hardness of the Lee syndrome decoding problem // Advances in Mathematics of Communications, April 2022. Publisher: Advances in Mathematics of Communications.
7. Craig Gentry. Key recovery and message attacks on ntru-composite. In Advances in Cryptology–EUROCRYPT 2001 // International Conference on the Theory and Application of Cryptographic Techniques Innsbruck, Austria, May 6-10, 2001 Proceedings 20, pages 182-194. Springer, 2001.
8. Carl Löndahl, Thomas Johansson, Masoumeh Koochak Shooshtari, Mahmoud Ahmadian-Attari, and Mohammad Reza Aref. Squaring attacks on McEliece public-key cryptosystems using quasicyclic codes of even dimension // Designs, Codes and Cryptography. 2016. 80:359-377.
9. Round 1 (Additional Signatures) OFFICIAL COMMENT: FuLeeca. URL: <https://eprint.iacr.org/2024/353>
10. Gustavo Banegas et al. Wave Round 1 Submission . NIST Computer Security Resource Center | CSRC. URL: <https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/wave-spec-web.pdf> .
11. Bénéteau J., Deneuville J.-C., Gaborit P., & Zémor G. Wave: A new family of trapdoor one-way preimage sampleable functions based on codes. Post-Quantum Cryptography, PQCrypto 2019. URL: https://doi.org/10.1007/978-3-030-25510-7_15.
12. Luk Bettale, Delaram Kahrobaei. Biscuit: Shorter MPC-based Signature from PoSSo. URL: <https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/Biscuit-spec-web.pdf>.
13. M. R. Garey and David S. Johnson. Computers and Intractability: A Guide to the Theory of NP-Completeness. W. H. Freeman, 1979.
14. Lisa Nicklasson. On the hilbert series of ideals generated by generic forms // Communications in Algebra. 2016. No45(8). P.3390–3395.
15. Aviad Kipnis, Jacques Patarin, and Louis Goubin. Unbalanced oil and vinegar signature schemes // Jacques Stern, editor, Advances in Cryptology – EUROCRYPT '99. P. 206–222. Berlin, Heidelberg, 1999. Springer Berlin Heidelberg.
16. Enrico Thomae and Christopher Wolf. Solving underdetermined systems of multivariate quadratic equations revisited // Marc Fischlin, Johannes Buchmann, and Mark Manulis, editors, Public Key Cryptography – PKC 2012. P. 156 Berlin, Heidelberg, 1999. Springer Berlin Heidelberg. 171. Springer Berlin Heidelberg 012.
17. H. Furue, S. Nakamura, and T. Takagi. Improving Thomae-Wolf algorithm for solving underdetermined multivariate quadratic polynomial problem // J. H. Cheon and J.-P. Tillich, editors, PQcrypto 2021. LNCS. P. 65–78, Cham, 2021. Springer International Publishing.
18. Hiroki Furue and Tsuyoshi Takagi. Fast enumeration algorithm for multivariate polynomials over general finite fields // Cryptology ePrint Archive, Paper 2023/619, 2023. <https://eprint.iacr.org/2023/619>.

19. Emanuele Bellini, Rusydi H. Makarim, Carlo Sanna, and Javier A. Verbel. An estimator for the hardness of the MQ problem. In Lejla Batina and Joan Daemen, editors, Progress in Cryptology – AFRICACRYPT 2022 // 13th International Conference on Cryptology in Africa, AFRICACRYPT 2022, Fes, Morocco, July 18-20, 2022, Proceedings, Lecture Notes in Computer Science. P. 323–347. Springer Nature Switzerland, 2022.
20. Peter Schwabe and Bas Westerbaan. Solving binary MQ with grover’s algorithm // Claude Carlet, M. Anwar Hasan, and Vishal Saraswat, editors, Security, Privacy, and Applied Cryptography Engineering – 6th International Conference, SPACE 2016, Hyderabad, India, December 14-18, 2016, Proceedings, volume 10076 of Lecture Notes in Computer Science. P. 303–322. Springer, 2016.
21. Nicolas Aragon et al. RYDE specifications. NIST Computer Security Resource Center | CSRC. URL: <https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/ryde-spec-web.pdf>
22. Rahul Mishra, Bhupendra Singh, Radhakrishnan Delhibabu. Searching for S-boxes with better Diffusion using Evolutionary Algorithm. IACR Cryptology ePrint Archive. URL: <https://eprint.iacr.org/2023/353>

Надійшла до редколегії 20.10.2025

Відомості про авторів:

Тельнова Аліна Анатоліївна – Харківський національний університет імені В. Н. Каразіна, магістр кафедри кібербезпеки інформаційних систем, мереж і технологій, Україна; e-mail: telnova.alina@student.karazin.ua; ORCID: <https://orcid.org/0009-0001-3574-7425>

Грінченко Тетяна Олексіївна – канд. техн. наук, доцент, Харківський національний університет радіоелектроніки, доцент кафедри безпеки інформаційних технологій, Україна; e-mail: tetiana.grinenko@nure.ua; ORCID: <https://orcid.org/0000-0002-8251-8991>

Нарезний Олексій Павлович – канд. техн. наук, Харківський національний університет імені В.Н. Каразіна, доцент кафедри кібербезпеки інформаційних систем, мереж і технологій, Україна; e-mail: o.nariezhnii@karazin.ua; ORCID: <https://orcid.org/0000-0003-4321-0510>

Т.І. КОРОБЕЙНИКОВА, канд. техн. наук, Н.В. КРАВЧУК

ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ML-WAF ДЛЯ КЛАСИФІКАЦІЇ ТА БЛОКУВАННЯ ІН'ЄКЦІЙНИХ АТАК У КОНТЕЙНЕРИЗОВАНОМУ ВЕБ-СЕРЕДОВИЩІ

Вступ

Сучасні веб-ресурси та серверні системи функціонують у середовищах, що характеризуються високою динамікою змін, широким застосуванням мікросервісної архітектури, контейнеризації, оркестрації та хмарних обчислень [1–4]. Популяризація контейнерних технологій, зокрема Kubernetes, зумовила появу нових вимог до забезпечення кібербезпеки, особливо щодо захисту трафіку на рівні HTTP(S)-запитів. В умовах горизонтального масштабування, динамічного створення/знищення контейнерів та автоматизованого керування навантаженням традиційні методи захисту втрачають ефективність [5–8]. Одним із найбільш загрозливих і поширених класів атак у веб-середовищі залишаються ін'єкційні атаки: SQL Injection, Cross-Site Scripting та Command Injection. У таких умовах традиційні засоби виявлення атак, зокрема сигнатурні WAF-рішення, демонструють обмежену ефективність у протидії ін'єкційним атакам через їхню варіативність, контекстну залежність та можливість модифікації обхідними техніками [9–10].

Запропонована у поданому тексті інформаційна технологія забезпечує: високоточну класифікацію HTTP(S)-запитів; адаптивне прийняття рішень на основі ризику; низьку затримку обробки в режимі реального часу; автоматичне масштабування та самооновлення ML-моделі.

Метою роботи є розроблення та експериментальна оцінка адаптивної ML-орієнтованої інформаційної технології для класифікації та блокування ін'єкційних атак у контейнеризованих веб-системах, що забезпечує високоточне виявлення шкідливих HTTP(S)-запитів, низьку затримку обробки та підтримку самооновлення моделі в MLOps-конвеєрі.

1. Інформаційна технологія ML-WAF для класифікації та блокування ін'єкційних атак

Концептуальна модель визначає логічну структуру ІТ, ключові етапи обробки веб-запитів і взаємодію модулів у процесі виявлення та блокування ін'єкційних атак. Тоді конвеєр обробки задається композицією функцій

$$r_{out} = f_n \circ f_{n-1} \circ \dots \circ f_1(r_{in}), \quad (1)$$

де r_{in} – вхідний HTTP(S)-запит, f_i – функціональний обробник (TLS-термінація, ML-фільтр, маршрутизатор), r_{out} – відповідь після проходження всіх етапів обробки.

ML-компонента обчислює ризик

$$risk_score = g(x); \quad (2)$$

де x – ознаковий вектор, сформований за TF/IDF та збагаченими ознаками.

Реакція визначається порогами T_{mid} та T_{high} :

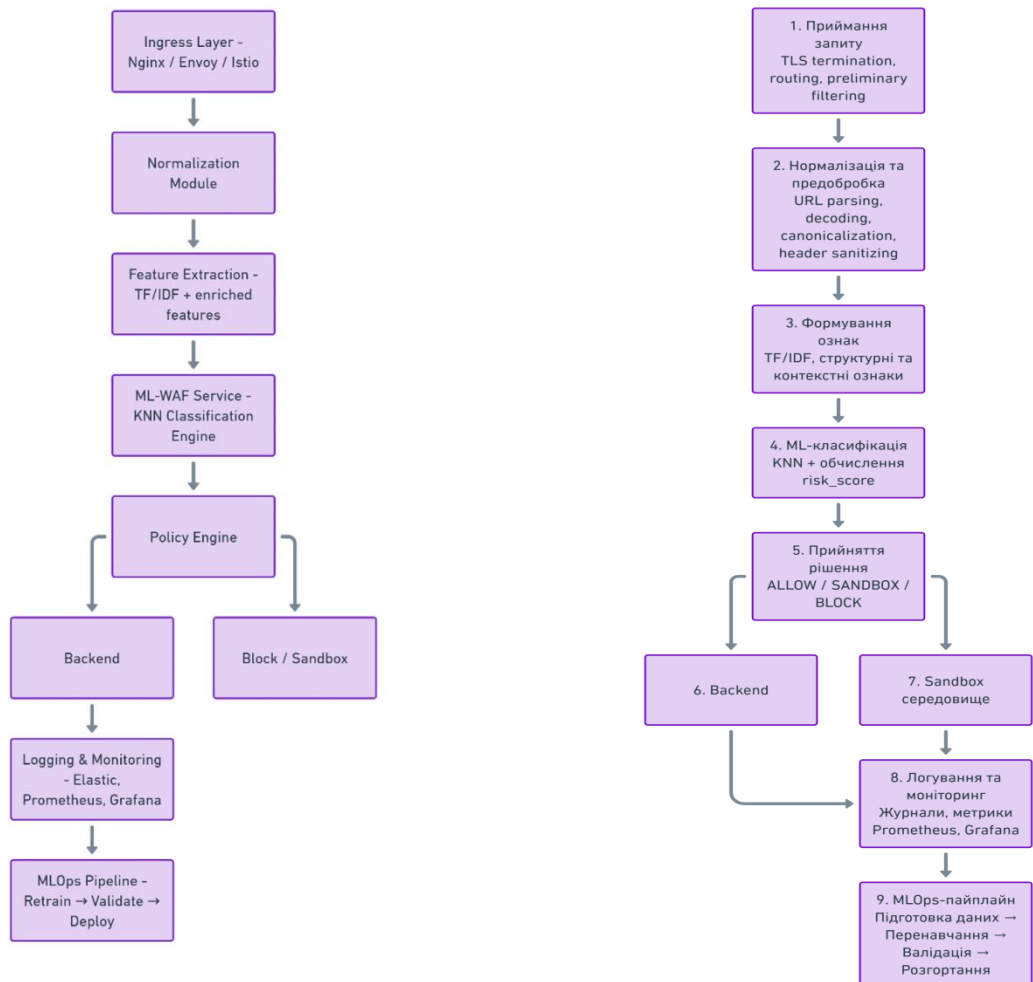
$$d = \begin{cases} ALLOW, & risk_score < T_{mid} \\ SANDBOX, & T_{mid} \leq risk_score < T_{high} \\ BLOCK, & highrisk_score \geq T_{high} \end{cases} \quad (3)$$

Ця політика є гнучкою та адаптується залежно від навантаження і контексту.

Структурна схема технології визначає логічно впорядковану сукупність модулів та підсистем, що реалізують функціональне наповнення механізму виявлення та блокування

ін'єкційних атак у контейнеризованому середовищі і демонструє горизонтально організований, модульний стек компонентів, які виконують послідовні етапи обробки запиту та генерують відповідні рішення щодо безпеки. Модульність забезпечує можливість незалежного масштабування та оновлення окремих компонентів, що є ключовою вимогою для Kubernetes-орієнтованих рішень. У верхній частині моделі (рис. 1, а) розташовано Ingress Layer, який відповідає за перехоплення, аналіз і первинну маршрутизацію трафіку. Normalization Module виконує лінгвістичну та структурну підготовку запиту. Наступні блоки формують ML-тракт: модуль витягання ознак та ML-WAF Service з KNN-класифікацією. Результати аналізу передаються до Policy Engine, який визначає остаточне рішення щодо обробки запиту. Нижня частина схеми відповідає за життєвий цикл рішення: обробка backend-додатком, фіксація інформації у журналах, передача метрик у систему моніторингу та участь у самооновленні моделі через MLOps Pipeline.

Функціональна схема відображає динамічну логіку роботи інформаційної технології, тобто спосіб, у який система змінює стан, передає дані та приймає рішення в реальному часі. На відміну від структурної схеми, що демонструє взаємне розташування компонентів, функціональна схема зосереджується на послідовності дій, тригерах переходів і функціональних обробниках, які формують повний сценарій обробки HTTP(S)-запиту. Як показано на рис. 1, б, робота технології складається з 9 функціональних етапів, що утворюють наскрізний конвеєр безпеки.



а – структурна схема технології

б – функціональна схема технології

Рис. 1. Моделі компонентів технології ML-WAF

Функціональна схема визначає як дані рухаються, які операції виконує система, коли і чому приймаються рішення, та які дані впливають на самооновлення моделі. Короткий опис етапів, що складають логіку роботи технології:

1) Приймання HTTP(S)-запиту. У процесі приймання запиту проводиться термінація TLS (за наявності), початкова валідація структури запиту, а також застосування базових правил безпеки, спрямованих на фільтрацію некоректних або очевидно шкідливих запитів.

2) Нормалізація та обробка запиту. Завдяки цьому формуються передбачувані, узгоджені текстові одиниці, які можуть бути оброблені модулями формування ознак.

3) Формування ознак (Feature Extraction). Система створює багатовимірний ознаковий опис запиту. На цьому кроці виконується TF/IDF-векторизація текстових компонентів. Сукупність TF/IDF-вектора та збагачених ознак створює комплексний ознаковий простір, що точно відображає як текстовий зміст запиту, так і його структурну форму.

4) Класифікація запиту ML-моделлю. Результатом класифікації є: визначений клас (наприклад: normal, SQLi, XSS, Command Injection); числова оцінка ризику (risk_score), яка показує ступінь небезпеки запиту.

5) Прийняття рішення (Policy Engine). На основі значення risk_score, отриманого від ML-модуля, Policy Engine порівнює його із порогами T_{mid} та T_{high} , які визначають межі між низьким, середнім та високим рівнями загрози. У залежності від співвідношення risk_score та порогів застосовується одне з трьох рішень: ALLOW – запит вважається безпечним та передається у backend; SANDBOX – запит є підозрілим, тому виконується у відокремленому середовищі або передається у додатковий модуль валідації; BLOCK – запит однозначно ідентифікується як атакуючий, і система повертає клієнту відповідь із заборonoю доступу (наприклад, HTTP 403).

6) Передача запиту у backend-додаток. Якщо прийняте рішення має тип ALLOW, запит потрапляє у backend-додаток або мікросервісну логіку, де виконується відповідна бізнес-функціональність. Таким чином, ML-WAF виступає фільтром між зовнішнім трафіком та ядром прикладної системи, захищаючи останню від шкідливого впливу.

7) Блокування або ізоляція (Sandbox Processing). Якщо активовано режим SANDBOX, запит надходить у спеціалізоване ізольоване середовище для безпечного виконання або детального аналізу.

8) Логування, журналювання та моніторинг. Формуються метрики продуктивності та стабільності, які передаються у Prometheus та візуалізуються за допомогою Grafana. Це забезпечує можливість: аналізу шкідливої активності; дослідження аномалій у трафіку; оцінки якості ML-моделі в режимі експлуатації.

9) MLOps-конвеєр адаптації моделі. Журнали та метрики передаються у модуль підготовки даних, де формуються нові вибірки для перенавчання моделі. Далі модель проходить процедури тренування, тестування, перевірки точності та CI/CD деплоймент у кластер Kubernetes. Це забезпечує безперервну адаптацію технології до нових варіантів атак та дає змогу підтримувати високий рівень захисту протягом всього життєвого циклу системи.

Інформаційно-логічна модель визначає структуру даних, їх взаємозв'язки та інформаційні потоки, що виникають у процесі функціонування інформаційної технології ML-WAF. На відміну від структурної та функціональної схем, які фокусуються відповідно на компонентній та процесній організації системи, інформаційно-логічна модель відображає сутності, інформаційні атрибути та логіку взаємодії даних, що забезпечують роботу механізмів виявлення атак, класифікації запитів, прийняття рішень і самооновлення моделі.

У межах інформаційної технології обробляються різні типи інформаційних об'єктів – від вихідних HTTP-запитів до ознакових векторів, класифікаційних результатів, рішень політик та ML-моделей. Сукупність таких сутностей та їх структурованих описів наведено у табл. 1.

Основні інформаційні сутності та їх атрибути

Сутність	Опис функціонального призначення та атрибутів
<i>HttpRequest</i>	Базова сутність, що містить method, URL, headers, body, IP-джерело, timestamp. Є вхідною одиницею всієї технології.
<i>NormalizedRequest</i>	Версія запиту після очищення та канонізації. Містить структуровані параметри, очищені заголовки, декодовані значення.
<i>FeatureVector</i>	Вектор ознак, що формується на основі TF/IDF-представлення та enriched-features: довжини, ентропії, структурних та контекстних ознак.
<i>MLModel (KNN)</i>	Містить k, набір тренувальних векторів, метрику відстані, версію моделі. Забезпечує класифікацію та обчислення risk score.
<i>ClassificationResult</i>	Містить label (клас), risk_score, посилання на модель, версію моделі та часову мітку класифікації.
<i>Decision</i>	Описує реакцію Policy Engine: action $\in \{\text{ALLOW, SANDBOX, BLOCK}\}$, причину, рівень ризику, порівняння з порогами Tmid, Thigh.
<i>BackendResponse</i>	Інформаційний об'єкт, що представляє відповідь backend-додатка на безпечний запит або блокування при небезпеці.
<i>LogRecord</i>	Журнал дій: запит, класифікація, рішення, час обробки, метрики, IP-джерело, версія моделі. Використовується SIEM або monitoring stack.
<i>MetricsRecord</i>	Значення latency, throughput, error rates, FPR/FNR. Забезпечує телеметрію та діагностику технічної роботи ML-WAF.
<i>TrainingDataset</i>	Сукупність FeatureVector та відповідних міток, сформованих на основі LogRecord і ручного аналізу фахівців.
<i>RetrainedMLModel</i>	Нова версія ML-моделі, що проходить валідацію (F1) та деплоймент через MLOps.

Початковою сутністю, яка ініціює усі інформаційні процеси, є *HttpRequest* – вхідний HTTP(S)-запит, що містить усю первинну інформацію від клієнта. Після проходження етапу нормалізації формується *NormalizedRequest*, який є стандартизованою версією початкових даних і виступає основою для побудови ознакового простору. Така нормалізація усуває обфускації, що дозволяє гарантувати коректність подальшого машинного аналізу.

На наступному етапі формується *FeatureVector*, який складається з кількох груп ознак: текстових TF/IDF-компонентів, структурних ознак (наприклад, кількість параметрів, довжина запиту, ентропія), а також контекстних характеристик, що відображають схожість до шкідливих шаблонів. Цей комплекс ознак передається до ML-модуля, де використовується *MLModel (KNN)*. Модель містить тренувальні вектори та правила визначення найближчих сусідів, що забезпечує класифікацію.

Результатом роботи моделі є сутність *ClassificationResult*, яка включає клас запиту та обчислений risk_score – числову характеристику небезпечності. На цій основі Policy Engine формує сутність *Decision*, яка визначає реакцію: пропуск, блокування або ізоляцію запиту. Надалі *Decision* впливає на формування *BackendResponse*, яка може бути як повноправною відповіддю backend-сервісу, так і повідомленням про блокування.

Для забезпечення повного контролю безпеки та можливості аудиту кожна операція фіксується у вигляді сутності *LogRecord*. Вона включає як власне результат класифікації та рішення, так і додаткові метрики. Зібрані журнали формують основу для побудови *TrainingDataset*, який використовується у MLOps-конвеєрі для створення нових версій моделі (*RetrainedMLModel*). Під час експлуатації всі технічні й обчислювальні параметри передаються у сутність *MetricsRecord*, що містить телеметричну інформацію про роботу системи. Логічні зв'язки між сутностями подано на рис. 2.

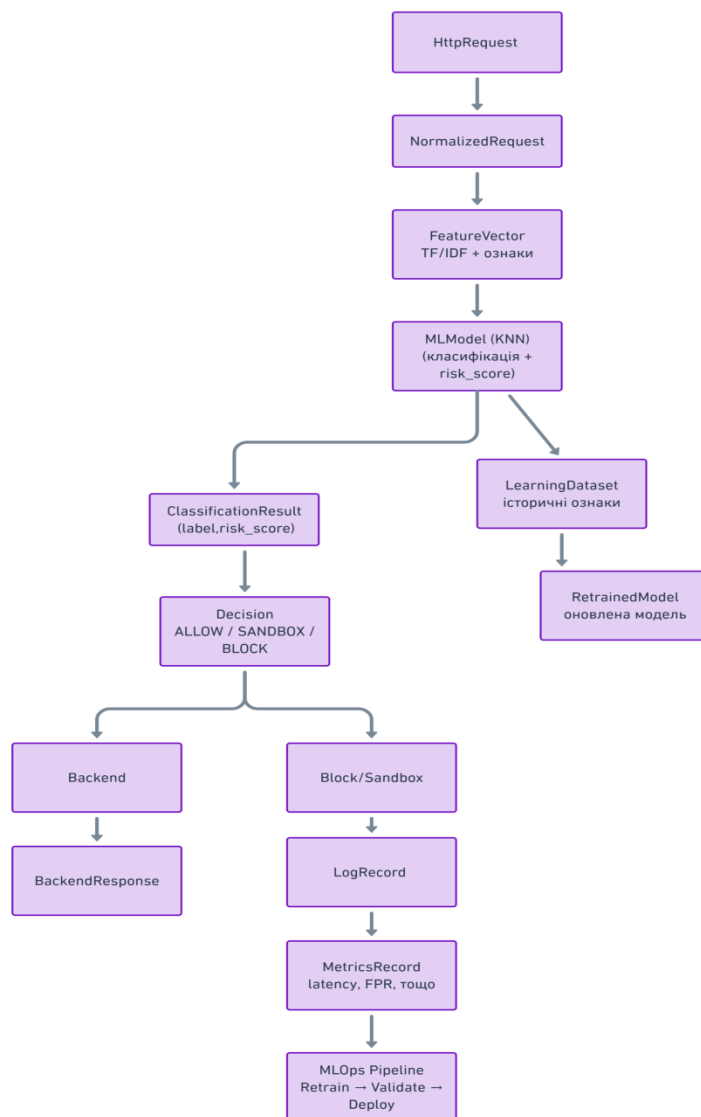


Рис. 2. Інформаційно-логічна схема технології ML-WAF

2. UML-представлення інформаційної технології ML-WAF

UML-моделі забезпечують формальне представлення структури, поведінки та взаємодії компонентів інформаційної технології ML-WAF. На відміну від концептуальних і структурних схем, UML-діаграми подають систему у стандартизованій, незалежній від реалізації формі, що дозволяє аналізувати її архітектуру, функціональність і комунікацію між підсистемами.

Для опису технології ML-WAF використано чотири ключові UML-діаграми: Use Case, Activity, Class та Sequence, кожна з яких відображає різний аспект системи. Їх текстові форми подані на рис. 4–6.

Use Case-модель (рис. 3) описує взаємодію основних користувачів та зовнішніх акторів із системою ML-WAF. Вона визначає, які саме функції надає технологія та які ролі впливають на процес виявлення атак, управління моделлю та експлуатаційний контроль.

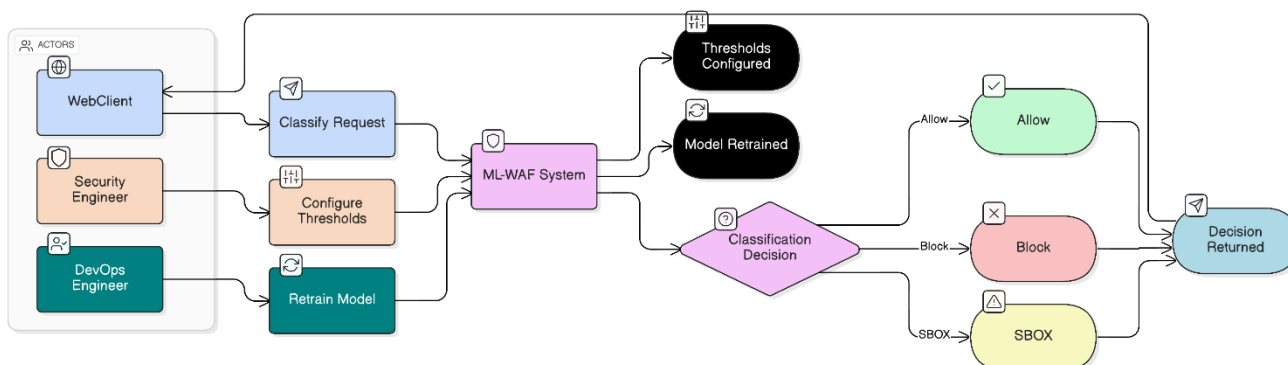


Рис. 3. UML Use Case для ML-WAF

У технології ML-WAF передбачено три ключові актори:

- 1) WebClient, який генерує HTTP-запити й опосередковано взаємодіє з процесом класифікації;
- 2) SecurityEngineer, що відповідає за налаштування порогів Tmid та Thigh, аналіз журналів, зміни політик безпеки; а) структурна схема технології
- 3) DevOpsEngineer, який контролює MLOps-процеси, розгортання моделей і CI/CD конвеєри.

Кожний актор виконує свій набір функцій, що забезпечує розмежування відповідальностей між безпекою та експлуатацією системи.

Activity-діаграма (рис. 4, а) відображає послідовність дій при обробці HTTP-запиту. Вона формалізує логіку виконання операцій у ML-WAF, описуючи динаміку системи з моменту надходження запиту до формування рішення та його документування. Ця діаграма фіксує логіку переходів між станами під час обробки одного запиту. Вона показує:

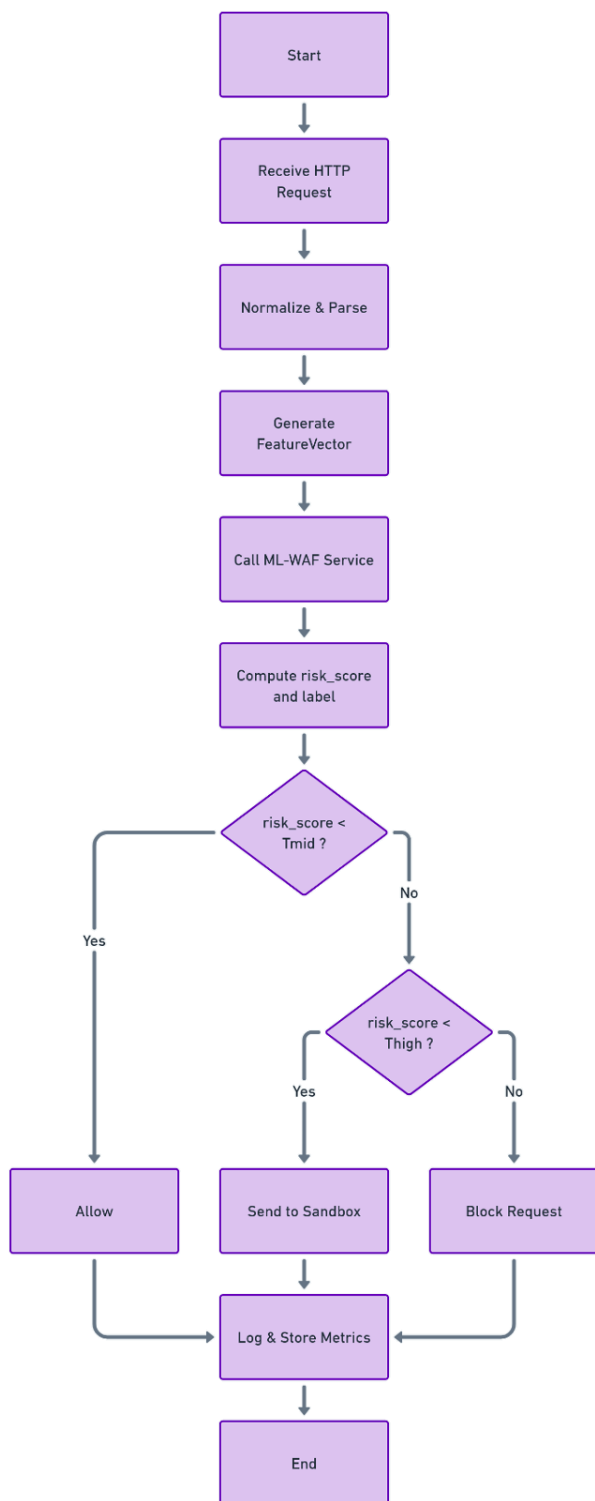
- фундаментальний взаємозв'язок між risk_score та рішенням Policy Engine;
- роль ML-класифікації як центрального етапу;
- паралельність процесів логування та моніторингу;
- три можливі траєкторії виконання (Allow, Sandbox, Block);
- завершення циклу після документування результату.

Class-діаграма (рис. 6) описує статичну структуру системи, її програмні сутності та атрибути, а також методи та зв'язки між класами. На відміну від інформаційно-логічної моделі, UML Class Diagram подає дані в контексті програмної реалізації.

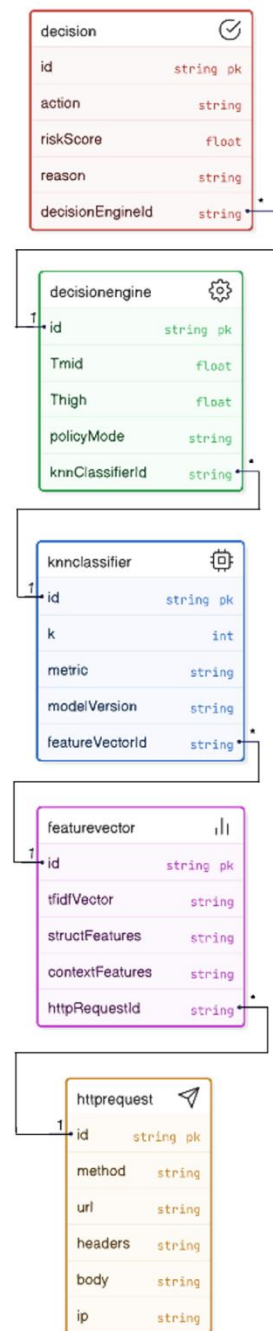
Class-модель описує логіку модульності ML-WAF:

- HttpRequest містить сирі дані, що підлягають обробці;
- FeatureVector формує структуроване математичне представлення запиту;
- KnnClassifier реалізує обчислення схожості та визначення risk_score;
- DecisionEngine відповідає за інтерпретацію результатів ML-класу;
- Decision є фінальною сутністю, що зберігає деталі рішення.

У сукупності класи формують ядро програмної логіки ML-WAF (рис. 4, б).



a – Activity-діаграма обробки запиту



b – Class-діаграма ML-WAF

Рис. 4. Діаграми компонентів технології ML-WAF

UML Sequence діаграма технології ML-WAF наведена на рис. 5.

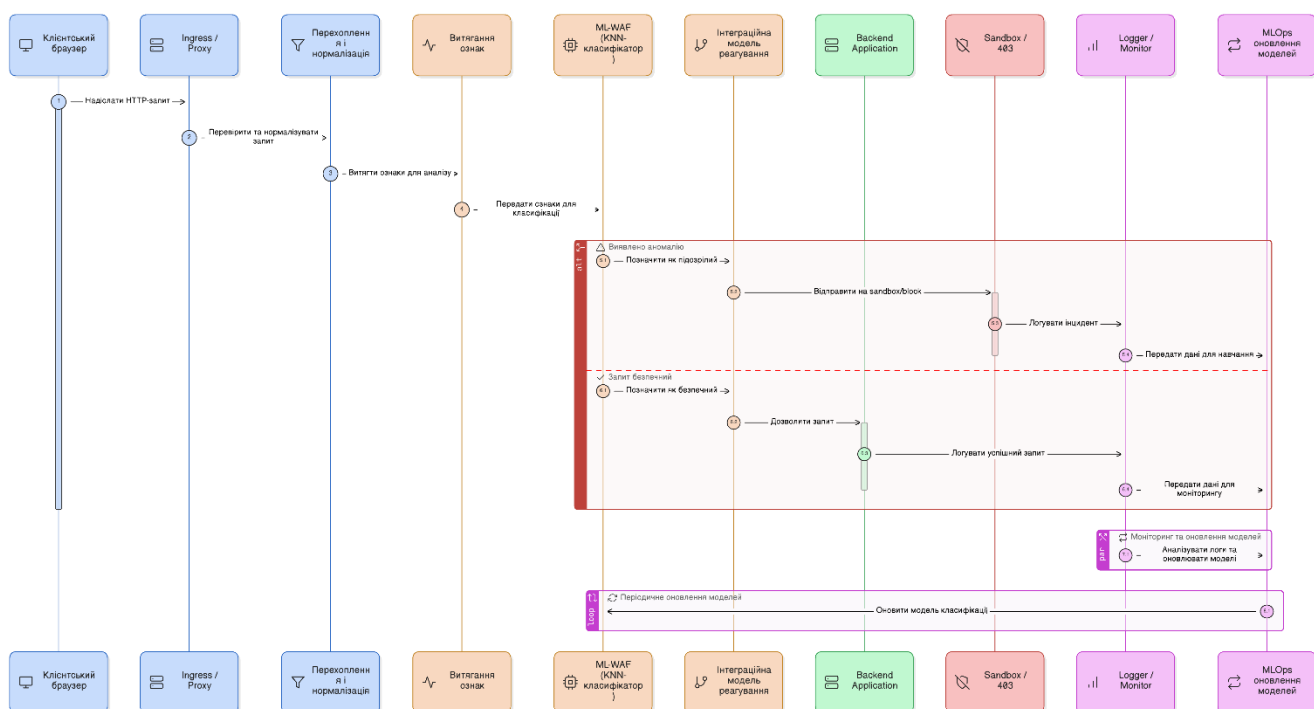


Рис. 5. UML Class діаграма ML-WAF

Sequence-модель подає часову послідовність викликів між компонентами. На відміну від Activity-діаграми, вона демонструє саме взаємодію між об'єктами.

3. Архітектурна схема інтеграції ML-WAF у середовище Kubernetes

Розгортання запропонованої ML-моделі виявлення і блокування небезпечних запитів у хмарному середовищі вимагає побудови чіткої архітектурної схеми взаємодії компонентів. Згідно з підходом Rathore та Park, ефективна інтеграція в Kubernetes має враховувати не лише логіку обробки трафіку, а й елементи спостережуваності, масштабування та оновлення моделі без зупинки сервісу.

Архітектура ML-WAF складається з наступних базових компонентів:

- Ingress Controller – приймає вхідні HTTP(S)-запити та здійснює їх первинну маршрутизацію;
- ML-WAF Service – мікросервіс, що реалізує модель класифікації (KNN+TF/IDF з ознаковим збагаченням) та повертає оцінку ризику r_i ;
- Backend Application – прикладна логіка користувача (система SCADA, інформаційний портал тощо);
- Monitor та Logger – модуль моніторингу та журналювання (на базі Prometheus та Elasticsearch);
- ConfigMap та Secrets – сховище конфігурацій порогів th , tm та API-ключів.

Потік запитів описується як композиція функцій:

$$R_{resp} = B(M(f_{ing}(R_{in}))), \quad (4)$$

де R_{in} – вхідний запит, f_{ing} – Ingress-фільтр (Nginx/Envoy), $M()$ – виклик ML-WAF модуля, $B()$ – бекенд-обробник.

Якщо $M()$ повертає $r_i \geq th$, запит не передається далі. Для масштабування ML-WAF у кластері використовується автоматичне збалансування навантаження на основі Horizontal Pod Autoscaler (HPA). Формально потужність кластеру визначається як

$$C_{eff} = \sum_{k=1}^n \frac{Q_k}{L_k}, \quad (5)$$

де Q_k – середня кількість оброблених запитів на Pod, а L_k – атримка (латентність). Згідно з дослідженням [11] динамічне масштабування НРА дозволяє підвищити пропускну здатність WAF на 35–40 % без збільшення затримки. Архітектурна схема роботи рішення зображена на рис. 6.

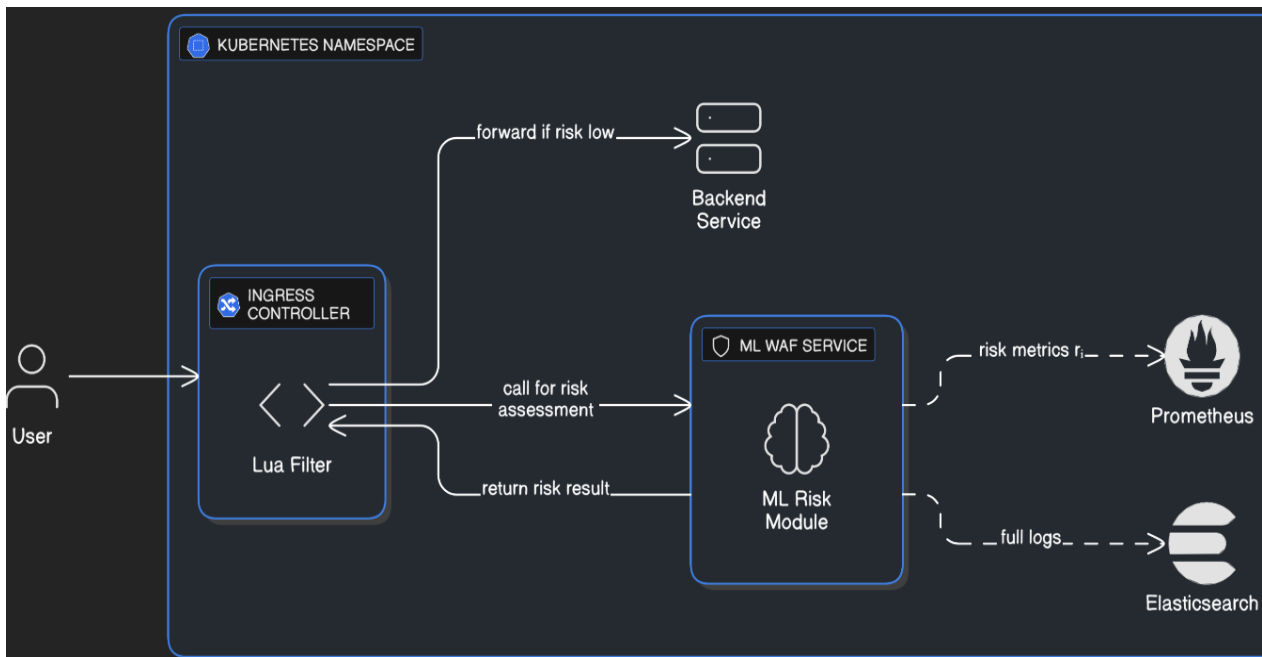


Рис. 6. Логічна архітектура системи машинного веб-фільтра (ML-WAF)

Якщо CPU перевищує порогове значення, НРА створює додаткові Pod, що гарантує стійкість до пікових навантажень. Дослідження [12] демонструє, що таке комбінування ML-WAF з НРА та Prometheus Exporter забезпечує автоматичну адаптацію системи до змінного трафіку та зменшує частку втрат запитів до 2 %.

4. Практична оцінка інтегрованої системи ML-WAF

Для підтвердження ефективності запропонованої архітектури ML-WAF проведено експериментальну оцінку роботи системи в умовах, наближених до реального середовища. Метою випробувань було визначити точність класифікації запитів, вплив інтеграції ML-модуля на продуктивність серверного конвеєра, а також порівняти результати з традиційними WAF-рішеннями.

Опис експериментального середовища. Випробування виконувалися у контейнеризованій інфраструктурі Kubernetes з двома вузлами, розгорнутими у Windows WSL2. Конфігурація середовища:

- Ingress Controller: Nginx 1.25 із Lua API;
- ML-компонента: KNN+TF/IDF з ознаковим збагаченням, реалізована на Flask 3.0;
- підсистема моніторингу: Prometheus + Grafana;
- набір даних: SQLi та XSS-запити з відкритих джерел (OWASP WebGoat, DVWA);
- сценарій тестування: 30 000 HTTP-запитів, з яких 30 % – шкідливі.

Тестування проводилося за допомогою утиліти Apache JMeter із 200 паралельними потоками. Замірювалися: середня затримка (ms), пропускну здатність (req/s), точність (precision), повнота (recall) та інтегральний показник F_1 .

Порівняння ефективності ML-WAF з традиційними рішеннями

Система	Precision	Recall	F ₁ -score	Latency (мс)	Пропускна здатність (req/s)
ModSecurity (OWASP CRS)	0.84	0.79	0.81	3.2	720
Snort + Reverse Proxy	0.88	0.82	0.85	4.1	680
ML-WAF (запропонована модель)	0.93	0.91	0.92	3.7	705
ML-WAF (з адаптацією порогів)	0.95	0.93	0.94	3.9	698

Результати свідчать, що інтегрована ML-модель забезпечує на 10–15 % вищу точність виявлення порівняно з сигнатурними системами, зберігаючи прийнятну продуктивність. Під час тестів із високим навантаженням (до 800 запитів/с) спостерігалось незначне зростання затримки, проте середній показник latency не перевищував 4 мс, що є прийнятним для більшості веб-додатків реального часу. У ході додаткових експериментів оцінено кількість хибнопозитивних спрацьовувань – для ML-WAF цей показник склав 2,3 %, тоді як у ModSecurity – 6,8 %.

Як показують дослідження [13], значення FP нижче 3 % вважається відмінним для промислових систем кіберзахисту. Важливим результатом також стало підтвердження масштабованості системи. При збільшенні кількості Pod до шести (через HPA) пропускна здатність зросла на 27 %, без зниження точності класифікації. Подібні результати продемонстровані [14], які відзначають, що контейнеризація ML-компонентів у WAF підвищує стійкість системи до DDoS-навантажень і спрощує горизонтальне масштабування.

Висновки

Представлено результати комплексного дослідження та розроблення адаптивної інформаційної технології ML-WAF, орієнтованої на класифікацію та блокування ін'єкційних атак у контейнеризованому веб-середовищі. Запропонована технологія охоплює всі ключові етапи життєвого циклу безпечної обробки HTTP(S)-трафіку – від перехоплення запиту до прийняття рішення, логування, моніторингу та безперервного оновлення ML-моделі. Побудовано концептуальну, структурну, функціональну та інформаційно-логічну моделі ML-WAF, а також UML-представлення, що формалізують архітектуру, поведінку та взаємодію компонентів у Kubernetes-орієнтованому середовищі.

Наукова новизна отриманих результатів полягає в такому. Вперше побудовано інтегровану інформаційну технологію ML-WAF для класифікації та блокування ін'єкційних атак у контейнеризованому веб-середовищі, що включає повний конвеєр HTTP(S)-обробки, модуль машинного навчання, багаторівневу адаптивну політику реагування, систему журналювання, моніторинг телеметрії та MLOps-процеси безперервного перенавчання моделі. Сформовано комплексну інформаційно-логічну модель, яка описує взаємозв'язки між сутностями HttpRequest, FeatureVector, ClassificationResult, Decision, LogRecord, MetricsRecord, TrainingDataset та RetrainedMLModel і відображає повний цикл еволюції моделі в умовах контейнеризованої інфраструктури. Запропоновано метод інтеграції ML-компоненти у WAF у гібридному режимі реагування (поєднання inline- та out-of-band-підходів), що забезпечує одночасно низьку латентність і підвищену стійкість до атак. Розроблено адаптивну модель прийняття рішень на основі risk_score з трирівневою реакцією (ALLOW, SANDBOX, BLOCK) та можливістю налаштування порогів з урахуванням навантаження і контексту трафіку.

Експериментальна оцінка підтвердила високу ефективність розробленої технології ML-WAF. На реалістичному наборі даних було досягнуто такі показники якості: точність (Precision) – 0,95, повнота (Recall) – 0,93, інтегральний F₁-score – 0,94. Середня затримка обробки одного запиту склала 3,9 мс, а пропускна здатність системи – близько 700 запитів/с. Важливим результатом є суттєве зниження частки хибнопозитивних спрацьовувань до 2,3 %, що майже утричі менше порівняно з ModSecurity (6,8 %). Після адаптивного перенавчання

моделі спостерігалось підвищення стійкості до нових варіантів атак і стабілізація показників якості при зростанні навантаження, що підтверджує ефективність запропонованого MLOps-підходу та масштабованість системи у контейнеризованих середовищах.

Отримані результати засвідчують, що розроблена інформаційна технологія ML-WAF здатна суттєво підвищити рівень захисту веб-систем від ін'єкційних атак, забезпечуючи високу точність класифікації запитів, низьку оперативну затримку та здатність до самоадаптації в динамічних хмарних інфраструктурах на базі Kubernetes. Це створює основу для подальшого розвитку систем проактивної кібербезпеки, зокрема шляхом інтеграції глибоких моделей (LSTM, BERT) і побудови повноцінних AI-керованих шлюзів безпеки наступного покоління.

Список літератури:

1. Терейковський І. А., Гнатюк С. О. Захист інформації в комп'ютерних системах : навч. посіб. Київ : КПІ, 2022.
2. Захарченко С. М., Трояновська Т. І., Бойко О. В. Побудова захищених мереж на базі обладнання компанії Cisco : навч. посіб. Вінниця : ВНТУ, 2017.
3. Коробейнікова Т. І., Захарченко С. М. Технології захисту локальних мереж на основі обладнання CISCO : навч. посіб. Львів : Львівська політехніка, 2021.
4. Korobeinikova T., Maidaniuk V., Romanyuk O., Chekhmestruk R., Romanyuk O. and Romanyuk S. Web-applications Fault Tolerance and Autoscaling Provided by the Combined Method of Databases Scaling // 2022 12th International Conference on Advanced Computer Information Technologies (ACIT). 2022. P. 27–32. doi: 10.1109/ACIT54803.2022.9913098.
5. Korobeinikova T. and Kravchuk N. ML-trained model and method for blocking dangerous queries // CEUR Workshop Proceedings. 2025. Vol. 4042 // Proceedings of the Cyber Security and Data Protection workshop (CSDP 2025), Lviv, Ukraine, July 31, 2025. P. 1–16.
6. Коробейнікова Т. І., Кравчук Н. В. Огляд безпечного доступу до веб-ресурсу за допомогою методів машинного навчання // International Scientific Integration 2023: Міжнар. наук. конф., 11 липня 2023 р.: тези доповідей. С. 26–33. Seattle, Washington, USA: ProConference, 2023.
7. Кравчук Н., Коробейнікова Т. Безпечний доступ до серверів інформаційних систем, забезпечений ML-моделлю для блокування шкідливих запитів // Herald of Khmelnytskyi National University. Technical Sciences. 2024. № 341(5). С. 327–333.
8. Korobeinikova T., Chekhmestruk R., Mykhaylov P., Romanyuk O., and Achanyar H. The Fault-Resistant Web Application Infrastructure Using Autoscaling // 2023 13th International Conference on Advanced Computer Information Technologies (ACIT), Wrocław, Poland, 2023. P. 479–482, doi: 10.1109/ACIT58437.2023.10275448
9. Bennouk K., Ait Aali N., El Bouzekri El Idrissi Y., Sebai B., Faroukhi A. Z., Mahouachi D. A Comprehensive Review and Assessment of Cybersecurity Vulnerability157 Detection Methodologies // Journal of Cybersecurity and Privacy. 2024. Vol. 4, No. 4. P. 853–908.
10. Wunder J., Kurtz A., Eichenmüller C., Gassmann F., Benenson Z. Shedding Light on CVSS Scoring Inconsistencies: A User-Centric Study on Evaluating Widespread Security Vulnerabilities // Proceedings of the 2024 IEEE Symposium on Security and Privacy (SP). San Francisco, CA, USA, 2024. P. 1102–1121.
11. Liang S., Wang Q. Dynamic Scaling of Containerized Security Services with HPA Policies // Future Internet. 2023. Vol. 15, No. 3. P. 88–102.
12. Palanisamy D., Kaur R. Adaptive Resource Management for AI-Driven WAF in Cloud Kubernetes Clusters // Journal of Cloud Computing: Advances, Systems and Applications. 2023. Vol. 12, No. 1. P. 1–17.
13. Wang X., Lyu C. Performance Evaluation Metrics for ML-Based Web Application Firewalls // IEEE Access. 2022. Vol. 10. P. 98451–98463.
14. Rahman M., Qiu Y. Containerized Intrusion Detection and Response in Cloud-Native WAF Systems // Journal of Network and Computer Applications. 2023. Vol. 216. P. 103670.

Надійшла до редколегії 12.10.2025

Відомості про авторів:

Коробейнікова Тетяна Іванівна – канд. техн. наук, Національний університет «Львівська політехніка», доцент кафедри безпеки інформаційних технологій, Україна; e-mail: tetianakorobeinikova@gmail.com; ORCID: <https://orcid.org/0000-0003-2487-8742>

Кравчук Назар Вікторович – Національний університет «Львівська політехніка», аспірант кафедри безпеки інформаційних технологій Україна; e-mail: nazar.v.kravchuk@lpnu.ua; ORCID: <https://orcid.org/0009-0002-1008-4765>

*М.О. ЄВДОКИМЕНКО, д-р техн. наук, В.Х. ЧАКРЯН, канд. техн. наук,
В.В. ЄВДОКИМЕНКО*

ЕТИЧНІ ЗАСАДИ ТА НОРМАТИВНЕ РЕГУЛЮВАННЯ ПРОФЕСІЙНОЇ ДІЯЛЬНОСТІ В СФЕРІ КІБЕРБЕЗПЕКИ: МІЖНАРОДНІ СТАНДАРТИ, УКРАЇНСЬКИЙ КОНТЕКСТ І ПРАКТИЧНІ ОРІЄНТИРИ

Вступ

У добу цифрової трансформації питання етики в сфері кібербезпеки набуває особливої актуальності. Зі зростанням залежності суспільства від інформаційних технологій, відповідальність за їхній захист стає не лише технічною, але й моральною проблемою. Кожен інцидент порушення конфіденційності, витоку даних чи неправомірного моніторингу викликає резонанс не лише в професійному середовищі, але й у суспільстві в цілому. Кібербезпека більше не обмежується шифруванням, фаєрволами чи реагуванням на інциденти – вона – вимагає етичної свідомості та стратегічного мислення.

Особливої ваги це набуває у сферах, де обробляються критично чутливі дані: охорона здоров'я, фінанси, енергетика, освіта. У подібних випадках від дій спеціаліста з кібербезпеки залежить не лише цілісність інформації, а й добробут, права і навіть життя людей. Професійна етика тут визначає межу між захистом і порушенням приватності.

Крім того, із впровадженням концепцій “Zero Trust”, “Data Sovereignty”, “Digital Identity” тощо, фахівець з кібербезпеки все частіше виступає не просто адміністратором системи, а агентом впливу на політику конфіденційності, прозорості та управління цифровими ризиками. Саме тому питання етики має розглядатися як фундаментальний елемент професійної компетентності, поряд із технічними знаннями.

Складність етичних дилем також зумовлюється багатоаспектністю ситуацій: від легітимності соціальної інженерії в тестуванні до повідомлення про вразливості в умовах національної безпеки. У таких випадках не існує однозначно правильного рішення без врахування правової, технічної та етичної площин.

Водночас нормативно-правове забезпечення діяльності у сфері кібербезпеки ще не завжди враховує динамічні зміни цифрового середовища. Багато міжнародних стандартів – таких як ISO/IEC 27001 [1], ISO/IEC 27032 [2] – лише окреслюють загальні рамки поведінки, залишаючи багато етичних питань відкритими для тлумачення.

Україна, яка стрімко впроваджує європейські принципи цифрової безпеки та прагне до кіберстійкості, потребує формування зрозумілої етичної моделі для підготовки професіоналів. Ця модель має включати як елементи права, так і м'які навички прийняття рішень у умовах невизначеності.

Таким чином, актуальність дослідження етичних засад діяльності у сфері кібербезпеки зумовлена необхідністю формування довіри до цифрової екосистеми, запобігання зловживанням владними повноваженнями фахівців, та забезпечення балансу між безпекою і правами людини.

Це дослідження спрямоване на систематизацію ключових етичних проблем, аналіз нормативної бази та розробку практичних орієнтирів для майбутніх фахівців. Його результати можуть бути використані у навчальному процесі, при підготовці політик інформаційної безпеки та у міждисциплінарних дослідженнях кіберетики.

Етичні основи професійної діяльності

Робота фахівця з кібербезпеки вимагає постійного балансу між захистом цифрових активів та дотриманням прав і свобод людини. У цифрову епоху, коли приватна інформація може бути зібрана, оброблена, збережена або скомпрометована за лічені секунди, етична

відповідальність спеціаліста виходить далеко за рамки технічної компетентності. Це зобов'язання перед суспільством, роботодавцем, клієнтами та самою професією.

Основні етичні принципи, що мають бути дотримані в професійній діяльності фахівця з кібербезпеки, представлені на рис. 1.

Конфіденційність	Цілісність	Підзвітність	Справедливість
Зобов'язання зберігати інформацію, до якої є доступ, в таємниці, не допускаючи її розголошення без дозволу.	Вимога діяти чесно, не спотворюючи інформацію та не маніпулюючи результатами.	Готовність пояснити свої дії і не перекладати відповідальність на інших.	Рівне ставлення до всіх користувачів та недопущення упередженості, дискримінації чи зловживань.

Рис. 1. Основні етичні принципи

На практиці ці принципи мають бути вбудовані в щоденну діяльність: від аналізу журналів подій до роботи з персональними даними користувачів. Наприклад, навіть якщо фахівець з кібербезпеки має технічну можливість доступу до приватної інформації (медичної документації, листування працівників, історії фінансових транзакцій тощо), він не має морального права використовувати ці знання поза межами своєї функції.

У відповідь на потребу в етичній регуляції в сфері ІТ та кібербезпеки, провідні професійні організації розробили відповідні кодекси поведінки.

Одним із найвпливовіших є (ISC)² Code of Ethics [3], який базується на чотирьох основних канонах:

1. Захищати суспільство, загальне благо, довіру та інфраструктуру.
2. Чесно виконувати свої обов'язки та діяти у найкращих інтересах клієнта.
3. Забезпечувати чесну та законну поведінку у професійній діяльності.
4. Підтримувати та вдосконалювати свою професійну компетентність.

Кожен сертифікований спеціаліст (наприклад, власник сертифіката CISSP) зобов'язаний неухильно дотримуватись цього кодексу. Його порушення може призвести до дисциплінарного розгляду і навіть втрати сертифікату.

Іншим авторитетним джерелом є ACM Code of Ethics and Professional Conduct [4], прийнятий Асоціацією обчислювальної техніки (Association for Computing Machinery). Він базується на таких принципах:

- діяти на благо суспільства і людства;
- уникати заподіяння шкоди;
- бути чесним і прозорим;
- поважати конфіденційність та приватність інших осіб;
- покращувати технічну компетентність і відповідати за свою діяльність.

ACM Code of Ethics передбачає як загальні моральні принципи, так і специфічні вказівки для фахівців у галузі розробки ПЗ, інформаційних систем та кібербезпеки. Наприклад, в ньому наголошується, що спеціалісти повинні уникати будь-якої діяльності, яка може завдати шкоди іншим, навіть якщо вона не є прямо забороненою законом.

Проте, попри наявність таких кодексів, у сфері кібербезпеки залишається чимало сірих зон. Зокрема, відсутність універсального міжнародного стандарту етики призводить до неоднозначного трактування ролі спеціаліста в умовах кібервійни, кіберспостереження чи роботи у приватному секторі. Також бракує чітких механізмів моніторингу та контролю етичної поведінки в професійній спільноті.

У зв'язку з цим, важливо не лише популяризувати наявні етичні кодекси, а й інтегрувати етику в системи підготовки фахівців, внутрішні політики компаній і процедури оцінки діяльності. Це дозволить зробити етику невід'ємною частиною цифрової безпеки, а не формальною декларацією.

Таким чином, етичні основи є не лише засадничою складовою професійної репутації, а й фактором підвищення стійкості кіберпростору в цілому.

Відповідальність і цифрова довіра

Цифрова довіра (digital trust) є фундаментальним елементом у сфері кібербезпеки, яка дедалі більше впливає на економічну, правову та соціальну стабільність сучасного інформаційного суспільства. Без належного рівня довіри жодна система не може функціонувати ефективно – ані технологічна, ані організаційна. Відповідальність фахівця з кібербезпеки охоплює не лише захист систем і даних, а й забезпечення прозорості, правомірності та етичності в кожній операції, пов'язаній із цифровими активами.

Центральним концептом, що лежить в основі цифрової довіри, є "надійна поведінка" (trustworthy behavior), яка поєднує правову відповідальність, професійну етику та дотримання міжнародних стандартів (наприклад, ISO/IEC 27001, ISO/IEC 27701). Принципи прозорості, достовірності, відповідальності (accountability), доступності, конфіденційності та мінімізації втручання формують основу цифрової довіри в контексті діяльності як окремого фахівця, так і організації загалом.

Один із ключових аспектів відповідальності полягає у своєчасному розкритті інцидентів. Замовчування зламів або компрометацій є серйозним етичним і правовим порушенням, що прямо шкодить довірі з боку клієнтів, партнерів та держави. Прикладом стала ситуація з Uber у 2016 р., коли компанія приховала факт витоку персональних даних понад 57 мільйонів користувачів і водіїв, заплативши хакерам за мовчання. Це порушення як законодавства з питань захисту персональних даних, так і фундаментальних етичних норм взаємодії з користувачами.

Концепція цифрової довіри передбачає також впровадження політики "ethics by design" – тобто закладення етичних принципів безпосередньо в архітектуру ІТ-рішень, алгоритмів та інтерфейсів взаємодії. Це означає не лише створення безпечного продукту, але і такого, що враховує приватність користувача, справедливий розподіл повноважень, і відсутність дискримінаційних моделей доступу чи контролю.

Іншим важливим підходом є "accountable cybersecurity" – концепція, згідно з якою кожен суб'єкт, залучений у процес управління безпекою, несе не лише технічну, але і юридичну відповідальність за прийняті рішення та їх наслідки. Такий підхід вимагає ведення чіткої документації, звітності, регулярного перегляду рішень та етичних аудитів (наприклад, шляхом впровадження внутрішніх кодексів поведінки, незалежних комітетів з етики та наглядових рад).

Не менш важливим є забезпечення відповідності принципам "data stewardship" – етичного управління даними, яке передбачає, що доступ до інформації здійснюється лише на основі чітко визначеної мети, з належними дозволами, із дотриманням принципу мінімізації збирання та обробки. Будь-яка маніпуляція з даними поза рамками призначення – наприклад, моніторинг листування працівників без юридичних підстав – прямо підриває цифрову довіру та порушує фундаментальні права особи.

Цифрова довіра також є предметом регуляторного нагляду. Наприклад, Загальний регламент захисту даних (GDPR) [5] вимагає обов'язкового повідомлення про витоки протягом 72 годин. Аналогічні вимоги включено у новітні директиви ЄС з кіберстійкості (наприклад, NIS 2 Directive) [6] та відповідні нормативні акти у США (як-от SEC Cybersecurity Rules) [7].

Слід також підкреслити роль культури відповідальності в організаціях. Етична поведінка не може бути забезпечена виключно технічними засобами – вона формується через інституційну культуру, де працівники отримують чіткі інструкції, навчання, мають канали для повідомлення про порушення без ризику репресій (whistleblowing policies), а також доступ до незалежного етичного консультанта.

Інноваційною концепцією є також впровадження довіри на основі блокчейн-рішень – auditability and transparency by design. Наприклад, зберігання логів подій у незмінному вигляді на блокчейні унеможливорює їх фальсифікацію та дозволяє здійснювати незалежну перевірку без компрометації джерела.

Крім того, актуальними залишаються питання відповідальності у випадку використання штучного інтелекту в безпеці: як бути, якщо рішення про блокування доступу було прийняте автоматичною системою, яка мала помилкові вхідні дані або містить упередженість у моделях? Це вимагає розробки чіткої процедури оскарження рішень (algorithmic accountability), які б дозволяли людині відновити свої права.

Отже, цифрова довіра не є абстрактним поняттям, а системою взаємопов'язаних етичних, правових та організаційних рішень, що впроваджуються в щоденну практику кіберзахисту. Вона вимагає усвідомлення відповідальності, постійного етичного рефлексування та розвитку систем внутрішнього контролю. Успішний фахівець з кібербезпеки має бути не лише технічно грамотним, а й морально відповідальним – здатним приймати рішення, які водночас захищають систему та поважають гідність особистості.

Саме тому, у контексті зростаючого значення цифрової довіри та професійної відповідальності особливого значення набуває нормативне закріплення етичних принципів у міжнародних та національних стандартах. Впровадження таких стандартів дозволяє формалізувати етичні вимоги до фахівців з кібербезпеки, забезпечити єдині правила взаємодії в цифровому середовищі, а також створити основу для механізмів оцінювання, сертифікації та нагляду за дотриманням професійної етики. Наступний розділ буде присвячено аналізу ключових етичних та професійних стандартів, прийнятих у США, ЄС та Україні, а також їх ролі у формуванні цифрової відповідальності в глобальному контексті.

Інституціональні та нормативні засади цифрової етики

У сучасному цифровому середовищі, де кіберзагрози набувають все більш витончених форм, а обсяг чутливих даних стрімко зростає, потреба в чітких нормативно-правових регулюваннях стає надзвичайно актуальною. Етика в галузі кібербезпеки не може залишатися суто моральною категорією – вона має отримати правову інституціоналізацію. З огляду на міждержавний характер Інтернету, важливо враховувати як національні законодавства, так і міжнародні стандарти, що встановлюють правила поведінки для фахівців з кібербезпеки. Особливо вагому роль у цьому контексті відіграють підходи Європейського Союзу та Сполучених Штатів Америки, які стали прикладами для впровадження етичних рамок на інституційному рівні. Ці стандарти визначають не лише технічні вимоги до безпеки, а й засади цифрової етики, відповідальності та прозорості. Вони мають імплементаційний вплив на організаційну культуру підприємств, освітні програми, державну політику у сфері цифрової трансформації. Дотримання таких норм є не лише показником професіоналізму, а й передумовою легітимності та суспільної довіри до цифрових рішень. У цьому розділі ми детально розглянемо, як побудована система етичних стандартів у ЄС та США, які принципи лежать в її основі та як вони реалізуються на практиці. Цей аналіз дозволяє виявити сильні сторони та потенційні напрями вдосконалення нормативно-правового поля в Україні з урахуванням кращих міжнародних практик.

Етичні стандарти та цифрова довіра: порівняльний аналіз підходів ЄС та США

Європейський Союз та Сполучені Штати Америки виступають провідними юрисдикціями у формуванні етичної інфраструктури для цифрового суспільства. Обидві системи враховують фундаментальні права людини, забезпечення цифрової довіри та відповідальність професійної спільноти.

В ЄС основною нормативною опорою для етичних принципів у цифровій сфері є Загальний регламент захисту даних (General Data Protection Regulation, GDPR), який встановлює високі стандарти прозорості, підзвітності та прав суб'єктів даних. Окрім суто правових вимог, GDPR формує культурний стандарт – розуміння, що обробка даних є не лише технічною, а й етичною дією. До регламенту додано принципи “privacy by design” та “privacy by default”, що змушують компанії закладати етичні підходи вже на етапі розробки продуктів.

Європейська комісія також ініціювала створення Етичних настанов зі штучного інтелекту (Ethics Guidelines for Trustworthy AI, 2019) [8], які визначають 7 ключових вимог до систем ШІ: зокрема, людський контроль, технічну надійність, конфіденційність та підзвітність. Ці настанови стали основою для майбутнього законодавства про AI Act.

Крім того, у рамках ініціативи Digital Europe та Cybersecurity Act, ЄС просуває ідею сертифікації спеціалістів і рішень, в яких етичні принципи становлять обов'язковий компонент [9]. Так, сертифікати відповідності вимагають не лише технічної безпеки, а й відповідності етичним нормам та доброчесності.

На рівні професійних об'єднань Європейський Союз підтримує розробку етичних кодексів для фахівців з кібербезпеки, наприклад, рекомендації ENISA (Агентство ЄС з кібербезпеки) щодо стандартів поведінки та рішень у сфері кіберризиків. ENISA підтримує створення стандартів на основі компетентностей та етики, включаючи рекомендації щодо кар'єрного шляху та етичного лідерства [10].

У США ключовим документом у сфері цифрової етики вважається ACM Code of Ethics and Professional Conduct (Кодекс етики та професійної поведінки Асоціації обчислювальної техніки), який зобов'язує спеціалістів діяти в інтересах суспільства, дотримуватись чесності, поважати конфіденційність і уникати шкоди. Кодекс є обов'язковим для всіх членів ACM і часто включається до навчальних програм з ІТ.

Ще один важливий документ – (ISC)² Code of Ethics, розроблений Міжнародним консорціумом сертифікованих спеціалістів з безпеки інформаційних систем. Цей кодекс чітко формулює чотири основні принципи: захист суспільства, чесність і справедливість, повага до довіри та обов'язок до розвитку знань. Він обов'язковий для всіх сертифікованих спеціалістів CISSP, SSCP, CCSP та інших.

У США також діє NIST Cybersecurity Framework [11], який не є кодексом етики, але включає положення щодо забезпечення відповідальності, прозорості та етичного управління ризиками. Рамка містить компоненти “Govern” та “Identify”, які стосуються етичної оцінки впливу технологій і обліку інтересів користувача.

Важливо відзначити, що американські компанії часто створюють внутрішні етичні комітети, особливо у великих корпораціях, які працюють з персональними даними або штучним інтелектом. Така практика вважається “best practice” в управлінні цифровими ризиками.

Таким чином, як ЄС, так і США демонструють багаторівневий підхід до етичного регулювання цифрового середовища – від загальних правових рамок до галузевих і професійних стандартів. Ці моделі є прикладом інтеграції етики в усі етапи життєвого циклу цифрових систем – від архітектурного дизайну до повсякденного використання. Україна, адаптуючи свої підходи до етичного врядування в ІКТ, може скористатися цими прикладами як основою для побудови власної національної системи цифрової етики.

Етичні норми та цифрова довіра в українському законодавстві

У контексті цифрової трансформації держави, побудови інформаційного суспільства та активної інтеграції у європейський кіберпростір, Україна поступово формує нормативно-правову базу, що включає етичні засади й принципи цифрової довіри. Хоча більшість українських законів не містять терміну “етика” у формальному визначенні, багато з них прямо чи опосередковано закладають фундамент етичної поведінки у сфері інформаційних технологій і кібербезпеки.

Закон України “Про національну безпеку” № 2469-VIII (2018) прямо визначає кібербезпеку як невід’ємну складову національної безпеки [12]. У Стратегії національної безпеки України акцент зроблено на необхідності формування культури довіри до цифрових сервісів і забезпечення захисту прав громадян у кіберпросторі.

Закон України “Про основні засади забезпечення кібербезпеки України” № 2163-VIII (2017) містить визначення кібербезпеки як стану захищеності кіберпростору та інтересів

особи, суспільства й держави [13]. У законі закладено принципи законності, пропорційності втручання, поваги до прав людини, конфіденційності та добросовісності, які відповідають етичним стандартам демократичних країн.

Закон України "Про захист персональних даних" № 2297-VI (2010, в останній редакції 2022 р.) є ключовим актом, що гарантує право на приватність [14]. Він встановлює підзвітність операторів персональних даних, принципи цільовості, пропорційності, обмеження строку зберігання даних, заборону на обробку чутливої інформації без згоди суб'єкта. Норма про обов'язок уповноваженої особи із захисту даних узгоджується з європейським підходом до етичного управління даними (GDPR).

Закон України "Про електронні комунікації" № 1089-IX (2020) встановлює правові засади діяльності провайдерів, у тому числі щодо захисту прав споживачів, прозорості умов надання послуг, а також контролю за ОТТ-сервісами (Over-the-top) [15]. Він містить положення про обов'язкове дотримання принципу недискримінації, забезпечення конфіденційності та безпеки електронних повідомлень.

Закон України "Про інформацію" № 2657-XII (1992, чинна редакція) визначає правові засади доступу, поширення, обробки інформації, зокрема принципи достовірності, відкритості, об'єктивності. Стаття 5 закріплює право на приватність і обов'язок не допускати порушення інформаційної безпеки [16]. Закон регламентує етичні аспекти обробки інформації, обмежуючи зловживання владою, пропаганду ворожнечі та втручання в особисте життя.

Закон України "Про електронні довірчі послуги" № 2155-VIII (2017) встановлює поняття довіри в цифровому середовищі через інституалізацію електронного підпису, електронної печатки, часових міток, сертифікації послуг [17]. В основі лежить принцип правової визначеності та цілісності інформації, що передбачає етичну відповідальність постачальників послуг перед користувачами.

Закон України "Про публічні електронні реєстри" № 2170-IX (2022) запроваджує стандарти надійності, прозорості та захисту даних у роботі державних інформаційних систем [18]. Закон визначає вимоги до забезпечення захисту персональної інформації в реєстрах та встановлює критерії етичного управління державними даними, зокрема щодо мінімізації збору, обмеження доступу та контролю на основі ризик-орієнтованого підходу.

Закон України "Про відкритість використання публічних коштів" № 183-VIII (2015) хоча і не стосується напряму ІКТ, але встановлює принципи прозорості, підзвітності та недопущення зловживань, що є базовими категоріями цифрової етики при адмініструванні електронних систем закупівель, бюджетного контролю тощо [19].

Законопроект "Про захист критичної інформаційної інфраструктури" (в процесі ухвалення) передбачає створення нормативних механізмів для управління ризиками, прозорого аудиту та відповідального поведіння з технологіями в об'єктах критичної інфраструктури [20].

Окрім законів підзаконні акти та стратегії, такі як "Національна стратегія з кібербезпеки України" (Указ Президента № 47/2021) [21], Стратегія цифрової трансформації сектору безпеки й оборони (2022) [22], програма "Дія.Цифрова держава", акти КМУ та Держспецзв'язку закріплюють засади етичного поведіння з даними, необхідність дотримання принципів "security by design" і "privacy by design".

Також Методичні рекомендації НАЗК щодо доброчесності у державному секторі прямо включають принципи прозорості, добросовісності, етичного врядування, що застосовні і до цифрових сервісів.

У сфері освіти, стандарти вищої освіти зі спеціальності "Кібербезпека" (галузь знань 12) затверджені МОН, містять компонент етичної поведінки та правових знань як обов'язкову складову професійної підготовки. Студенти повинні демонструвати здатність діяти етично в ситуаціях, пов'язаних з обробкою конфіденційної інформації, тестуванням безпеки та взаємодією з особистими даними.

На рівні професійних об'єднань, як-от IT Ukraine Association, ISACA Kyiv Chapter, Ukrainian Cyber Alliance, також діють ініціативи щодо розробки професійних стандартів поведінки, кодексів доброчесності, антикорупційних положень та норм захисту цифрових прав.

Отже, українське законодавство поступово формує системну етичну рамку для функціонування цифрового середовища, базуючись на таких принципах як прозорість, підзвітність, недискримінація, безпека і повага до прав людини. Проте відчутною є потреба в консолідації норм, прийнятті національного кодексу етики для кіберфахівців і гармонізації із міжнародними підходами. Наступним логічним кроком у цьому напрямку є формування етичних стандартів, які стали б обов'язковими в сертифікації, публічних закупівлях та акредитації цифрових послуг.

Перспективи гармонізації етичних та правових підходів України з моделями ЄС і США

В умовах стратегічного курсу України на євроінтеграцію та розвиток цифрової держави особливого значення набуває гармонізація національного правового поля з етичними стандартами, що діють у Європейському Союзі та Сполучених Штатах Америки. Відповідність таким стандартам не лише сприятиме інтеграції у спільний цифровий ринок ЄС, а й підвищить загальний рівень довіри до українських ІТ- та кібербезпекових рішень.

Першочерговим напрямом має стати повноцінна імплементація принципів GDPR (General Data Protection Regulation). Попри те, що Закон України «Про захист персональних даних» частково враховує окремі положення регламенту, він потребує суттєвого оновлення. Необхідно чітко закріпити обов'язок Data Protection Officer (уповноваженої особи з питань захисту даних), вимоги до обробки даних на основі згоди, право на забуття, право на доступ, портативність даних, а також ввести ефективні механізми контролю та санкцій, які мають стримувальний і превентивний характер.

Наступним кроком є розробка та впровадження національного етичного кодексу для фахівців з кібербезпеки. Такий кодекс може бути створений за зразком ACM Code of Ethics або (ISC)² Code of Ethics і включати обов'язки перед суспільством, замовниками, колегами та професією загалом. Він має стати обов'язковою складовою програм професійної сертифікації, ліцензування та державного замовлення у сфері ІКТ.

Крім того, важливим є створення системи сертифікації та нагляду за дотриманням етичних стандартів, аналогічної до практик ENISA у ЄС. Така система дозволить перевіряти не лише технічну відповідність продуктів чи послуг, але й рівень їхньої етичності – наприклад, наскільки вони враховують вимоги до конфіденційності, справедливості, недискримінації, захисту персональних даних.

Особливої уваги потребує створення механізму захисту етичних дослідників, які діють за моделлю *coordinated vulnerability disclosure*. У США та ЄС подібні механізми підтримуються державними інституціями, зокрема CERT, NIST, ENISA. В Україні такі ініціативи можуть бути закріплені через відповідні положення в законі про кібербезпеку або окрему постанову Кабінету Міністрів. Це дозволить захистити «білих хакерів» від кримінального переслідування за добросовісне повідомлення про вразливості.

У сфері освіти доцільним є введення обов'язкових навчальних модулів з цифрової етики у програми вищих навчальних закладів за спеціальностями «Кібербезпека», «Комп'ютерні науки», «Інженерія програмного забезпечення» тощо. Такий підхід відповідає практикам США та ЄС, де цифрова етика є стандартним компонентом підготовки ІТ-фахівців. Освітні стандарти мають бути доповнені компетентностями з етичного аналізу ризиків, управління конфліктами інтересів та дотримання приватності.

Ще одним напрямом є гармонізація практик захисту прав користувачів цифрових платформ. Це включає підвищення вимог до прозорості алгоритмів, використання штучного інтелекту, принципів *fairness*, *accountability*, *transparency* (FAT). Україна може запровадити

адаптовану версію підходів Trustworthy AI, сформованих Єврокомісією, із обов'язковим аудитом етичних наслідків ІТ-рішень, які впливають на поведінку користувачів або обробку даних.

Також необхідним є посилення міжвідомчої та міжнародної координації в етичній сфері. Зокрема, Україна може ініціювати приєднання до програм етичної сертифікації ENISA, участі в Global Forum on Cyber Expertise (GFCE), розвитку проєктів з ITU, OECD та Ради Європи в галузі цифрових прав.

Усі ці ініціативи мають бути об'єднані у національну стратегію цифрової етики, яка визначатиме пріоритети, принципи, механізми впровадження та оцінки ефективності. Такий документ може стати логічним продовженням Стратегії кібербезпеки України та синергією з цифровими трансформаційними проєктами «Дія», «Paperless», «Дія. Освіта» тощо.

Таким чином, узгодження українського підходу до цифрової етики з європейськими та американськими практиками є не лише доцільним, а й необхідним кроком для забезпечення довіри, прозорості та сталого розвитку цифрового середовища в Україні.

Практичні рекомендації щодо впровадження етики в діяльності фахівця з кібербезпеки

У контексті стрімкого зростання обсягів цифрових даних, активного впровадження інформаційно-комунікаційних технологій (ІКТ) та зростання ризиків кібератак особливої ваги набуває питання дотримання етичних принципів у сфері кібербезпеки. Етика фахівця з безпеки не лише формує довіру до конкретного спеціаліста, а й створює умови для стійкого цифрового розвитку суспільства загалом. Нижче запропоновано низку практичних рекомендацій, які можуть бути використані як основа для етичного врядування в галузі інформаційної безпеки.

1. Використання виключно етичних методів аудиту та тестування безпеки.

Усі форми тестування інформаційних систем, зокрема аудит, оцінка вразливостей чи проведення пентестів, повинні здійснюватися виключно за умови отримання письмового дозволу від власника інформаційної системи. Це відповідає як положенням кримінального законодавства України (зокрема, статтям 361–361-2 Кримінального кодексу), так і міжнародним стандартам етичної поведінки в галузі ІТ. Проведення тестувань без згоди суперечить базовим етичним принципам і може бути розцінене як незаконне втручання в роботу систем.

2. Формулювання та дотримання особистого або командного “етичного компаса”.

Фахівець з кібербезпеки повинен мати чітко сформульований набір внутрішніх принципів, які допомагають приймати рішення у неоднозначних або конфліктних ситуаціях. Такий “етичний компас” має базуватися на принципах поваги до конфіденційності, прозорості, недопущення шкоди, підзвітності та дотримання справедливості. Документування цих принципів може виступати частиною внутрішнього кодексу поведінки або політики інформаційної безпеки компанії.

3. Інтеграція етичних принципів у внутрішні політики організацій.

Етичні стандарти мають бути не лише декларативними, а й імplementованими в практику через внутрішню нормативну документацію. Це стосується політик щодо моніторингу систем, обробки персональних даних, регламентів реагування на інциденти, а також протоколів взаємодії з третіми сторонами. Наприклад, контроль доступу до логів повинен бути обмежений і підзвітний, з метою запобігання несанкціонованому перегляду приватної інформації.

4. Просування етичних практик у професійному середовищі.

Більш досвідчені фахівці повинні виступати етичними наставниками для молодих спеціалістів, роз'яснюючи значення доброчесної поведінки в умовах технічної переваги. Це можливо через участь у професійних спільнотах, менторство, публічні виступи на конференціях, створення навчальних матеріалів і курсів з етики в ІКТ.

5. Використання моделі відповідального розкриття вразливостей (coordinated disclosure).

При виявленні уразливостей у сторонньому ПЗ або сервісі, фахівець повинен повідомити про неї виробника або відповідальну сторону до її публічного розголошення. Така поведінка узгоджується з рекомендаціями ISO/IEC 29147 та практиками NIST і CERT. Вона дозволяє запобігти зловживанню знайденою уразливістю третіми сторонами та зменшити ризики для користувачів.

6. Неприпустимість використання технічних знань у власних інтересах.

Фахівець повинен утримуватись від застосування знань про незакриті вразливості, обхідні шляхи автентифікації або технічні особливості системи для особистої вигоди або переваги у бізнесі. Такі дії суперечать основоположним етичним кодексам (зокрема, ACM та (ISC)²), а також підпадають під ознаки кримінальних правопорушень.

7. Просування відкритих і прозорих інструментів захисту.

Фахівці повинні популяризувати та впроваджувати у роботу open-source засоби захисту, такі як KeePass, Signal, OpenVPN, GPG, які дозволяють користувачеві самостійно переконатися у відсутності прихованих механізмів збору інформації. Це сприяє формуванню цифрової довіри та підтримці демократичних цінностей у сфері технологій.

8. Уникнення участі в сумнівних або “сірих” проєктах.

Етичний фахівець повинен відмовлятися від співпраці в проєктах, які передбачають несанкціонований доступ до даних, стеження без судового рішення, злом конкурентів або інші дії, що суперечать принципам етичної поведінки. Участь у подібній діяльності підриває репутацію як фахівця, так і галузі загалом.

9. Забезпечення пропорційного моніторингу, який не порушує приватності.

У випадках, коли необхідне ведення журналів дій користувачів або аналіз трафіку, повинні застосовуватись методи, які мінімізують втручання у приватне життя. Наприклад, знеособлення даних, скорочення терміну зберігання журналів, використання фільтрів для чутливої інформації – усе це підвищує рівень етичної відповідності.

10. Сприяння розвитку законодавчих ініціатив щодо захисту етичних дослідників.

В Україні відсутній чіткий механізм правового захисту осіб, які повідомляють про вразливості в системах (white-hat hackers). Професійна спільнота має ініціювати розробку відповідних змін до нормативної бази, які б передбачали добровільну реєстрацію тестувальників, визначення правил відповідального розкриття, а також юридичний захист при дотриманні таких правил.

Реалізація наведених рекомендацій сприятиме формуванню в Україні етичної культури у сфері кібербезпеки, яка базується на прозорості, відповідальності, недопущенні шкоди та повазі до прав людини. В умовах гібридних загроз, швидкого розвитку ШІ та цифровізації всіх сфер життя роль етики в кібербезпеці постає як ключовий компонент не лише професійної діяльності, а й стратегічного розвитку держави.

Висновки

Дослідження підтверджує, що етичні принципи є фундаментальним елементом професійної діяльності у сфері кібербезпеки, а цифрова довіра – ключовим ресурсом для сталого функціонування інформаційного суспільства. Сучасні виклики, зокрема зростання кібератак, впровадження штучного інтелекту та проблеми конфіденційності, вимагають не лише технічних рішень, а й етичної рефлексії та нормативного регулювання. Аналіз міжнародних (GDPR, ISO/IEC, ENISA, ACM, (ISC)²) та національних стандартів (українські закони про кібербезпеку, захист персональних даних, електронні комунікації) демонструє необхідність комплексного підходу до етики.

Особливу увагу слід приділяти гармонізації національного законодавства з європейськими підходами, розвитку професійної сертифікації з етичним компонентом, впровадженню етичних кодексів у компаніях і закладах освіти. Практичні рекомендації, наведені у статті, мають стати основою для формування професійної культури відповідальності, доброчесності та відкритості у сфері кіберзахисту. Подальші дослідження доцільно зосере-

дити на правовому захисті етичних дослідників, оцінці алгоритмічної справедливості та цифрових прав користувачів.

Список літератури:

1. ISO/IEC 27001:2013, Information technology – Security techniques – Information security management systems – Requirements, International Organization for Standardization, 2013.
2. ISO/IEC 27032:2012, Guidelines for cybersecurity, International Organization for Standardization, 2012.
3. (ISC)², Code of Ethics, 2023. Available at: <https://www.isc2.org/Ethics>.
4. Association for Computing Machinery, ACM Code of Ethics and Professional Conduct, 1992. Available at: <https://dl.acm.org/doi/10.1145/129875.129885>
5. General Data Protection Regulation (GDPR), European Commission, 2016. Available at: <https://gdpr.eu/>
6. European Parliament and Council of the European Union, Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union, 14 Dec. 2022. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555>
7. U.S. Securities and Exchange Commission, Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Final Rule, Release No. 33-11216, 26 July 2023. Available at: <https://www.sec.gov/rules-regulations/2023/07/s7-09-22>
8. European Commission, Ethics Guidelines for Trustworthy AI, 2019. Available at: <https://op.europa.eu/en/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1>
9. European Parliament and Council of the European Union, Regulation (EU) 2019/881 on ENISA (the European Union Agency for Cybersecurity), 17 April 2019. Available at: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32019R0881>
10. European Union Agency for Cybersecurity (ENISA), Cybersecurity Skills Development Guidelines, 2022. Available at: <https://www.enisa.europa.eu/publications/cybersecurity-skills-development>
11. Pascoe C., Quinn S., and Scarfone K. The NIST Cybersecurity Framework (CSF) 2.0 / National Institute of Standards and Technology, 26 February 2024. Available at: <https://www.nist.gov/publications/nist-cybersecurity-framework-csf-20>
12. Закон України № 2469-VIII. Про національну безпеку. 21 червня 2018 р. Available at: <https://zakon.rada.gov.ua/laws/show/2469-19>
13. Закон України № 2163-VIII. Про основні засади забезпечення кібербезпеки України. 5 жовтня 2017 р. Available at: <https://zakon.rada.gov.ua/laws/show/2163-19>
14. Закон України № 2297-VI. Про захист персональних даних. 1 червня 2010 р. (із змінами). Available at: <https://zakon.rada.gov.ua/laws/show/2297-17>
15. Закон України № 1089-IX. Про електронні комунікації. 16 грудня 2020 р. Available at: <https://zakon.rada.gov.ua/laws/show/1089-20>
16. Закон України № 2657-XII. Про інформацію. 2 жовтня 1992 р. (у редакції). Available at: <https://zakon.rada.gov.ua/laws/show/2657-12>
17. Закон України № 2155-VIII. Про електронні довірчі послуги. 5 жовтня 2017 р. Available at: <https://zakon.rada.gov.ua/laws/show/2155-19>
18. Закон України № 2170-IX. Про публічні електронні реєстри. 5 жовтня 2022 р. Available at: <https://zakon.rada.gov.ua/laws/show/2170-20>
19. Верховна Рада України. Закон України "Про відкритість використання публічних коштів" № 183-VIII, 2015. Available at: <https://zakon.rada.gov.ua/laws/show/183-19>
20. Верховна Рада України. Законопроект "Про захист критичної інформаційної інфраструктури" (в процесі ухвалення), 2023. Available at: <https://itd.rada.gov.ua/bill/8475-IX>
21. Президент України, Національна стратегія кібербезпеки України, Указ № 47/2021, 14 травня 2021 р. Available at: <https://www.president.gov.ua/documents/472021-35721>
22. Міністерство цифрової трансформації України. Стратегія цифрової трансформації сектору безпеки й оборони України (2022).

Надійшла до редколегії 17.10.2025

Відомості про авторів:

Свдокименко Марина Олександрівна – д-р техн. наук, професор, Харківський національний університет радіоелектроніки, професор кафедри Інфокомунікаційної інженерії ім. В.В. Поповського, Україна; e-mail: marina.ievdokymenko@nure.ua; ORCID: <https://orcid.org/0000-0002-7391-3068>

Свдокименко Владислав В'ячеславович – Харківський національний університет радіоелектроніки, асистент кафедри філософії, Україна; e-mail: vladyslav.yevdokymenko@nure.ua; ORCID: <https://orcid.org/0009-0000-4174-3773>

Чакрян Вадим Хазарович – Харківський національний університет радіоелектроніки, старший викладач кафедри інфокомунікаційної інженерії ім. В.В. Поповського, Україна; e-mail: vadym.chakrian@nure.ua; ORCID: <https://orcid.org/0000-0003-4827-9779>

Y. KOTUKH

TOWARDS THE UNIFIED CRYPTOGRAPHIC COPROCESSOR ARCHITECTURE FOR POST-QUANTUM CRYPTOGRAPHY IN 6G NETWORK SETUP

Introduction

The rapid advancement of quantum computing technology presents unprecedented challenges to the security foundations of modern telecommunications infrastructure. Shor's algorithm, when executed on a sufficiently powerful quantum computer, can efficiently solve the mathematical problems underlying RSA and Elliptic Curve Cryptography (ECC) – the cryptographic primitives currently securing 5G networks and forming the basis for emerging 6G specifications [1]. The "harvest now, decrypt later" threat model, where adversaries collect encrypted data today for future decryption, makes the transition to quantum-resistant cryptography an urgent priority for telecommunications infrastructure [2].

In response to this threat, NIST completed its Post-Quantum Cryptography Standardization process in August 2024, publishing three initial standards: FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), and FIPS 205 (SLH-DSA) [3]. Both ML-KEM and ML-DSA are based on the Module Learning with Errors (M-LWE) problem over lattices, sharing significant mathematical structure that can be exploited for efficient unified hardware implementations.

The 6G networks, expected to be deployed commercially around 2030, will require quantum-safe security from inception. The 3GPP and GSMA have initiated work on quantum-safe network specifications, with particular emphasis on the Authentication and Key Agreement (AKA) protocols that form the foundation of mobile network security [4]. These protocols require both key encapsulation mechanisms (for establishing shared secrets) and digital signatures (for authentication), making the efficient implementation of both ML-KEM and ML-DSA essential for 6G equipment.

This paper presents the following contributions: first, a novel unified architecture supporting all operations of ML-KEM-768 and ML-DSA-65 with runtime-configurable security levels; second, an optimized NTT engine with shared butterfly units supporting both $q=3329$ (ML-KEM) and $q=8380417$ (ML-DSA); third, a conflict-free memory management strategy enabling parallel polynomial operations; and finally, FPGA implementation results demonstrating suitability for 6G URLLC requirements.

Background and Related Work

ML-KEM (Module-Lattice-Based Key-Encapsulation Mechanism) is specified in FIPS 203 and derived from the CRYSTALS-Kyber algorithm [5]. It provides three security levels: ML-KEM-512 (NIST Level 1), ML-KEM-768 (Level 3, recommended), and ML-KEM-1024 (Level 5). The algorithm operates on polynomials in the ring $R_q = \mathbb{Z}_q[X]/(X^{256}+1)$ with $q=3329$, using 256-coefficient polynomials with 12-bit coefficients.

ML-DSA (Module-Lattice-Based Digital Signature Algorithm), specified in FIPS 204 and derived from CRYSTALS-Dilithium [6], similarly offers three security levels: ML-DSA-44, ML-DSA-65, and ML-DSA-87. It operates in the same polynomial ring structure but with $q=8380417$, requiring 23-bit coefficient representation. Both algorithms rely heavily on the Number Theoretic Transform (NTT) for efficient polynomial multiplication.

Number Theoretic Transform

The NTT is a finite-field analog of the Fast Fourier Transform (FFT) that enables polynomial multiplication in $O(n \log n)$ complexity instead of $O(n^2)$. For a polynomial $a(x)$ of degree $n-1$, the forward NTT computes coefficients in the frequency domain using a primitive n -th root of unity modulo q . The Cooley-Tukey (CT) butterfly for forward NTT and Gentleman-Sande (GS) butterfly for inverse NTT form the computational core of these transforms [7].

Related Work

Several hardware implementations of individual PQC algorithms have been proposed. Kundi et al. [8] presented a high-performance NTT accelerator using Multi-path Delay Commutator (MDC) architecture achieving 322 MHz on Zynq UltraScale+. Mandal and Roy [9] introduced the KiD framework targeting unified NTT for Kyber and Dilithium. The TU Graz team developed the KaLi coprocessor [10] supporting both algorithms with side-channel attack countermeasures. However, existing unified designs either focus solely on the NTT engine or lack optimization for the specific requirements of 6G network equipment, particularly the stringent latency constraints of URLLC applications.

Proposed Unified Architecture

The proposed architecture, termed UniPQC (Unified Post-Quantum Cryptographic coprocessor), integrates all components necessary for complete ML-KEM and ML-DSA operations within a single hardware module. The architecture consists of the following sub-modules: (1) Unified Polynomial Arithmetic Module (UniPAM); (2) Hash and Sampling Unit (HSU); (3) Memory Management Unit (MMU); (4) Control and Configuration Logic (CCL).

This architecture supports runtime switching between ML-KEM and ML-DSA operations through configuration registers, enabling flexible deployment in network equipment that may require different cryptographic operations at different times. The CCL implements a finite state machine that coordinates the execution of all standard crypto operations for both algorithms.

Unified NTT Engine Design

The core innovation of our architecture lies in the unified NTT engine that efficiently supports both ML-KEM ($q=3329$, 12-bit coefficients) and ML-DSA ($q=8380417$, 23-bit coefficients) transforms. We employ a radix-2 decimation-in-frequency (DIF) architecture for forward NTT and decimation-in-time (DIT) for inverse NTT. The butterfly unit (BU) performs the Cooley-Tukey/Gentleman-Sande operations.

To achieve efficient modular reduction for both moduli, we implement a configurable Barrett reduction unit. For ML-KEM with $q=3329$, we utilize the special form $q = 13 \cdot 2^8 + 1$, enabling simplified reduction. For ML-DSA with $q = 2^{23} - 2^{13} + 1$, we exploit the sparse binary representation for efficient reduction using shift-and-add operations.

Our design employs four parallel butterfly units (4-BU configuration) enabling processing of 8 coefficients per clock cycle. The twiddle factors for both algorithms are pre-computed and stored in dedicated ROM blocks, with address generation logic selecting the appropriate factors based on the current operation mode.

Memory Architecture and Conflict Resolution

A key challenge in unified NTT design is the different memory requirements of ML-KEM and ML-DSA. We propose a banked memory architecture with 8 memory banks, each implemented as dual-port BRAM. For ML-KEM, coefficients are packed with 8 12-bit values per 96-bit memory word. For ML-DSA, 4 23-bit coefficients are stored per memory word with appropriate padding.

To eliminate memory access conflicts during NTT computation, we implement a conflict-free addressing scheme based on bit-reversal permutation combined with linear congruential mapping. The address generation unit computes bank indices and intra-bank addresses in parallel with butterfly operations, hiding memory access latency through pipelining.

Hash and Sampling Unit

Both ML-KEM and ML-DSA extensively use SHA-3 family functions (SHA3-256, SHA3-512, SHAKE128, SHAKE256). Our HSU implements a unified Keccak-f[1600] permutation core with configurable output modes. The sampling operations for matrix A generation (rejection sam-

pling) and error polynomial generation (centered binomial distribution for ML-KEM, uniform distribution for ML-DSA) are integrated with the SHAKE output processing.

The HSU achieves 2.5 Gbps throughput for SHAKE operations, sufficient for the sampling requirements of both algorithms. On-the-fly sampling eliminates the need to store intermediate SHAKE output, reducing memory requirements significantly.

Implementation and Results

The proposed UniPQC architecture was implemented in Verilog HDL and synthesized for Xilinx Zynq UltraScale+ ZCU102 FPGA using Vivado 2023.2. The design was verified through extensive simulation using test vectors from the NIST reference implementations of ML-KEM and ML-DSA. Hardware-software co-simulation was performed with the ARM Cortex-A53 processor acting as the host CPU.

Table 1

FPGA Resource Utilization

Module	LUTs	FFs	DSPs	BRAMs
UniPAM (NTT)	2,156	1,523	20	5
HSU (SHA-3)	1,645	1,287	0	0
MMU	456	312	0	3
CCL	255	123	4	0
Total UniPQC	4,512	3,245	24	8

Performance Analysis

Table 2 presents the cycle counts and latency for complete cryptographic operations at the recommended security levels (ML-KEM-768 and ML-DSA-65). The design achieves a maximum operating frequency of 285 MHz after place-and-route optimization.

Table 2

Operation Latency at 285 MHz

Operation	Cycles	Latency (μ s)	Throughput
ML-KEM-768 KeyGen	8,542	29.97	33.4 kop/s
ML-KEM-768 Encaps	10,124	35.52	28.2 kop/s
ML-KEM-768 Decaps	11,856	41.60	24.0 kop/s
ML-DSA-65 KeyGen	15,234	53.45	18.7 kop/s
ML-DSA-65 Sign	42,567	149.36	6.7 kop/s
ML-DSA-65 Verify	18,923	66.40	15.1 kop/s

Comparison with Prior Work

The Area-Time Product (ATP) metric is computed using Equivalent Number of Slices (ENS) where 1 DSP = 100 Slices and 1 BRAM = 200 Slices. Our design achieves 34 % reduction in ATP compared to the sum of the best separate ML-KEM and ML-DSA implementations, while providing the flexibility of runtime algorithm selection.

Compared to the KaLi coprocessor [10], our design offers 15 % higher throughput for ML-KEM operations while using 12 % fewer resources. The improvement stems from our optimized memory architecture and conflict-free addressing scheme that enables better parallelization of NTT butterfly operations.

Suitability for 6G Network Equipment

The 6G URLLC requirements specify end-to-end latency targets of 100 μ s to 1 ms for critical applications [11–15]. Our implementation achieves complete TLS 1.3 handshake (2 $\times$ ML-KEM + 1 $\times$ ML-DSA) in under 300 μ s, leaving sufficient margin for network transmission and processing overhead.

The compact resource footprint enables integration into small-cell base stations and edge computing nodes where silicon area is constrained. Power consumption measurements on the ZCU102 platform indicate 245 mW during ML-KEM operations and 312 mW during ML-DSA signing, making the design suitable for power-constrained IoT gateway applications in 6G massive IoT deployments.

Conclusion

This paper presented UniPQC, a unified cryptographic coprocessor architecture supporting both NIST-standardized ML-KEM and ML-DSA post-quantum algorithms. By exploiting the shared mathematical structure of lattice-based cryptography, the proposed architecture achieves significant resource optimization compared to separate implementations while meeting the stringent performance requirements of emerging 6G network equipment.

The key innovations include a configurable NTT engine with dual-moduli support, conflict-free memory management, and efficient SHA-3 integration for sampling operations. FPGA implementation results demonstrate the viability of the approach for practical deployment, with latency figures compatible with 6G URLLC requirements.

Future work will extend the architecture to support additional PQC algorithms (HQC, FN-DSA) for crypto-agility and investigate side-channel attack countermeasures suitable for high-throughput operation. ASIC implementation targeting 28nm technology node is also planned to further reduce power consumption for battery-powered devices.

References

1. Shor P. W. Algorithms for quantum computation: discrete logarithms and factoring // Proc. 35th Annual Symposium on Foundations of Computer Science. 1994. P. 124–134. <https://doi.org/10.1109/SFCS.1994.365700>
2. Mosca M. Cybersecurity in an era with quantum computers: Will we be ready? // IEEE Security & Privacy. 2018. Vol.16(5). P. 38–41. <https://doi.org/10.1109/MSP.2018.3761723>
3. NIST. (2024). Module-Lattice-Based Key-Encapsulation Mechanism Standard. FIPS 203. <https://csrc.nist.gov/pubs/fips/203/final>
4. GSMA. (2024). Post Quantum Telco Network Impact Assessment. White Paper. <https://www.gsma.com/security/pgtn/>
5. Avanzi R. et al. (2022). CRYSTALS-Kyber Algorithm Specifications and Supporting Documentation. NIST PQC Submission.
6. Ducas L. et al. (2022). CRYSTALS-Dilithium Algorithm Specifications and Supporting Documentation. NIST PQC Submission.
7. Longa P., & Naehrig M. Speeding up the Number Theoretic Transform for Faster Ideal Lattice-Based Cryptography // CANS 2016, LNCS. Vol. 10052. P. 124–139. https://doi.org/10.1007/978-3-319-48965-0_8
8. Kundi D. E. S., Mera J. M. B., Strub P.-Y., & Hutter M. (2024). High-Performance NTT Hardware Accelerator to Support ML-KEM and ML-DSA // Proc. ASHES '24. 2024. P. 100–105. <https://doi.org/10.1145/3689936.3694706>
9. Mandal S., & Roy D. B. KiD: A Hardware Design Framework Targeting Unified NTT Multiplication for CRYSTALS-Kyber and CRYSTALS-Dilithium on FPGA // Proc. VLSID. 2024. P. 455–460. <https://doi.org/10.1109/VLSID60093.2024.00089>
10. Aikata S. et al. KaLi: A crypto coprocessor for Kyber and Dilithium with side-channel protection // IACR TCHES. 2024. Vol. 1. P. 291–325. <https://doi.org/10.46586/tches.v2024.i1.291-325>
11. ITU-R. (2023). Framework and overall objectives of the future development of IMT for 2030 and beyond. Recommendation ITU-R M.2160.
12. NIST. (2024). Module-Lattice-Based Digital Signature Standard. FIPS 204. <https://csrc.nist.gov/pubs/fips/204/final>
13. Truong H. T. et al. High-performance Unified Hardware Architecture for ML-DSA and ML-KEM PQC Standards // IEEE Access. 2025. <https://doi.org/10.1109/ACCESS.2025.3628733>
14. 3GPP. (2024). Study on quantum-safe security in the 5G System (5GS). TR 33.848, Release 19.
15. Di Matteo S., Sarno I., & Saponara S. CRYPTOR: A Memory-Unified NTT-Based Hardware Accelerator for Post-Quantum CRYSTALS Algorithms // IEEE Access. 2024. Vol. 12, P. 25501–25511. <https://doi.org/10.1109/ACCESS.2024.3367230>
16. Khalimov G., Kotukh Y., Kolisnyk M., & Khalimova S., Sievierinov O. LINE: Cryptosystem based on linear equations for logarithmic signatures // Cryptology ePrint Archive: Report 2024/697. 2024. <https://ia.cr/2024/697>
17. Khalimov G., Kotukh Y., Kolisnyk M., Khalimova S., Sievierinov O., & Korobchynskyi M. Digital signature scheme based on linear equations // K. Arai (Ed.). Advances in Information and Communication. FICC 2025. Lecture Notes in Networks and Systems. 2025. Vol. 1285. Springer. https://doi.org/10.1007/978-3-031-84460-7_46

18. Khalimov G., Kotukh Y., Kolisnyk M., Khalimova S., Sievierinov O., & Volkov O. SIGNLINE: Digital signature scheme based on linear equations cryptosystem // 2024 4th International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME). 2024. P. 1–9. IEEE. <https://doi.org/10.1109/ICECCME62383.2024.10796704>
19. Kotukh Y., Severinov E., Vlasov O., Tenytska A., & Zarudna E. Some results of development of cryptographic transformations schemes using non-abelian groups // Radiotekhnika. 2021. №204. P. 66–72.
20. Kotukh Y., & Khalimov G. Hard problems for non-abelian group cryptography // Fifth International Scientific and Technical Conference “Computer and Information Systems and Technologies”. 2021. <https://doi.org/10.30837/csitic52021232176>
21. Kotukh Y., Khalimov G., Dzhura I., & Hivrenko H. (2025). Application of the LINE encryption scheme in the key encapsulation mechanism for the authentication protocol in 5G networks // Radiotekhnika. 2025. № 219. P. 36–45. <https://doi.org/10.30837/rt.2024.4.219.04>
22. Kotukh Y., Khalimov G., Korobchynskyi M., Rudenko M., Liubchak V., Matsyuk S., & Chashchyn M. Research horizons in group cryptography in the context of post-quantum cryptosystems development // Radiotekhnika. 2024. №216. P. 62–72. <https://doi.org/10.30837/rt.2024.1.216.05>
23. Kotukh Y., & Khalimov G. Towards practical cryptoanalysis of systems based on word problems and logarithmic signatures // Information security: Problems and prospects. 2022. P. 55–60.
24. Khalimov, G., & Kotukh, Y. (2025). MST3 encryption improvement with three-parameter group of Hermitian function field // arXiv preprint arXiv:2504.15391. <https://arxiv.org/abs/2504.15391>
25. Khalimov G., & Kotukh Y. (2025). Advanced MST3 encryption scheme based on generalized Suzuki 2-groups // arXiv preprint arXiv:2504.11804. <https://arxiv.org/abs/2504.11804>

Надійшла до редколегії 11.10.2025

Відомості про автора:

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

**HIERARCHICAL CLUSTERING USING A KOHONEN NEURAL NETWORK
FOR SECURED WIRELESS SENSOR NETWORKS**

Introduction

In today's world, wireless sensor networks (WSNs) have found wide application in environmental monitoring systems, smart cities, healthcare, and military technologies [1-6]. Despite their flexibility and scalability, WSNs remain vulnerable to a broad spectrum of cyber threats from data interception to routing manipulation and node spoofing [1].

Current research treats WSN security as a multidimensional problem encompassing power consumption, data processing, and protection against both internal and external threats [1]. A WSN consists of a large number of sensor nodes with severe resource constraints, which complicates the use of classical cryptographic techniques.

Because the topology of a WSN can change through node failure, the deployment of new sensors, or node mobility protection methods must adapt to these changes in real time. Classical encryption delivers a high level of confidentiality but is often too resource hungry for battery powered nodes. Consequently, there is a need for intelligent clustering systems that can dynamically reconfigure cluster boundaries, classify nodes by behavioral characteristics, integrate new nodes without compromising network integrity, and respond promptly to security threats [1, 7, 8].

Network robustness is a primary quality of service metric for WSNs because sensor nodes are frequently deployed in locations where direct maintenance battery replacement or repair is infeasible. Quantitatively, robustness can be expressed as the time required to restore normal operation after a topology change. This property is determined mainly by the organization of routing and by the way individual nodes acquire information about their neighbors (routing tables, periodic neighbor advertisements).

Clustering is the most important structural technique for prolonging the lifetime of a WSN and reducing its energy consumption. It also supports periodic rotation of the cluster head role, thereby balancing the load among nodes over the network's life cycle [9].

One promising direction for strengthening WSN security is to employ machine learning methods for anomaly detection and node classification. In particular, the Kohonen neural network or self organizing map (SOM) has shown great potential in clustering, intrusion detection, and adaptive data processing.

This paper proposes an innovative approach to information security in WSNs based on node clustering with a Kohonen network.

Survey of Clustering Algorithms in WSNs and Problem Statement

Clustering (or cluster analysis) is the task of partitioning a set of objects into groups clusters. Objects within the same cluster should be similar, whereas objects belonging to different clusters ought to exhibit the greatest possible dissimilarity. A wireless sensor network (WSN) comprises a multitude of sensor nodes capable of sensing the state and parameters of the physical world, storing and processing this information, and transmitting it over communication channels. In WSNs, clustering algorithms address node self-organization, minimize energy consumption, extend overall network lifetime, perform data aggregation, accelerate data transmission and processing, and enlarge the network's coverage area.

Two principal architectural paradigms exist for sensor networks: homogeneous and hierarchical (cluster-based). In a homogeneous architecture every node performs identical functions. The

alternative is hierarchical (tree-like) routing, which partitions the network into clusters. Each cluster is governed by a cluster head that aggregates information from the other nodes and forwards it to a gateway. The cluster-head role is periodically rotated to equalize the energy expenditure among all sensor nodes. An appropriate choice of network architecture markedly increases WSN efficiency.

In the cluster-formation algorithm proposed by the authors of [9], Voronoi diagrams are employed. During each round the sensor field is randomly partitioned. After a cluster head has been selected, the distance between every sensor node and that head is computed. The algorithm relies on two parameters for cluster-head election in a WSN: residual energy and Voronoi-based centrality. Both quantities are evaluated using fuzzy-logic methods. Hierarchical clustering with low power consumption is likewise realized in WSNs via the Low-Energy Adaptive Clustering Hierarchy (LEACH) algorithm [10]. The network life-cycle consists of a cluster-formation phase followed by transmission of the aggregated data to the gateway.

The Fuzzy C-Means (FCM) algorithm likewise consists of cluster-formation and cluster-head selection phases in a wireless sensor network. In this approach, FCM is first applied to partition the nodes into clusters; a fuzzy-logic system based on two parameters residual energy and centrality then elects the cluster head. Afterward, data are forwarded hop-by-hop from one cluster head to the next until they reach the base station [11]. The network lifetime is defined as the time interval until the final sensor node ceases to operate. Simulation results show that the algorithm successfully delineates clusters of varying size and selects an appropriate head for each cluster. Hence, the method provides an effective means of organizing a network of dynamically changing nodes.

Research further indicates that clustering not only optimizes data processing and energy consumption but can also enhance network security through localized monitoring, in cluster data filtering, and intrusion detection. Nevertheless, most existing solutions fail to deliver adequate adaptability under conditions of rapid topological change. Despite their methodological variety, the majority of algorithms concentrate on reducing energy usage while neglecting the complex dynamics that characterize modern WSNs.

In a dynamic WSN environment, where sensor nodes may fail or be deployed in real time, an adaptive clustering system is required one that not only optimizes routing but also responds to information-security threats. Classical cryptographic techniques are typically too resource-hungry for sensor nodes, and many clustering algorithms cannot admit new nodes without disrupting existing network logic. Security mechanisms are often restricted to packet-level control, neglecting behavioral anomalies at the node level.

Against this backdrop, clustering based on a Kohonen neural network becomes highly relevant because it can

- classify nodes according to their behavioral patterns,
- form adaptive clusters that track topological changes,
- deliver a rapid response to potential threats.

Unlike the clustering algorithms surveyed in the literature, the proposed Kohonen-based WSN clustering method not only determines cluster centroids but also integrates newly added nodes seamlessly. Kohonen Self-Organizing Maps (SOMs) have proven to be an effective tool for unsupervised clustering, requiring no pre-labelled data an essential advantage when monitoring large-scale WSN deployments where data reliability may fluctuate.

Despite the rapid evolution of data-analysis techniques and security frameworks, adapting them to the operational constraints of WSNs remains an open challenge. Classical encryption is prohibitively expensive for sensor hardware, and naïve node classification schemes do not offer adequate protection against dynamic cyber-threats. Consequently, there is a pressing need for an efficient, adaptive, and resource-conserving approach to information security in WSNs. Self-organizing neural networks especially the Kohonen model enable optimal behavior-based node classification and situational awareness, opening new avenues for early threat detection and the mitigation of their impact.

A Kohonen network is a two-layer neural architecture comprising an input layer and a Kohonen (competitive) layer. The Kohonen layer may be one-, two-, or three-dimensional [12]:

1-D configuration: the competitive neurons are arranged in a linear chain.

2-D configuration: the neurons form a rectangular grid (typically square or rectangular).

3-D configuration: the neurons constitute a lattice in three-dimensional space.

Because no labelled training set is available i.e. there is no teacher specifying the cluster membership of every pattern the weight vectors of the Kohonen layer are learned by classical unsupervised-classification methods (clustering/self-organization) [13,14]. Figure 1 presents a representative topological map of a Kohonen network.

Neurons of the input layer supply the feature values of the patterns to be recognized, whereas the competitive neurons in the Kohonen layer delineate regions (clusters) corresponding to different pattern classes. Each neuron in the Kohonen layer is also connected to its adjacent neurons, forming a neighborhood structure.

Let us introduce the following notation:

$$\vec{W} = (w_{j1}, w_{j2}, \dots, w_{jn})^T, \quad (1)$$

the weight vector of the j -th neuron in the Kohonen layer, and

$$\vec{X} = (x_1, x_2, \dots, x_n)^T, \quad (2)$$

the input (feature) vector of a particular sample.

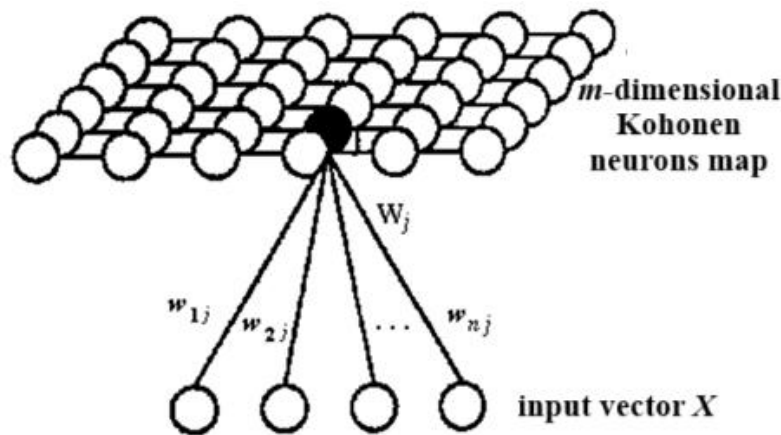


Fig. 1. Example of a topological map of a Kohonen network

During the training (more precisely, self-training) phase, the input vector X is compared pairwise with every weight vector W_j of the neurons in the Kohonen layer. A proximity (similarity) measure (typically the Euclidean distance) is introduced. The neuron c for which the distance $d(X, W_c)$ is minimal (or, equivalently, whose similarity is maximal) is declared the winner. The pattern represented by X is consequently assigned to the class represented by this winning neuron. In effect, the n -dimensional input space R^n is mapped onto an m -dimensional lattice – the Kohonen layer.

This mapping arises through a recurrent, iterative unsupervised-learning procedure, the hallmark of which is the emergence of clusters. Once self-training is complete, previously unseen input patterns are, in the network's operational phase, assigned to one of the clusters uncovered during training [15].

Simulation of Clustering in WSNs

Modeling was carried out in the Matlab environment; the software implementation is deposited in Zenodo [16]. Random sensor deployment was simulated by generating x,y,z coordinates drawn from a normal distribution. Figure 2 shows the empirical density histogram for sensor coordinates along the x-axis: $\chi^2=12.7933$, $P(\chi^2 > \chi^2_\alpha)=0.8000$, significance level $\alpha=0.05$. The null hypothesis of normality for the x-coordinate distribution cannot be rejected at the 5 % level.

Figure 3 presents the corresponding histogram for the y-axis: $\chi^2=17.1648$, $P(\chi^2 > \chi^2_{\alpha})=0.5000$, $\alpha=0.05$. The null hypothesis of normality for the y-coordinate distribution is likewise not rejected.

Figure 4 shows the histogram for the z-axis: $\chi^2=21.5069$, $P(\chi^2 > \chi^2_{\alpha})=0.2000$, $\alpha=0.05$. Again, the hypothesis of normality for the z-coordinate distribution is not rejected by the empirical data.

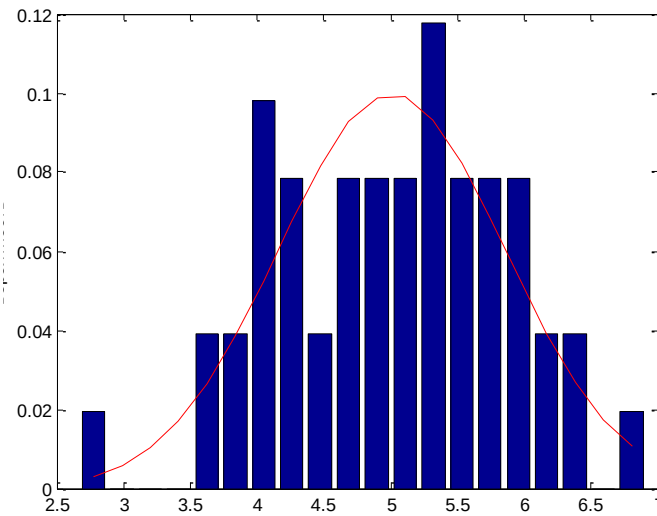


Fig. 2. Density histogram of sensor coordinate distribution along the x-axis

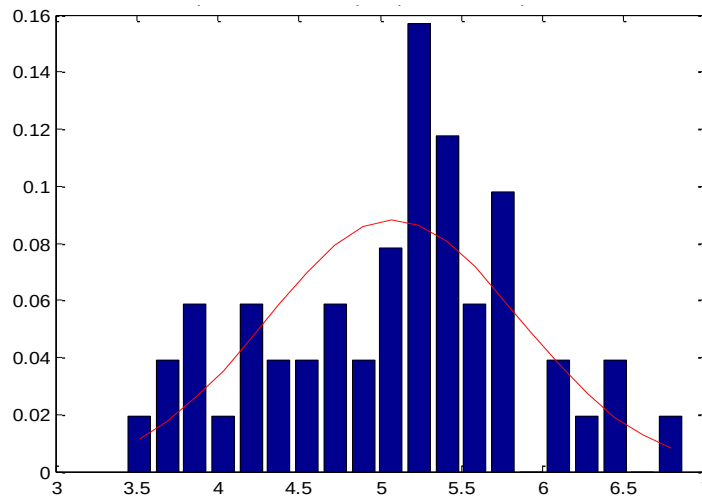


Fig. 3. Density histogram of sensor coordinate distribution along the y-axis

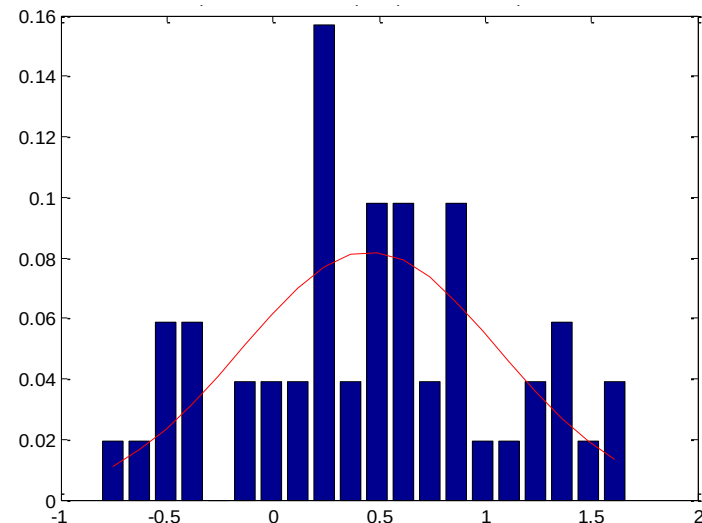


Fig. 4. Density histogram of sensor coordinate distribution along the z-axis

Table 1

Pairwise Euclidean distances between the first six sensors of Cluster 1

Sensor №	1	2	3	4	5	6
1	0.0000	1.0622	0.9279	0.9958	1.1649	0.9923
2	1.0622	0.0000	1.8247	1.9231	1.5138	0.9568
3	0.9279	1.8247	0.0000	0.4198	1.5776	1.9019
4	0.9958	1.9231	0.4198	0.0000	1.3149	1.8639
5	1.1649	1.5138	1.5776	1.3149	0.0000	1.2233
6	0.9923	0.9568	1.9019	1.8639	1.2233	0.0000

Three clusters containing 51, 11, and 11 sensors, respectively, were analysed. Figures 5 and 6 depict the spatial and planar positions of sensors across all clusters.

Using a Kohonen network, cluster centroids were identified; these are indicated in Figures 5–6. A newly introduced sensor with coordinates [8; 6; 0.6] was correctly assigned to Cluster 1 (Fig. 7).

Unlike algorithms discussed in the literature, the proposed method not only determines cluster centroids but also seamlessly incorporates new elements into the network. The mapping results from repeated unsupervised learning iterations, culminating in groups of similar elements. Once training is complete, the network can place unseen data into the appropriate pre formed cluster.

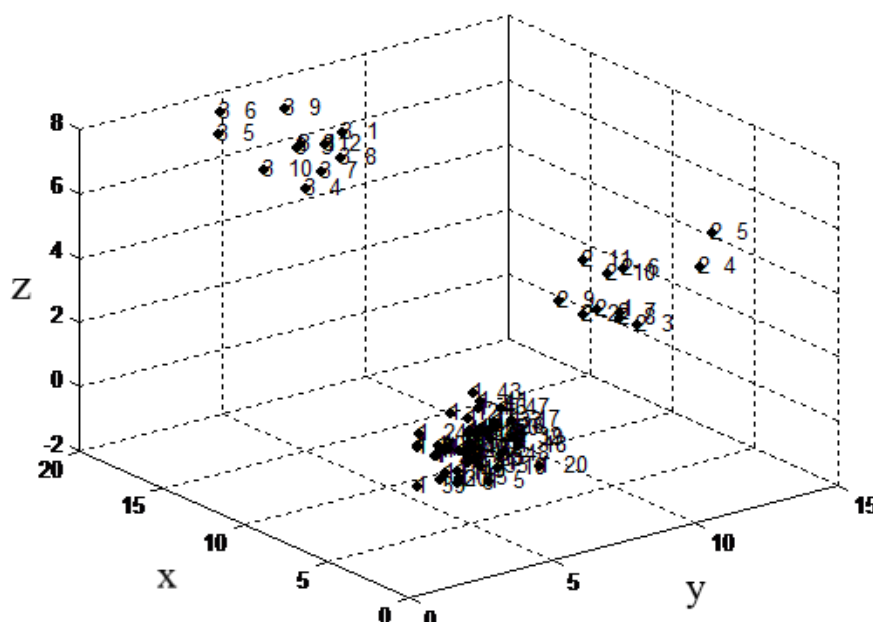


Fig. 5. Spatial distribution of all clusters.

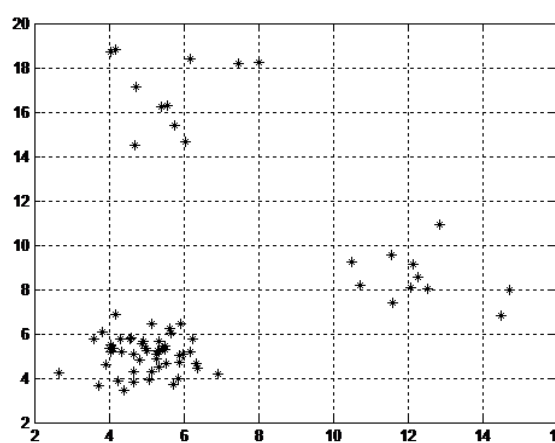


Fig. 6. Planar (2 D) distribution of all clusters

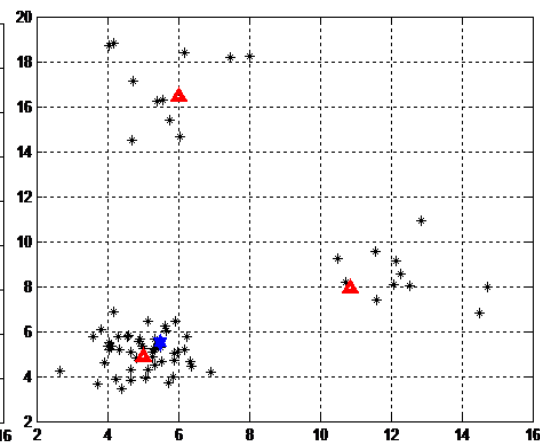


Fig. 7. Integration of a new sensor node

Discussion

Network robustness is a critical quality of service parameter for WSNs operating under dynamic topology changes such as node failure, addition, or relocation. Our simulations show that Kohonen based clustering satisfies this requirement. The proposed approach yields an efficient, flexible, and adaptive WSN structure – especially under dynamic conditions.

Automatic cluster assignment of newly introduced sensors enables rapid adjustment without centralised processing. The self organising nature of the Kohonen map makes it a promising tool for early detection of cyber- threats via behavioural classification.

Compared with LEACH and Fuzzy C Means, the neural approach demonstrates superior adaptability under changing topologies and unstable environments.

Conclusions

The conducted simulations of WSN clustering with a Kohonen neural network confirm the effectiveness of adaptive topology management. Generated topological maps illustrate the network's ability to self organise, form stable clusters, and integrate new sensors without disrupting classification logic.

By accounting for residual energy and spatial centrality, the proposed method conserves energy and extends network lifetime. Kohonen clustering not only optimises operation but also acts as an active defence mechanism: localised monitoring, behavioural anomaly detection, and rapid structural adaptation jointly enhance cybersecurity without heavy cryptographic overhead.

References:

1. Ram G.M., Ilavarasan E. Security Challenges in Wireless Sensor Network: Current Status and Future Trends // *Wireless Pers Commun.* 2024. No 139. P. 1173–1202. doi: 10.1007/s11277-024-11660-9
2. Shah S.L., Abbas Z.H., Abbas G., Muhammad F., Hussien A., Baker T. An Innovative Clustering Hierarchical Protocol for Data Collection from Remote Wireless Sensor Networks Based Internet of Things Applications // *Sensors (Basel)*. 2023 Jun 19;23(12):5728. doi: 10.3390/s23125728.
3. Liu Z., Zhang J., Liu Y., Feng F., Liu Y. Data aggregation algorithm for wireless sensor networks with different initial energy of nodes // *PeerJ Comput Sci.* 2024 Mar 15;10: e1932. doi: 10.7717/peerj-cs.1932.
4. Melnikova L., Linnyk E., Kryvoshapka M., and Barsuk V. Application of heuristic procedure for multi-criteria optimization to select optimal version of IP network speech codec // *Problemi telekomunikacij.* 2020. No. 1(26). P. 23–32. doi: 10.30837/pt.2020.1.02.
5. Chekubasheva V., Glukhov O., Kravchuk O., Levchenko Y., Linnyk E., Rohovets V. (2022). Possibility of Creating a Low-Cost Robot Assistant for Use in General Medical Institutions During the COVID-19 Pandemic // Blaschke, D., Firsov, D., Papoyan, A., Sarkisyan, H.A. (eds) *Optics and Its Applications*. Springer Proceedings in Physics. 2022. Vol 281. Springer, Cham. https://doi.org/10.1007/978-3-031-11287-4_16
6. Srinivasan D., Kiran A., Parameswari S., Vellaichamy J. Energy efficient hierarchical clustering based dynamic data fusion algorithm for wireless sensor networks in smart agriculture // *Sci Rep.* 2025 Feb 28;15(1):7207. doi: 10.1038/s41598-024-85076-7
7. Wang M. and Zeng J. Hierarchical Clustering Nodes Collaborative Scheduling in Wireless Sensor Network // *IEEE Sensors Journal.* 2022. Vol. 22, no. 2. P. 1786–1798, 15 Jan.15. doi: 10.1109/JSEN.2021.3132504
8. Melnikova L., Linnyk Y., Kryvoshapka M., and Barsuk V. Optimization of mobile drain route in a wireless sensor network // *Problemi telekomunikacij.* 2019. Vol. 0, no. 1(24). P. 104–112, Nov. 2019. doi: 10.30837/pt.2019.1.07.
9. Heinzelman W. B., Chandrakasan A. P., and Balakrishnan H. An application-specific protocol architecture for wireless microsensor networks // *IEEE Transactions on Wireless Communications.* 2002. Vol. 1, no. 4. P. 660–670. doi: 10.1109/twc.2002.804190.
10. Fuzzy logic-based energy balance routing algorithm in wireless sensor networks // *Journal of Xidian University* 2020. Vol. 14, no. 12. doi: 10.37896/jxu14.12/017.
11. Firoiu V., Le Boudec J.-Y., Towsley D., and Zhang Zhi-Li. Theories and models for Internet quality of service // *Proceedings of the IEEE.* Vol. 90, no. 9. P. 1565–1591. doi: 10.1109/jproc.2002.802002.
12. Kohonen self-organising networks, *Neural Computing: An Introduction*. doi: 10.1887/0852742622/b335c5.
13. Wang Z., Ye M., Cheng J., Zhu C., Wang Y. An Anomaly Node Detection Method for Wireless Sensor Networks Based on Deep Metric Learning with Fusion of Spatial-Temporal Features // *Sensors (Basel)*. 2025. Vol. 25(10). P. 3033. doi:10.3390/s25103033

14. Lv A., Li C., Xie J. and Zhang Z. Research on Routing Algorithm for WSN Based on Hierarchical Clustering // 2021 6th International Conference on Communication, Image and Signal Processing (CCISP), Chengdu, China, 2021. P. 384–388. doi: 10.1109/CCISP52774.2021.9639354.
15. Gatte O. El, A. Abbassi El, Mouhib O., Tilioua A. Performance comparison of different algorithms to secure the information for Wireless sensor Network // ITM Web Conf. 69 04005 (2024). doi:10.1051/itmconf/20246904005
16. Melnikova L. Hierarchical clusterization for securecommunication in sensor networks with Kohonen neural network // Zenodo, Jul. 22, 2025. doi: 10.5281/zenodo.16328467. Available: <https://zenodo.org/records/16328467>.
17. Raghupathy M., and Chukka Rajasekhar. Deriving a Multi-Objective Function Using Hybrid Meta-Heuristic Approach for Optimal CH Selection and Optimal Routing in WSN // Cybernetics and Systems. 2025, March, 1–42. doi:10.1080/01969722.2025.2468191.

Received 27.09.2025

Information about the authors:

Lyubov Melnikova – Ph.D. (Technical Sciences), Associate Professor, Department of Infocommunication Engineering V.V. Popovsky, Kharkiv National University of Radio Electronics, Ukraine; e-mail: liubov.melnikova@nure.ua; ORCID: <https://orcid.org/0000-0003-0439-7108>

Olena Linnyk – Ph.D. (Technical Sciences), Associate Professor, Department of Physical Foundations of Electronic Engineering, Kharkiv National University of Radio Electronics, Ukraine; e-mail: elena.linnyk@nure.ua; ORCID: <https://orcid.org/0000-0002-4906-3796>

Svitlana Shtangei – Ph.D. (Technical Sciences), Associate Professor, Department of Infocommunication Engineering V.V. Popovsky, Kharkiv National University of Radio Electronics, Ukraine; e-mail: svitlana.shtanhei@nure.ua; ORCID: <https://orcid.org/0000-0002-9200-3959>.

В.М. БЕЗРУК, д-р техн. наук, Ю.М. ГОЛОБОРОДЬКО, канд. техн. наук,

В.І. ЗАБОЛОТНИЙ, канд. техн. наук

ВИЯВЛЕННЯ НОВИХ РАДІОВИПРОМІНЮВАНЬ ПРИ АВТОМАТИЗОВАНОМУ РАДІОКОНТРОЛІ

Вступ

Під час проведення автоматизованого радіоконтролю важливим завданням є виявлення нових радіовипромінювань (РВ) в аналізованих частотних каналах [1–3]. З точки зору обробки сигналів, це завдання виявлення нових сигналів на тлі заданої стаціонарної завади. Таку задачу можна розглядати як задачу виявлення зміни ймовірнісних властивостей випадкових сигналів, що є інтенсивно розвиненим напрямом у математичній статистиці.

При цьому до появи нового РВ у каналі спостерігається лише стаціонарна завада з відомими ймовірнісними властивостями. Після появи нового, невідомого РВ в аналізованому каналі, ймовірнісні властивості спостережуваного сигналу змінюються. Завдання виявлення нового сигналу з невідомими ймовірнісними властивостями на тлі заданої завади є окремим випадком завдання виявлення сигналів в умовах підвищеної апіорної невизначеності [4].

У статті досліджуються методи виявлення нових сигналів з невідомими ймовірнісними властивостями на тлі заданої завади для випадку, коли спостереження представляються ймовірнісною моделлю у вигляді ортогональних розкладів. Наведено результати досліджень робочих характеристик виявлення, які були проведені шляхом статистичних випробувань на вибірках реальних сигналів та завад.

Постановка задачі виявлення нових сигналів на тлі заданої завади

Припускається, що випадкові сигнали, які спостерігаються на інтервалі часу $(0, T)$, представляються скінченновимірними векторами спостережень $\mathbf{x}$. При переході від одного інтервалу спостереження до наступного ймовірнісні властивості сигналів можуть різко змінюватися. Введемо дві гіпотези:

- H^0 – гіпотеза про спостереження сигналу до зміни його ймовірнісних властивостей;
- H^1 – гіпотеза про спостереження сигналу зі зміненими ймовірнісними властивостями.

Ймовірності гіпотез відповідно P_0 і P_1 ($P_0 + P_1 = 1$).

Нехай щільність розподілу статистик сигналу за умови справедливості гіпотези H^0 є гаусівською $N(\mathbf{x}/\boldsymbol{\mu}^0, \mathbf{R}^0)$ з невідомим середнім вектором $\boldsymbol{\mu}^0$ та кореляційною матрицею $\mathbf{R}^0$. Задається навчальна вибірка спостережень $\{\mathbf{x}_r^0, r = \overline{1, n_0}\}$, яка отримана до зміни ймовірнісних властивостей сигналу і може бути використана для оцінювання параметрів розподілів $\boldsymbol{\mu}^0$, $\mathbf{R}^0$. Щільність розподілу статистик сигналу після зміни його властивостей невідома, і відсутня можливість отримання відповідної вибірки для оцінювання його ймовірнісних властивостей.

Поставлена задача вирішується у два етапи. Спочатку знаходиться алгоритм виявлення за скороченою сукупністю показників $k_1(\alpha), k_2(\alpha)$, які визначаються відповідно ймовірністю хибної тривоги та об'ємом критичної області відхилення гіпотези H^1 . Далі на основі отриманого рішення формується деяка множина допустимих, повністю описаних алгоритмів виявлення [5].

Алгоритми виявлення зміни ймовірнісних властивостей сигналів

Оптимізація виявника зміни ймовірнісних властивостей сигналів зводиться до варіаційної задачі забезпечення мінімального значення показника хибної тривоги $k_1(\alpha)$ за фіксованого об'єму критичної області відхилення гіпотези H^1 , який характеризується показником $k_2(\alpha)$. Отриманий при цьому алгоритм виявлення змін ймовірнісних властивостей сигналів для випадку гаусівських розподілів визначається таким вирішальним правилом:

$$H^1: P_0 N(\mathbf{x}/\mu^0, \mathbf{R}^0) < \lambda \quad (1a)$$

- приймається гіпотеза про зміну властивостей сигналу;

$$H^0: P_0 N(\mathbf{x}/\mu^0, \mathbf{R}^0) \geq \lambda \quad (1б)$$

- відхиляється гіпотеза про зміну властивостей сигналу.

Тут λ – поріг, який визначається при розв'язанні зазначеного варіаційного завдання за умови забезпечення заданого значення ймовірності хибної тривоги.

З урахуванням аналітичного виразу для гаусівського розподілу вектора ухвалення рішень за допомогою вирішального правила (1) зводиться до порівняння відстані Махаланобіса з деяким порогом:

$$H^1: (\mathbf{x} - \mu^0)^T (\mathbf{R}^0)^{-1} (\mathbf{x} - \mu^0) > \Delta^0, \quad (2a)$$

- приймається гіпотеза про зміну властивостей сигналу;

$$H^0: (\mathbf{x} - \mu^0)^T (\mathbf{R}^0)^{-1} (\mathbf{x} - \mu^0) \leq \Delta^0. \quad (2б)$$

- відхиляється гіпотеза про зміну властивостей сигналу.

Тут $\mu^0, \mathbf{R}^0$ – оцінки середнього вектора та кореляційної матриці, отримані за навчальною вибіркою сигналу до зміни його ймовірнісних властивостей; Δ^0 – деяке порогове значення.

На основі отриманого вирішального правила може бути сформована деяка множина допустимих алгоритмів виявлення ймовірнісних властивостей сигналів у рамках опису спостережень в аналізованому каналі ймовірнісною моделлю у вигляді ортогональних розкладів. Зокрема, вирішальне правило типу (2) може бути отримано в координатній області, коли спостереження сигналів представляються вектором коефіцієнтів розкладів $\mathbf{b}$ у деякому ортонормованому базисі:

$$H^1: (\mathbf{b} - \mu_b^0)^T (\mathbf{R}_b^0)^{-1} (\mathbf{b} - \mu_b^0) > \Delta_b^0, \quad (3a)$$

$$H^0: (\mathbf{b} - \mu_b^0)^T (\mathbf{R}_b^0)^{-1} (\mathbf{b} - \mu_b^0) \leq \Delta_b^0, \quad (3б)$$

де $\mathbf{b}, \mu_b^0, \mathbf{R}_b^0$ – відображення відповідно $\mathbf{x}, \mu^0, \mathbf{R}^0$ у координатну область, що визначається обраним базисом з розмірністю L .

Вибираючи базис Карунена–Лоева, який призводить до некорельованих координат, отримуємо вирішальне правило у вигляді співвідношення:

$$H^1: \sum_{j=1}^N \frac{(c_j - \mu_{jc}^0)^2}{(\sigma_{jc}^0)^2} > \Delta_c^0; \quad H^0: \sum_{j=1}^N \frac{(c_j - \mu_{jc}^0)^2}{(\sigma_{jc}^0)^2} \leq \Delta_c^0, \quad (4)$$

де $(\sigma_{jc}^0)^2 = \lambda_j$ – власні числа вибіркової кореляційної матриці сигналу $\mathbf{R}^0$ до зміни його властивостей, c_j – координати представлення вектора спостережень сигналу $\mathbf{x}$ розмірністю L у базисі Карунена–Лоева з розмірністю $N < L$.

При забезпеченні відповідних нормувань, що призводять до рівності дисперсій у координатному представленні сигналів, може бути використано простіше вирішальне правило:

$$H^1: \sum_{j=1}^N (c_j - \mu_{jc}^0)^2 > \Delta_c^0; \quad H^0: \sum_{j=1}^N (c_j - \mu_{jc}^0)^2 \leq \Delta_c^0. \quad (5)$$

Якщо рішення приймається за вибіркою об'ємом v реалізацій $\mathbf{X}_v$, вирішальне правило (4) набуває такого вигляду:

$$H^1: \sum_{r=1}^v \sum_{j=1}^N \frac{(c_{jr} - \mu_{jc}^0)^2}{(\sigma_{jc}^0)^2} > \Delta_{cv}^0; \quad H^0: \sum_{r=1}^v \sum_{j=1}^N \frac{(c_{jr} - \mu_{jc}^0)^2}{(\sigma_{jc}^0)^2} \leq \Delta_{cv}^0. \quad (6)$$

Вибираючи статистики (інформативні ознаки) сигналів у вигляді сукупності координат енергетичних спектрів сигналів у деякому ортонормованому базисі, аналогічно (5) отримуємо вирішальне правило, засноване на порівнянні евклідових відстаней поточних оцінок енергетичного спектра до еталонів:

$$H^1: \sum_{j=1}^N (G_j - G_{jc}^0)^2 > \Delta_G^0; \quad H^0: \sum_{j=1}^N (G_j - G_j^0)^2 \leq \Delta_G^0. \quad (7)$$

Тут $G_j^0 = \frac{1}{n_0} \sum_{r=1}^{n_0} (c_{jr}^0 - \mu_{jc}^0)^2$, $j = \overline{1, N}$ – оцінки координат енергетичного спектра сигналу до зміни ймовірнісних властивостей, знайдені за навчальною вибіркою об'ємом n_0 реалізацій;
 $G_j = \frac{1}{v} \sum_{r=1}^v (c_{jr} - \mu_{jc}^0)^2$, $j = \overline{1, N}$ – поточна оцінка енергетичного спектра спостережуваного сигналу, знайдена за вибіркою об'ємом $v \ll n_0$.

Наведені вирішальні правила визначають деякі можливі алгоритми виявлення зміни властивостей випадкових сигналів, що отримуються в рамках ймовірнісної моделі у вигляді ортогональних розкладів. Вони можуть бути використані при багатокритеріальній оптимізації алгоритмів виявлення. При цьому для кожного варіанта алгоритму виявлення слід оцінити значення показників якості виявлення змін ймовірнісних властивостей сигналів, а також значення показників реалізаційних витрат. У результаті допустима множина алгоритмів виявлення буде представлена в критеріальному просторі введених показників якості. Тут з використанням безумовного критерію переваги виключаються безумовно гірші варіанти та виділяється підмножина Парето-оптимальних алгоритмів виявлення зміни ймовірнісних властивостей сигналів. Оскільки Парето-оптимальні алгоритми виявлення є непорівнянними між собою, в подальшому для практичної реалізації може бути обраний будь-який з них.

Результати експериментальних досліджень алгоритмів виявлення нових РВ

Дослідження алгоритмів виявлення нових РВ на тлі заданої стаціонарної завади виконано шляхом статистичних випробувань на вибірках реалізацій реальних сигналів та завад. Схема установки для прийому та формування вибірок реальних сигналів і завад включала: радіоприймальний пристрій для прийому РВ у короткохвильовому діапазоні, магнітофон для запису реалізацій сигналів і завад з виходу радіоприймального пристрою, аналізатор спектра, аналого-цифровий перетворювач та пристрій введення спектральних відліків сигналів і завад в ЕОМ.

Були сформовані навчальні вибірки стаціонарних завад об'ємом по 100 реалізацій для 22 різних дослідів. Ці навчальні вибірки були використані для оцінювання параметрів вирішального правила. Результати досліджень наведено для випадку використання алгоритму виявлення нових сигналів, заснованого на вирішальному правилі (7).

Для оцінювання показників якості виявлення нових РВ на тлі стаціонарної завади були накопичені контрольні вибірки реалізацій сигналів та стаціонарних завад об'ємом по 100 реалізацій. Для ілюстрації на рис. 1 наведено усереднені спектри стаціонарних завад (а) та сигналів (б) у частотному каналі зі смугою 3 кГц для двох різних дослідів.

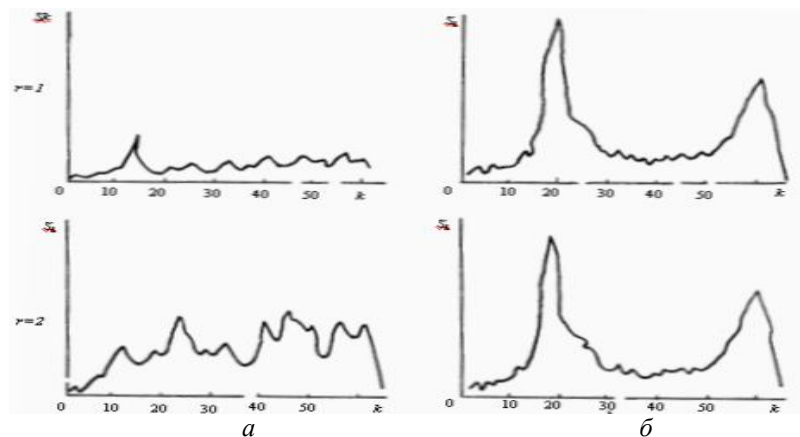


Рис. 1. Усереднені спектри стаціонарних завад (а) та сигналів (б) у частотних каналах для двох різних дослідів

Навчальні вибірки реалізацій стаціонарних завад були використані для оцінювання параметрів алгоритмів виявлення. Контрольні вибірки реалізацій сигналів і завад об'ємом по 100 реалізацій використані для отримання показників якості виявлення сигналів.

У табл. 1 наведено ймовірності правильного виявлення нових сигналів P_{no}^j при фіксованих ймовірностях хибної тривоги $P_{лт}'' = 10^{-1}; 10^{-2}$ для різних видів стаціонарних завад і сигналів у кожному досліді.

Таблиця 1

Ймовірності правильного виявлення нових сигналів, отримані для різних дослідів

Номер досліду j	P_{no}^j	
	a	b
2	1.0	0.97
3	0.99	0.95
4	1.0	0.9
5	0.98	0.93
6	1.0	1.0
7	1.0	1.0
8	1.0	0.82
9	1.0	1.0
10	1.0	0.89
11	1.0	1.0
12	1.0	1.0
13	1.0	1.0
14	1.0	1.0
15	1.0	1.0
16	1.0	0.89
17	1.0	1.0
18	1.0	1.0
19	1.0	1.0
20	1.0	0.61
21	1.0	1.0
22	1.0	1.0
P_{nocp}	0,99	0,95

Примітка: результати отримано при $P_{лт}'' = 10^{-1}; 10^{-2}$ (відповідно стовпці a і b).

Ці характеристики представлено у вигляді оцінок ймовірності правильного виявлення нових сигналів при фіксованій ймовірності хибної тривоги в заданій смузі частотного каналу. На рис. 2 наведено робочі характеристики у вигляді залежності ймовірності правильного виявлення нових сигналів від тривалості спостережень для 8 різних дослідів, а також усереднена характеристика виявлення.

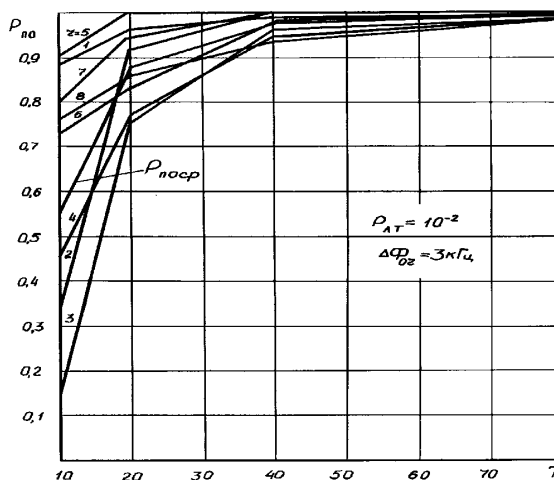


Рис. 2. Залежності ймовірності правильного виявлення нових сигналів від часу спостереження при фіксованій ймовірності хибної тривоги для 8 різних дослідів

Висновки

1. Задача виявлення нових РВ на тлі стаціонарної завади вирішується як виявлення зміни ймовірнісних властивостей сигналів у частотному каналі..
2. Наведено алгоритми виявлення невідомих сигналів на тлі заданої завади для випадку гаусівських розподілів спостережень..
3. Отримано результати експериментальних досліджень алгоритмів виявлення нових РВ на тлі стаціонарної завади з використанням вибірок реальних сигналів та завад.
4. Запропоновані алгоритми виявлення нових РВ на тлі заданих стаціонарних завад можуть бути використані при вирішенні завдань автоматизованого радіоконтролю.

Список літератури:

1. Майборода І. М., Власов К. В., Глушенко М. О., Застосування і перспективи розвитку мобільних засобів радіоелектронної розвідки тактичної ланки сил сектору безпеки та оборони України // Честь і закон. 2024. No 2 (89). С. 83–90; https://dspace.nlu.edu.ua/jspui/bitstream/123456789/20200/1/Vlasov_83%E2%80%939390.pdf.
2. Слободянюк П.В., Благодарный В.Г. Радиомониторинг: вчера, сегодня, завтра (Теория и практика построения системы радиомониторинга). Прилуки : ООО «Издательство «Айр-Поліграф», 2010. 296 с.
3. Обухов Н. П., Кикоть А. В., Голобородько Ю. Н., Горбачинский И. С., Авторское свидетельство № 177720 от 09.04.82 «Устройство автоматического панорамного обнаружения и пеленгования с дискриминацией радиоизлучений источников дальней или ближней зоны».
4. Omelchenko V. A., Balabanov V. V., Bezruk V. M., Goloborod'ko Ju. N. Detection of Changes in the Random Signal Properties by Spectral Methods Under the Conditions of A Priori Uncertainty // Telecommunications and Radio Engineering. 1999. Vol. 53 (9 -10). P. 1–10.
5. Безрук В.М., Певцов Г.В. Теоретические основы проектирования систем распознавания сигналов для автоматизированного радиоконтроля. Харьков : Коллегиум, 2007. 430 с.

Надійшла до редколегії 27.09.2025

Відомості про авторів:

Безрук Валерій Михайлович – доктор технічних наук, професор, Харківський національний університет радіоелектроніки, професор кафедри інформаційно-мережної інженерії; Україна; email: valerii.bezruk@nure.ua; ORCID: <https://orcid.org/0000-0002-5482-9960>

Голобородько Юрій Миколайович – кандидат технічних наук, Харківський національний університет радіоелектроніки, доцент кафедри безпеки інформаційних технологій; Україна; email: yurii.holoborodko@nure.ua; ORCID: <https://orcid.org/0009-0007-4040-9467>

Заболотний Володимир Ілліч – кандидат технічних наук, доцент, Харківський національний університет радіоелектроніки, професор кафедри безпеки інформаційних технологій, Україна; email: volodymyr.zabolotnyi@nure.ua; ORCID: <https://orcid.org/0000-0003-3258-8489>

КРИТИЧНИЙ АНАЛІЗ ВІДОМИХ МЕТОДІВ НАВЕДЕННЯ РАКЕТ

Вступ

Одним з центральних завдань, що стоять перед розробниками нових систем ПВО/ПРО, є вибір доцільного метода наведення, використання якого дозволить отримувати найкращі показники зі знищення ворожих цілей. При цьому виникають питання: які властивості мають бути у обраного метода наведення та чи мають існуючі методи всі такі властивості?

Метою даної статті є, з одного боку, спроба відповісти на ці питання, та з іншого боку, визначити завдання, які з цього випливають.

Коротка характеристика відомих методів наведення

Відомі стратегії наведення розроблено для військового призначення. Їх дослідженню присвячено багато спеціалізованої літератури, в тому числі [1–4, 7–9]. Методи, що лежать в основі таких стратегій, можна розподілити на дві підгрупи [4]:

- методи з фіксованим положенням необхідного напрямлення вектору швидкості відносно лінії «ракета – ціль» (до таких методів належать *метод погоні* та *метод постійного випередження*);

- методи зі змінним положенням необхідного напрямлення вектору швидкості відносно лінії «ракета – ціль» (до таких методів належать *метод пропорційного зближення* та *метод паралельного зближення*).

Тут і далі під *методом наведення* будемо розуміти [4] заданий закон зближення ракети з ціллю, який в залежності від координат і параметрів руху цілі визначає потрібний рух ракети, який забезпечує потрапляння ракети в ціль. Теоретичну траєкторію ракети, що визначається алгоритмом метода наведення, прийнято називати *кінематичною траєкторією*.

Коротко розглянемо зазначені методи наведення.

Методом погоні називають такий метод наведення, при якому в кожний момент часу вектор швидкості ракети направлений на ціль (рис. 1).

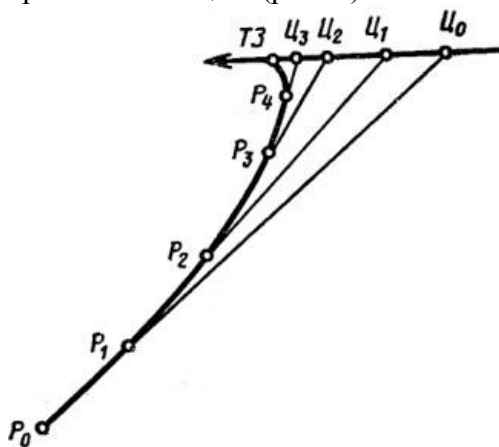


Рис. 1. Кінематична траєкторія польоту ракети за методом погоні (адаптовано з [4])

На рисунку точками $\mathcal{C}_0, \mathcal{C}_1, \mathcal{C}_2, \dots$ та $P_0, P_1, P_2, \dots$ позначено положення цілі та ракети через достатньо малі проміжки часу Δt , де положення ракети відносно цілі в кожний такий момент часу показано за допомогою відповідних прямих ліній. З'єднавши точки $P_0, P_1, P_2, \dots$, отримаємо кінематичну траєкторію польоту ракети за методом погоні. За методом погоні ракета, незалежно від початкових умов, підходить до точки зустрічі (на рис. 1 – ТЗ) з ціллю строго у її хвіст.

Як зазначено в [2, 4], метод погоні дає прийнятні за точністю наведення результати лише при обстрілі малорухомих та нерухомих цілей, або при стрільбі вдогін. Використання методу погоні у якості стратегії переслідування призводить до того, що траєкторія польоту ракети буде криволінійною за винятком двох окремих випадків (при пуску ракети точно вдогін цілі або точно назустріч цілі).

Метод постійного випередження (або метод наведення з постійним кутом випередження) – це метод наведення, при якому необхідний рух ракети визначається умовою, що протягом всього часу польоту ракети до точки зустрічі кут між вектором швидкості ракети і лінією «ракета – ціль» (кут випередження) залишається постійним (рис. 2).

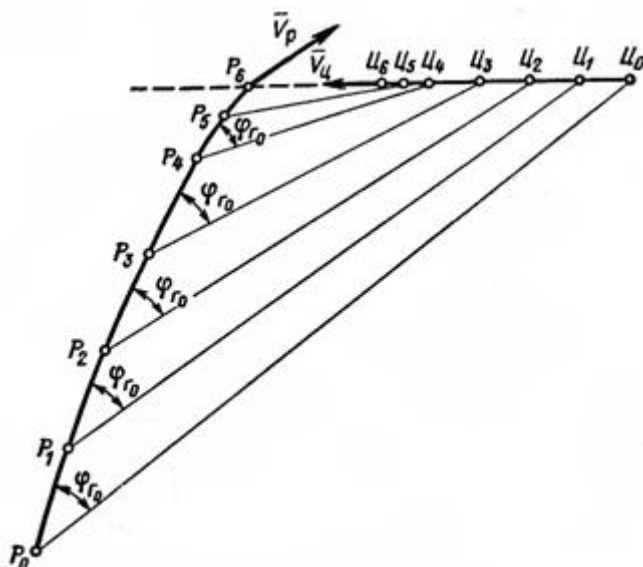


Рис. 2. Кінематична траєкторія польоту ракети за методом постійного випередження (адаптовано з [4])

На рис. 2 точки $\mathcal{C}_0$ та P_0 визначають розташування цілі та ракети на початку процесу наведення. Кут випередження ϕ_{r0} , що визначається як різниця між кутом напрямку руху ракети та кутом лінії «ракета – ціль», є постійним та має позитивне значення і призначається на початку процесу наведення. Для побудови траєкторії руху ракети за методом постійного випередження траєкторія цілі розбивається на достатньо малі відрізки шляху, які дорівнюють $\bar{V}_\mathcal{C} \Delta t$. Для знаходження положення ракети в момент часу t_1 необхідно з'єднати точки P_0 та $\mathcal{C}_0$, побудувати відносно прямої $P_0\mathcal{C}_0$ кут випередження ϕ_{r0} та відкласти на утвореній лінії відрізок шляху, що проходить ракета за час $\Delta t = t_1 - t_0$ $\Delta t = t_1 - t_0$.

На рис. 2 утворену точку позначено як P_1 . Для точок $P_2, P_3, P_4, \dots$ виконуються аналогічні побудови. З'єднуючи точки $P_0, P_1, P_2, \dots$, отримуємо кінематичну траєкторію польоту ракети за методом постійного випередження.

Використання методу постійного випередження є ефективним у випадку зустрічних курсів цілі та ракети. При цьому кінематична траєкторія польоту ракети буде криволінійною.

Метод пропорційного зближення – це метод наведення, при якому протягом всього часу польоту ракети до цілі кутова швидкість повороту вектору швидкості ракети залишається пропорційною кутовій швидкості лінії «ракета – ціль» (рис. 3).

Нехай ціль рухається прямолінійно та рівномірно і в момент початку наведення t_0 знаходиться в точці $\mathcal{C}_0$ (рис. 3). Через достатньо малі проміжки часу Δt ціль проходить відстань $\bar{V}_\mathcal{C} \Delta t$. Положення цілі через моменти часу $t_1, t_2, \dots, t_1, t_2, \dots$ позначено точками $\mathcal{C}_1, \mathcal{C}_2, \dots$. Ракета в момент початку наведення знаходиться в точці P_0 і летить з постійною швидкістю $\bar{V}_p$ точно на ціль.

Через проміжок часу $\Delta t = t_1 - t_0$ ракета долетить до точки P_1 і при цьому лінія P_1C_1 повернеться у просторі відносно лінії P_0C_0 на деякий кут θ_1 (на рисунку умовно не показаний), який відповідає кутовій швидкості повороту вектору швидкості ракети у відповідній площині управління. Далі через проміжок часу $\Delta t = t_2 - t_1$ ракета переміститься в точку P_2 , лінія P_2C_2 повернеться у просторі відносно лінії P_1C_1 на деякий кут θ_2 . Для точок $P_3, P_4, P_5, \dots$ виконуються аналогічні побудови. З'єднуючи точки $P_0, P_1, P_2, \dots$, отримуємо кінематичну траєкторію польоту ракети за методом пропорційного зближення. Особливістю метода є те, що кутова швидкість θ_i повороту вектору швидкості ракети у i -й площині управління завжди буде пропорційна кутовій швидкості ϕ_i повороту лінії «ракета-ціль» у цій же площині управління. При виконанні умови, що $\theta_i = \phi_i$, метод зводиться до метода погоні, а при виконанні умови, що $\theta_i = 0$, – до метода паралельного зближення (див. нижче).

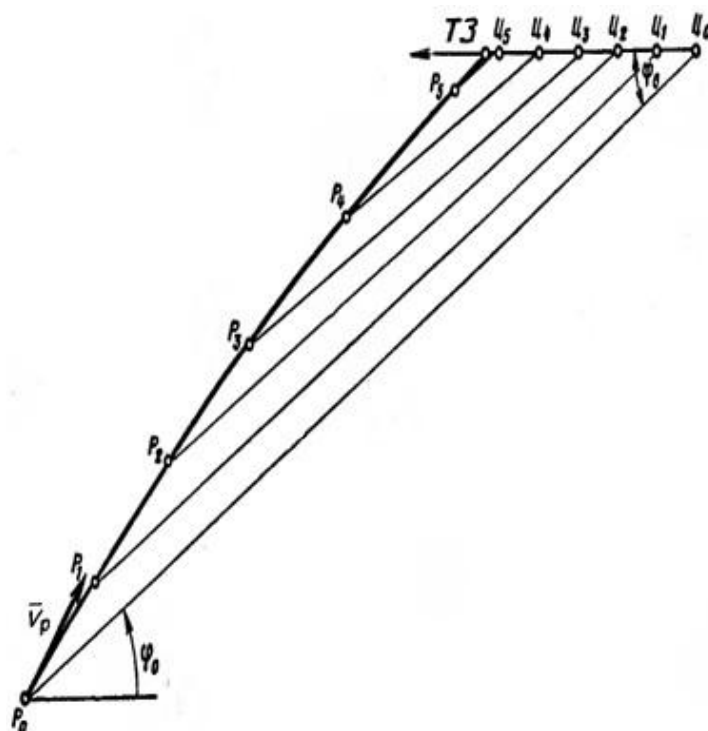


Рис. 3. Кінематична траєкторія польоту ракети за методом пропорційного зближення (адаптовано з [4])

Метод пропорційного зближення отримав широке використання для розв'язання задач наведення ракет. Його дослідженню присвячено багато літературних джерел, зокрема [1, 7–9]. Цей метод доцільно використовувати у випадку зустрічних курсів цілі та ракети або при стрільбі вдогін. За цього методу кінематична траєкторія польоту ракети займає проміжне місце між траєкторією за методом погоні та траєкторією за методом паралельного зближення.

Метод паралельного зближення – це метод наведення [4], при якому протягом всього часу польоту ракети до точки зустрічі лінія «ракета – ціль» залишається паралельною заданому напрямленню (тобто $\varphi = \text{const}$ – рис. 4).

Для графічної побудови кінематичної траєкторії польоту ракети при наведенні її за методом паралельного зближення необхідно задати рух цілі та швидкість ракети як функцію часу. Нехай рух цілі задано прямою (рис.4), на якій точками $C_0, C_1, C_2, \dots$ відмічені послідовні положення цілі в моменти часу $t_0, t_1, t_2, \dots$. Ракета в початковий момент часу t_0 знаходиться в точці P_0 . Пряма P_0C_0 відповідає початковому положенню лінії «ракета – ціль».

Для побудови кінематичної траєкторії за методом паралельного зближення необхідно з точок $C_1, C_2, C_3, \dots$ провести сімейство прямих, паралельних прямій P_0C_0 , визначити значення

кута доцільного напрямку руху ракети за формулою $\phi = \arcsin\left(\frac{\bar{V}_C}{\bar{V}_P} \sin \beta\right)$

$\phi = \arcsin\left(\frac{\bar{V}_C}{\bar{V}_P} \sin \beta\right)$, відкласти його відносно лінії P_0C_0 та провести пряму під цим кутом від точки P_0 до перетину з лінією руху цілі в точці $TЗ$ (точки зустрічі – див. рис. 4). Точки перетину цієї прямої з сімейством проведених прямих позначити як $P_1, P_2, P_3, \dots$. Пряма, що з'єднує точки $P_0, P_1, P_2, \dots$ з точкою $TЗ$, утворює кінематичну траєкторію польоту ракети за методом паралельного зближення. Отже, якщо ціль рухається рівномірно та прямолінійно ($\bar{V}_C = \bar{V}_C = \text{const}$), а ракета має постійну швидкість польоту ($\bar{V}_P = \bar{V}_P = \text{const}$), то кут ϕ не буде змінюватись у часі, що означає, що для даних умов наведення кінематична траєкторія ракети буде прямою лінією. При цьому кажуть, що вектор швидкості ракети направлений у миттєву точку зустрічі, під якою розуміють точку, в якій би відбулась зустріч ракети з ціллю, якщо б починаючи з даного моменту часу ракета і ціль рухались би прямолінійно та рівномірно. Відповідно до цього метод паралельного зближення також називають *методом наведення у миттєву точку зустрічі*.

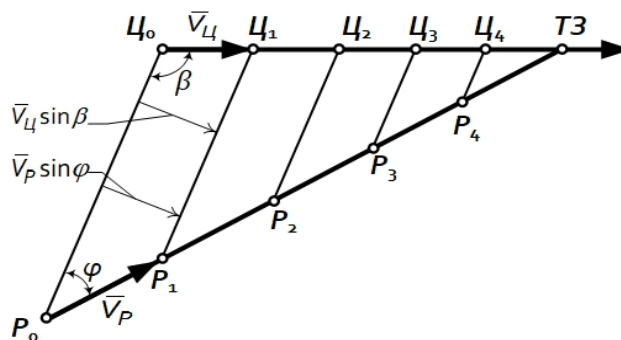


Рис. 4. Кінематична траєкторія польоту ракети за методом паралельного зближення

Таким чином, за даним методом ракета направляється не на ціль, а на точку зустрічі ракети при різних курсах цілі, в тому числі і для ураження високошвидкісних цілей на з ціллю, і її рух утворює пряму кінетичну траєкторію польоту. Цей метод доцільно використовувати зустрічних курсах.

Основні вимоги, що пред'являються до методів наведення ракет

В [4] наведено такі основні вимоги:

1. Метод наведення має забезпечувати найменшу кривизну кінематичної траєкторії на всіх ділянках польоту, особливо в районі точки зустрічі. Зокрема, спрямлення кінематичної траєкторії приводить до зменшення шляху та польотного часу ракети до цілі, що дозволяє покращити характеристики ракети та підвищити вогневу продуктивність зенітно-ракетного комплексу.

2. Метод наведення має забезпечувати зустріч ракети з повітряною ціллю по всіх заданих діапазонах швидкостей, висот та курсових параметрів її руху. Так, швидкість руху повітряної цілі може дорівнювати від десятків до тисяч метрів в секунду, а висота розташування – від десятків метрів до десятків кілометрів. Напрями руху цілей теж можуть бути будь-які. Тому метод наведення має враховувати можливий широкий діапазон зміни координат цілі, напрямів та швидкості її руху.

3. Метод наведення має забезпечувати потрібну точність зближення ракети з ціллю у різних умовах її запуску. Може статися, що пілотована повітряна ціль виявила запуск ракети та намагається запобігти ураженню шляхом використання протиракетного маневру. Тому

важливо, щоби метод наведення міг би дозволяти оптимізувати кінематичну траєкторію ракети з метою перехоплення цілі, що маневрує.

4. Метод наведення має бути достатньо простим для забезпечення його програмно-апаратної реалізації.

Аналіз методів наведення ракет з точки зору зазначених вимог

Проаналізуємо розглянуті методи наведення з точки зору наведених вимог.

Очевидно, що вимога 1 задовольняється лише у випадку розгляду метода паралельного зближення, і, відповідно, не задовольняється при розгляді інших трьох методів, використання яких призводить до формування криволінійної кінематичної траєкторії.

Вимога 2 може бути задоволена при розгляді методів пропорційного зближення та паралельного зближення, і, відповідно, не задовольняється у випадку розгляду метода погоні (за якого наведення здійснюється лише в напрямку стрільби вдогін) та метода постійного випередження (за якого наведення здійснюється лише при зустрічних курсах цілі та ракети).

Вимога 3 в більшій степені може бути задоволена при розгляді метода пропорційного зближення, ніж інших методів, оскільки цей метод дозволяє краще враховувати ситуації, коли відбуваються зміни у поведінці цілі.

І, нарешті, вимога 4 задовольняється при розгляді метода пропорційного зближення та метода паралельного зближення. При цьому відомо [3], що метод пропорційного зближення ідеально підходить для апаратної реалізації метода паралельного зближення.

Таким чином, узагальнюючи викладене, можна стверджувати, що жодний з розглянутих методів наведення одночасно не задовольняє всім зазначеним вимогам.

Визначення задач досліджень

З викладеного стає очевидною актуальність задачі розроблення нового метода наведення, який має одночасно задовольняти всім вищенаведеним вимогам. З проведеного аналізу випливає, що новий метод має бути розвитком метода паралельного зближення як метода, що в найбільшій мірі задовольняє вищенаведеним вимогам.

Окрім цих вимог до розроблюваного метода треба пред'явити додаткові вимоги.

Як відомо [4], управління ракетою здійснюється у двох взаємно перпендикулярних площинах. Як наслідок, створюваний метод має формувати доцільні кути напрямку руху ракети як їх проекції на ці площини (тобто кути у площинах XOY та XOZ), де напрям руху має бути направлений на точку зустрічі у 3D-просторі з ціллю.

Зазначимо, що всі розглянуті методи призначені для використання у тривимірному просторі. Однак в дійсності розгляд кожного з них виконується на площині, утвореній напрямками руху цілі та ракети, а не у двох взаємно перпендикулярних площинах, що, на нашу думку, ускладнює процес управління рухом ракети, оскільки не дозволяє забезпечити своєчасне реагування на зміну напрямку руху цілі із площини.

Для запобігання таких ситуацій необхідно, щоби створюваний метод ґрунтувався на агентно-орієнтованому підході [5], в рамках якого ракета та ціль розглядаються як мобільні агенти, де ціль виступає як утікач, в ракета – як переслідувач. Однією з властивостей агента-переслідувача має бути те, що він є реактивним, тобто здатним своєчасно реагувати на зміну поведінки (напрямку руху та/або швидкості) агента-утікача та перевизначати свою поведінку з метою перехоплення агента-утікача.

Як зазначено вище, в основі створюваного метода наведення має бути метод паралельного зближення. Однак у цього метода є недоліки, які не дозволяють його використовувати для формування оптимальної стратегії переслідування з точки зору агентно-орієнтованого підходу: по-перше, цей метод орієнтований тільки на простий рух утікача (тобто прямолінійний рух з постійною швидкістю); по-друге, цей метод явно не використовує ортогональної системи координат, що необхідно для постановки задачі наведення у тривимірному просторі, в рамках якої, як зауважено вище, управління ракетою здійснюється у двох взаємно перпендикулярних площинах, що безпосередньо передбачає використання у цих площинах ортогональної системи координат.

У якості метода, що не має таких недоліків та може виступати основою для створення нового метода наведення у тривимірному просторі, слід розглядати метод агентного переслідування, запропонований в [5, 6], де також доведено, що цей метод зводиться як до метода паралельного зближення, так і до метода кола Аполлонія.

Висновки

Виконано критичний аналіз відомих методів наведення ракет, в тому числі метода погоні, метода постійного випередження, метода пропорційного зближення та метода паралельного зближення. При цьому наведено основні властивості цих методів та визначено ситуації, при яких ці методи доцільно використовувати. Визначено основні вимоги, що традиційно пред'являються до таких методів, та здійснено аналіз їх задовільнення цим вимогам. Встановлено, що жодний з розглянутих методів наведення одночасно не задовольняє всім таким вимогам. На основі виконаного аналізу обґрунтовано актуальність та доцільність розроблення нового метода наведення, який має задовольняти всім зазначеним вимогам.

Список літератури:

1. Кан В.Л., Кельзон А.С. Теория пропорциональной навигации. Л. : Судостроение, 1965. 423 с.
2. Куркоткин В.И., Стерлигов В.Л. Самонаведение ракет. М. : Воениздат, 1963. 88 с.
3. Локк А.С. Управление снарядами. М. : Гос. изд-во техн.-теорет. лит-ры, 1957. 775 с.
4. Неупокоев Ф.К. Стрельба зенитными ракетами. М. : Воениздат, 1991. 343 с.
5. Яловець А.Л. Мультиагентне моделювання переслідування на площині: від теорії до програмної реалізації. К. : Наук. думка, 2019. 165 с.
6. Яловець А.Л. Про один метод переслідування на площині // Проблеми програмування. 2013. № 3. С. 117–124.
7. Balakrishnan S.N., Tsourdos A., & White B.A. (Eds.). Advances in Missile Guidance, Control, and Estimation // CRC Press, 2013. 722 p. DOI: 10.1201/b12503
8. Siouris G.M. Missile Guidance and Control Systems. Springer, 2004. 681 p. DOI: 10.1002/rnc.1056
9. Yanushevsky R. Modern Missile Guidance. CRC Press, 2018. 343 p. DOI: 10.1201/9781351202954

Надійшла до редколегії 11.10.2025

Відомості про авторів:

Романенко Ігор Олександрович – д-р техн. наук, професор, Інститут проблем математичних машин і систем НАН України, провідний науковий співробітник, Україна, e-mail: zzz223@ukr.net, ORCID: <https://orcid.org/0000-0001-5339-7900>

Яловець Андрій Леонідович – д-р техн. наук, с.н.с., Інститут проблем математичних машин і систем НАН України, головний науковий співробітник, Україна, e-mail: andriy.yalovets@gmail.com, ORCID: <http://orcid.org/0000-0001-6542-3483>

*А.А. СОКОЛОВ, д-р філософії, О.Г АВРУНІН, д-р техн. наук,
Я.В. НОСОВА, канд. техн. наук, Т.В. НОСОВА, канд. техн. наук*

**ОЦІНКА ЕФЕКТИВНОСТІ ВИЗНАЧЕННЯ ВІДСТАНІ ЗАСОБАМИ
ФРЕЙМВОРКУ ARCORE В УМОВАХ НИЗЬКОГО ОСВІТЛЕННЯ**

Вступ

Розвиток сучасних біомедичних систем вимагає накопичення експериментальних даних, що дозволяють підтвердити працездатність нових алгоритмів та апаратних рішень. Теоретичні моделі не враховують усі реальні чинники, тоді як реальні вимірювання відображають вплив зовнішніх чинників і технологічних обмежень, які неможливо врахувати повністю при побудові моделі.

Особливе значення мають дослідження, спрямовані на отримання кількісних характеристик вузлів системи, оскільки саме вони забезпечують базу для подальшої оптимізації конструкцій та алгоритмів обробки даних. Експериментальні дані дозволяють оцінити стабільність роботи, рівень завадостійкості, відтворюваність результатів і визначити напрямки вдосконалення.

Дана робота є логічним продовженням попередніх праць у напрямку створення навігаційних систем на базі фреймворку ARCore [1–3]. Метою представленої роботи є демонстрація результатів експериментальних досліджень ефективності вимірювання відстані за допомогою смартфона в умовах низького освітлення.

Опис умов експерименту

Експериментальні дослідження проводилися в умовах затемненого приміщення з контрольованими параметрами освітлення. У якості тестового пристрою використовувався смартфон POCO X5 Pro із попередньо встановленим прототипом мобільного застосунку, розробленого для оцінки глибини сцени на основі ARCore. Для забезпечення точного вимірювання відстані та фіксації умов експерименту додатково використовувалися фотометр Екотензор-03 та лазерний далекомір INKERSI KE50, що був еталоном значень відстані [4, 5], рис. 1.

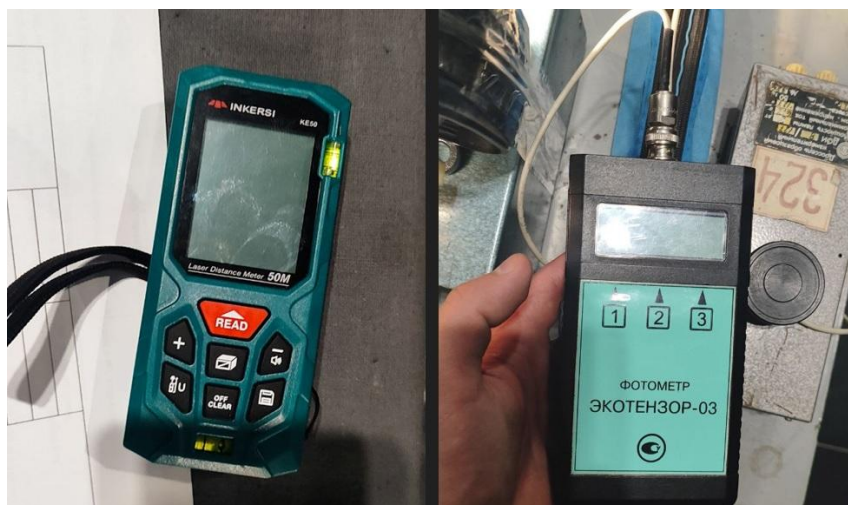


Рис. 1. Використане у експерименті обладнання

Для імітації типових об'єктів реального світу було обрано три цілі, що відрізняються за структурою та щільністю текстур, рис. 2. Кожна з них була надрукована на аркуші формату А4 та закріплена на білій освітленій стіні. Ціль № 1 – шахова дошка з великою сіткою, яка генерує обмежену кількість ключових точок, проте легко розпізнається навіть за слабого освітлення або на значній відстані. Мішень № 2 – сітка з вищою щільністю клітинок, що формує більшу кількість ключових точок з підвищеною деталізацією. Мішень № 3 – QR-код, який містить численні дрібні графічні елементи, здатні створювати високу концентрацію ключових точок, але водночас є більш чутливим до зниження якості зображення та освітленості сцени [6–8].

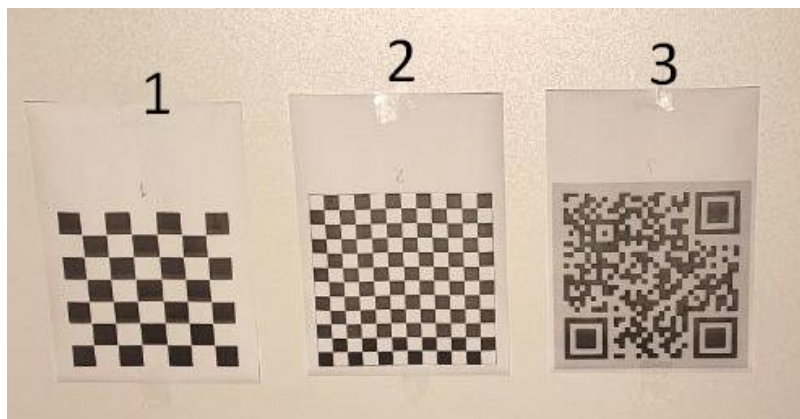


Рис. 2. Цілі, що імітують об'єкти з різною щільністю ключових точок

Така комбінація мішеней дозволяє змодельовати типові сценарії взаємодії користувача з реальними об'єктами: від простих із чіткою геометрією до складних із насиченою текстурною структурою.

Процедура вимірювання здійснювалася в умовах фіксованої геометрії сцени та контрольованого освітлення. Джерело світла розміщувалося на визначених відстанях від мішеней у межах від 1 до 4 метрів з кроком у 1 метр, причому відстань встановлювалася за допомогою лазерного далекоміра. На кожному етапі експерименту проводилося по три вимірювання відстані до кожної цілей за допомогою мобільного застосунку, рис. 3.

Після завершення циклу з трьох вимірів рівень освітленості змінювався шляхом зниження напруги на джерелі світла. В експерименті використовувалася фара з лампою розжарювання.

Для забезпечення статистичної надійності процес повторювався тричі в однакових умовах, тобто загалом на кожному рівні освітленості збиралося по 9 значень: по три для кожної мішені. Така методика дозволила отримати порівнювані дані для різних рівнів освітленості на однаковій дистанції.

Оцінка отриманих результатів

За підсумками експериментальних вимірювань було сформовано структурований набір даних, що містить усі ключові параметри, необхідні для подальшого аналізу точності системи. До таблиці увійшли такі поля: Distance laser, metr – еталонна відстань, визначена за допомогою лазерного далекоміра; Illumination, lux – рівень освітленості в момент вимірювання, зафіксований фотометром; Distance AR x, y, metr – відстань, розрахована за допомогою системи ARCore, де x позначає номер цілі (від 1 до 3), а y порядковий номер вимірювання (від 1 до 3) у межах одного рівня освітленості. –1 означає що не вдалося отримати дані, або занадто велике значення, щоб бути реальною відстанню. Отримані результати наведено у табл. 1.

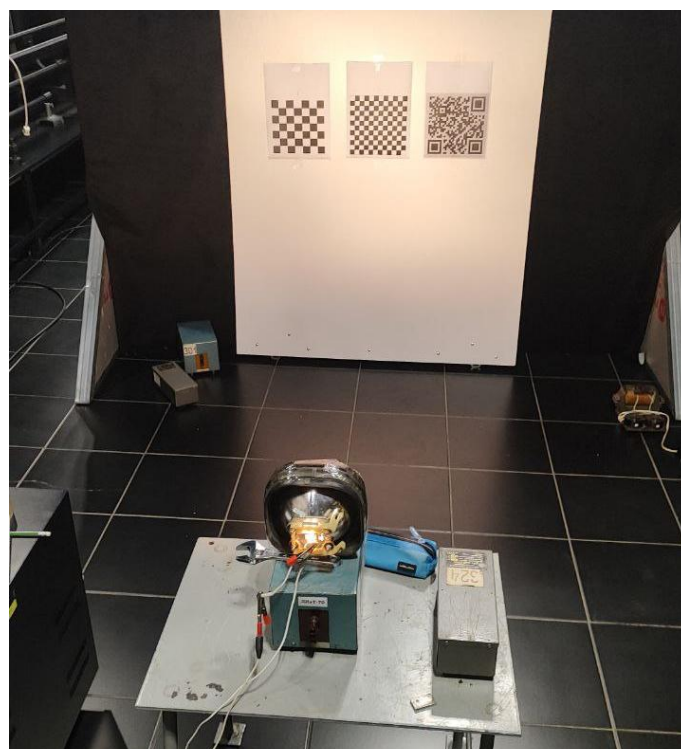


Рис. 3. Експериментальна установка

Таблиця 1

Отримані експериментальні дані

Distance laser, metr	Distance AR 1.1, metr	Distance AR 1.2, metr	Distance AR 1.3, metr	Distance AR 2.1, metr	Distance AR 2.2, metr	Distance AR 2.3, metr	Distance AR 3.1, metr	Distance AR 3.2, metr	Distance AR 3.3, metr	Illumination, lux
4,00	3,77	3,74	3,75	3,86	3,79	3,82	4,52	3,80	3,79	91,00
3,04	3,97	3,91	4,05	3,99	4,01	3,50	22,00	3,43	3,72	91,00
2,05	1,98	1,84	1,87	2,06	1,98	2,01	2,02	2,02	2,02	91,00
1,02	0,94	0,94	0,96	1,06	1,08	1,10	0,99	1,00	1,00	91,00
4,00	3,80	3,84	3,84	3,80	3,84	3,84	3,83	3,79	3,82	68,80
3,04	4,47	4,32	4,30	6,04	4,29	4,19	4,25	4,15	4,04	68,80
2,05	2,03	2,04	2,03	2,03	2,04	2,07	2,03	2,07	2,07	68,80
1,02	0,97	0,95	0,96	0,95	0,96	0,96	0,96	0,95	0,95	68,80
4,00	4,03	3,83	3,80	3,83	3,86	3,86	3,43	3,86	3,78	50,00
3,04	2,93	2,94	3,03	2,93	2,95	2,97	2,93	2,57	2,73	50,00
2,05	1,96	1,99	2,03	1,99	1,99	2,04	2,01	2,02	2,03	50,00
1,02	0,99	0,98	1,00	1,02	1,01	1,02	1,02	1,01	1,01	50,00
4,00	3,83	3,59	3,89	4,68	3,58	3,97	4,53	3,63	3,74	27,60
3,04	2,64	2,64	2,58	2,58	2,59	2,81	2,63	2,68	2,70	27,60
2,05	1,85	1,82	1,79	1,74	1,97	1,76	1,78	1,81	1,79	27,60
1,02	0,93	0,92	0,97	1,08	1,04	1,05	0,91	0,91	1,14	27,60
4,00	3,53	3,73	3,58	3,41	3,53	3,69	3,26	3,47	5,30	7,03
3,04	0,80	11,00	2,95	2,83	3,10	2,89	3,00	3,04	2,89	7,03
2,05	11,00	0,00	9,05	0,00	2,00	12,00	0,00	1,99	2,62	7,03
1,02	0,94	0,94	0,96	0,92	0,96	0,93	0,91	0,91	0,91	7,03
4,00	0,00	20,09	1,68	2,18	1,79	1,68	1,74	1,57	1,62	5,85
3,04	3,84	3,49	3,91	3,43	3,45	4,17	3,56	4,42	5,39	5,85
2,05	1,62	1,55	1,67	1,86	1,78	2,03	1,88	1,88	2,08	5,85
1,02	0,92	0,87	0,89	0,95	0,89	0,90	0,93	0,92	0,90	5,85
4,00	-1,00	-1,00	-1,00	-1,00	-1,00	-1,00	-1,00	-1,00	-1,00	3,17
3,04	-1,00	-1,00	-1,00	-1,00	-1,00	-1,00	-1,00	-1,00	-1,00	3,17
2,05	-1,00	-1,00	-1,00	-1,00	-1,00	-1,00	-1,00	-1,00	-1,00	3,17
1,02	0,93	0,95	0,97	0,96	0,96	0,99	0,96	0,94	0,98	3,17

Для кожного вимірювання було обчислено абсолютне відхилення між відстанню, отриманою за допомогою ARCore, та еталонною відстанню, визначеною лазерним далекоміром. Усі отримані значення були згруповані відповідно до цілі та дистанції, після чого розраховано середнє відхилення та побудовано візуалізацію результатів у вигляді чотирьох окремих графіків – по одному для кожної фіксованої відстані, рис. 4.

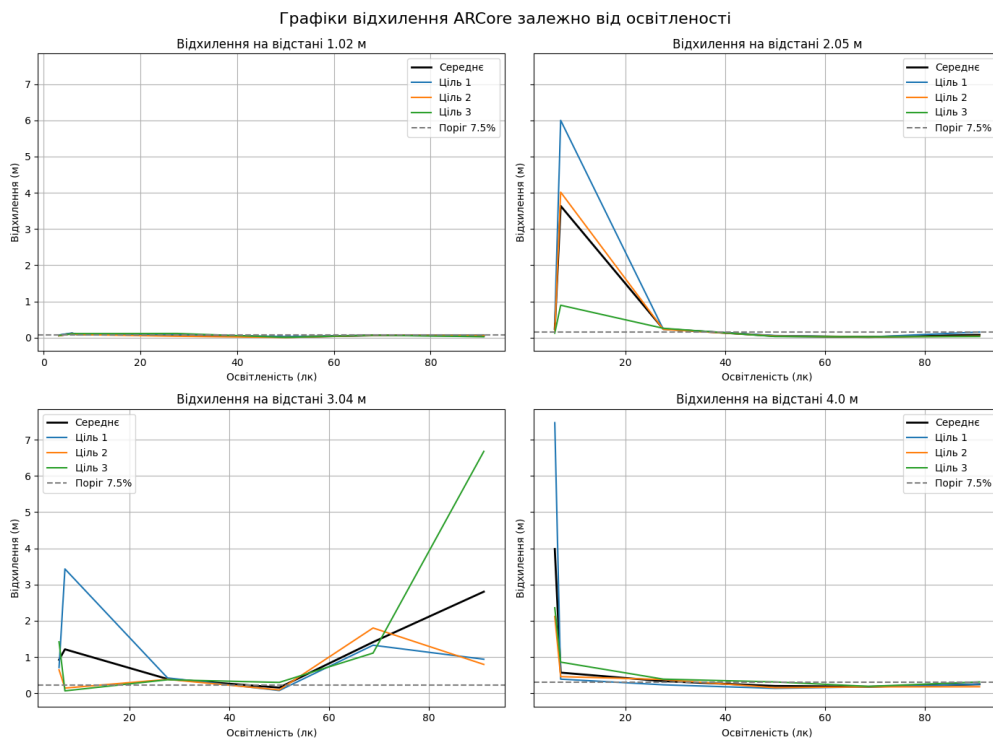


Рис. 4. Графіки відхилення на різній дистанції

При відстані 1.02 м система демонструє стабільну роботу в усьому діапазоні освітленості, з відхиленнями, що не перевищують 7,5 %. Це значення було визначено як максимальний рівень похибки при вимірюванні відстані в умовах денного освітлення. На відстані 2.05 м вже спостерігається чітка тенденція до зростання похибок при освітленості нижче 20 лк. Ще більш критична ситуація спостерігається на відстанях 3.04 і 4.00 м: при освітленості нижче 30–40 лк значна частина вимірювань демонструє нестабільність або повний зрив глибини система повертає завідомо хибні значення (умовно позначені як 10 м), що вказує на втрату коректної оцінки просторової сцени. У поодиноких випадках нестабільність фіксується навіть при помірному освітленні (до 60 лк), що свідчить про наявність граничного порогу, нижче якого система працює ненадійно.

Результати експерименту свідчать про виражену залежність точності роботи ARCore від рівня освітлення. Зниження освітленості безпосередньо впливає на якість формування карти глибини, що призводить до системних помилок у вимірюванні, особливо на відстанях понад 2 м [9].

Для підвищення ефективності вимірів, логічно витікає гіпотеза, що усереднення або використання медіанного значення з декількох незалежних вимірів у межах однієї сцени може знизити похибку, зумовлену локальними артефактами карти глибини або поодинокими вибросами в оцінці ключових точок, рис. 5.

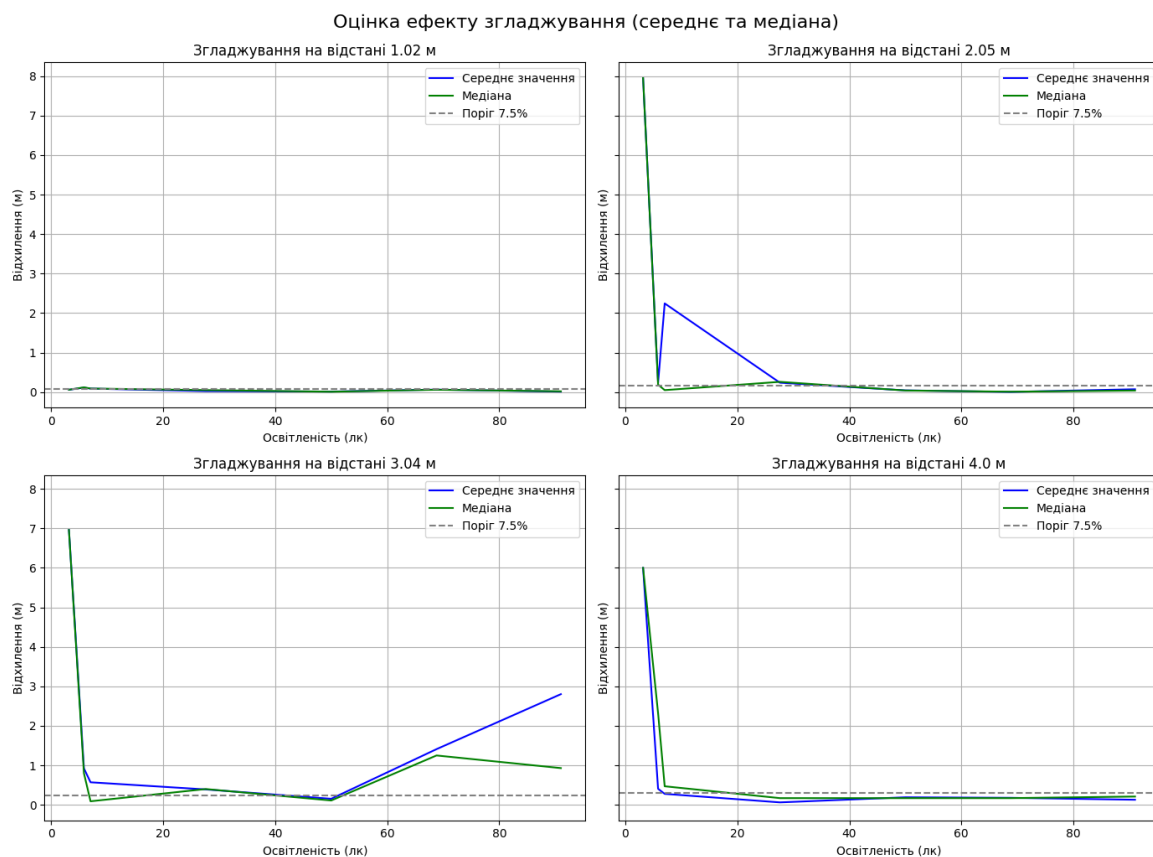


Рис. 5. Оцінка ефективності фільтрації

Для перевірки цієї гіпотези у рамках кожного циклу вимірювань було розраховано два згладжених показники: середнє та медіанне значення відстані, отримані з трьох паралельних вимірів до кожної з мішеней за однакових умов (фіксована відстань та рівень освітленості). Після цього для кожного із зазначених показників обчислювалося абсолютне відхилення від еталонної відстані, визначеної лазерним далекоміром. Отримані результати дозволили порівняти вплив типу згладжування на точність вимірювання, а також виявити критичні умови, за яких похибка перестає компенсуватися навіть після обробки кількох кадрів.

Результати аналізу підтверджують доцільність використання згладжування як методу підвищення надійності системи ARCore. Зокрема, медіанне значення продемонструвало кращу стійкість до поодиноких збоїв: у випадках, коли одне з трьох вимірів було суттєво зміщене або помилкове, медіана дозволяла зменшити вплив цього викиду на фінальний результат. Усереднення також покращувало результати в умовах помірного освітлення, проте було чутливим до окремих відхилень.

Дискусійні положення

Отримані результати експериментальних досліджень свідчать, що точність та надійність визначення відстані із використанням ARCore істотно залежать від рівня освітленості сцени та текстурних характеристик об'єкта. За умов достатнього рівня світла система забезпечує похибку в межах допустимих значень, проте зниження освітленості нижче 30 – 40 лк призводить до помітного зростання похибки та у ряді випадків до зриву побудови карти глибини навіть на відносно малих дистанціях. Використання алгоритмів згладжування на основі кількох послідовних вимірювань частково підвищує стабільність отриманих даних, зокрема при застосуванні медіанного значення, однак не усуває базової залежності системи від умов освітлення.

Для порівняння, у природних денних умовах рівень освітленості становить у середньому 10 000 – 25 000 лк при сонячній погоді та близько 1 000 – 2 000 лк за похмурої погоди, що в

десятки й сотні разів перевищує порогові значення, за яких у проведених експериментах спостерігалася деградація роботи системи [10, 11]. Цей контраст пояснює відсутність значних похибок у більшості попередніх досліджень, де експерименти виконувалися за умов належного освітлення.

Зокрема, у роботі «Accuracy and Usability of Smartphone-Based Distance Estimation» та інших [12–15], було підтверджено стабільність результатів для низки методів визначення відстані за умов достатнього денного освітлення. Отримані дані доповнюють ці висновки, демонструючи межі застосовності ARCore в умовах низької освітленості та підкреслюючи необхідність використання додаткових алгоритмічних або апаратних механізмів компенсації для практичного застосування у навігаційних системах на основі технологій доповненої реальності.

Додатково було проведено порівняння ефективності вимірювання відстані між тестовим застосунком, реалізованим на базі ARCore, та програмою Лінійка для iPhone, що використовує ARKit. Умови досліджу відповідали типовому денному освітленню, і результати показали похибку вимірювання на рівні не більше 1. Обидва фреймворки продемонстрували порівняльний рівень точності та ефективності, що підтверджує їхню придатність до використання у прикладних завданнях просторової навігації.

Висновки

Представлено результати експериментальних досліджень ефективності вимірювання відстані за допомогою фреймворку ARCore в умовах низької освітленості. Аналіз показав, що система здатна забезпечувати прийнятну точність при освітленості понад 60 лк та на відстанях до 2 м, проте за зниження рівня освітленості спостерігається суттєве зростання похибки, а в окремих випадках – повний зрив побудови карти глибини. Використання методів згладжування (середнє та медіанне значення) дозволяє частково зменшити нестабільність результатів, однак не усуває фундаментальної залежності технології від умов освітлення.

Отримані дані логічно узгоджуються з попередніми роботами, що підтвердили високу ефективність аналогічних систем за умов стандартного денного освітлення. Наше дослідження доповнює наявну наукову базу, визначаючи граничні умови застосування ARCore у реальних сценаріях із низьким рівнем освітленості.

Практична значущість роботи полягає у формуванні чітких вимог до апаратних та алгоритмічних засобів компенсації, необхідних для створення навігаційних рішень на базі технологій доповненої реальності. Такі рішення мають забезпечувати стабільну роботу в умовах змінного освітлення та мінімальне когнітивне навантаження для користувача. Отримані результати можуть бути використані у розробці тифлотехнічних систем, зокрема персоналізованих навігаційних помічників для осіб з порушенням зору.

Список літератури:

1. Соколов А. А., Аврунін О. Г. Перспективи використання технологій доповненої реальності при розробці засобів навігації для незрячих // Опт.-ел. інф.-енерг. техн. 2023. Вип. 46, вип. 2. С. 55–63.
2. Соколов А. А., Аврунін О. Г. Оцінка можливостей бібліотеки ARCORE для визначення дистанції до об'єктів у кадрі // Опт.-ел. інф.-енерг. техн. 2024. Вип. 47, вип. 1. С. 58–65.
3. Соколов А. А., Аврунін О. Г. Використання бібліотеки ARCore для візуалізації хмари ключових точок у навігаційних системах // Радіотехніка. 2025. Вип. 219. С. 53–58. <https://doi.org/10.30837/rt.2024.4.219.06>
4. Тензор. Вимірювальне та метрологічне обладнання. Режим доступу: <https://tenzor.ua>.
5. user-manual-inkersi-ke70 : Free Download, Borrow, and Streaming : Internet Archive. Internet Archive. URL: <https://archive.org/details/inkersi-ke70-manual>
6. Overview of ARCore and supported development environments / Google for Developers. Google for Developers. URL: <https://developers.google.com/ar/develop>
7. Use the ARCore Depth API for immersive augmented reality experiences,” Google Codelabs. <https://codelabs.developers.google.com/codelabs/arcore-depth/#0>
8. Computer Vision: Algorithms and Applications, 2nd ed.,” szeliski.org. <https://szeliski.org/Book/>
9. Maksym Tymkovych, Oleg Avrunin, K. Selivanova, A. Kolomiets, Taras Bednarchyk, and Saule Smailova // CORRESPONDENCE MATCHING IN 3D MODELS FOR 3D HAND FITTING. Informatyka, Automatyka,

Pomiary w Gospodarce i Ochronie Środowiska. 2024. Vol. 14, no. 1. P. 78–82. doi: <https://doi.org/10.35784/iapgos.5498>.

10. Hossein Z., Mohammad H. D. M. An Accurate Scheme for Distance Measurement using an Ordinary Webcam // International Journal of Electrical and Computer Engineering (IJECE). 2017. Vol. 7, no. 1. P. 209–215. URL: <https://doi.org/10.11591/ijece.v7i1.pp209-215>

11. Engineeringtoolbox E. Illuminance – Recommended Light Levels. The Engineering ToolBox. URL: https://www.engineeringtoolbox.com/light-level-rooms-d_708.html

12. ARKit | Apple Developer Documentation. Apple Developer Documentation. URL: <https://developer.apple.com/documentation/arkit>.

13. INTEGRATION OF DEPTH MAPS FROM ARCORE TO PROCESS POINT CLOUDS IN REAL TIME ON A SMARTPHONE / R. Haenel et al. The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences. 2022. XLIII-B2-2022. P. 201–208. URL: <https://doi.org/10.5194/isprs-archives-xliii-b2-2022-201-2022>

14. Accuracy and Usability of Smartphone-based Distance Estimation Approaches for Visual Assistive Technology Development / G. Hamilton-Fletcher та ін. // IEEE Open Journal of Engineering in Medicine and Biology. 2024. C. 1–5. URL: <https://doi.org/10.1109/ojemb.2024.3358562>

15. A virtual reality platform to simulate orientation and mobility training for the visually impaired / F. S. Ricci et al. Virtual Reality, 2022. URL: <https://doi.org/10.1007/s10055-022-00691-x>

Надійшла до редколегії 01.11.2025

Відомості про авторів:

Соколов Андрій Андрійович – д-р філософії, Харківський національний університет радіоелектроніки, асистент кафедри біомедичної інженерії, Україна; e-mail: andrii.sokolov@nure.ua; ORCID: <https://orcid.org/0000-0002-8087-698X>

Аврунін Олег Григорович – д-р техн. наук, професор, Харківський національний університет радіоелектроніки, завідувач кафедри біомедичної інженерії, Україна; e-mail: oleh.avrunin@nure.ua; ORCID: <https://orcid.org/0000-0002-6312-687X>

Носова Яна Віталіївна – канд. техн. наук, доцент, Харківський національний університет радіоелектроніки, Україна; e-mail: yana.nosova@nure.ua; ORCID: <https://orcid.org/0000-0003-4310-5833>

Носова Тетяна Віталіївна – канд. техн. наук, доцент, Харківський національний університет радіоелектроніки, Україна; e-mail: tatyana.nosova@nure.ua; ORCID: <https://orcid.org/0000-0003-4442-8001>

С.О. ФІЛІМОНОВ, Л.О. АВЕР'ЯНОВА, канд. техн. наук

**МОДЕЛЮВАННЯ ФАНТОМА ЗРІЗУ
ТРАБЕКУЛЯРНОЇ ТКАНИНИ ХРЕБЦЯ ЛЮДИНИ
ДЛЯ ДОСЛІДЖЕННЯ ЙОГО КТ-РЕКОНСТРУКЦІЇ**

Вступ

Губчаста тканина хребця відіграє ключову роль у забезпеченні структурної цілісності тіл хребців та біомеханічній стабільності хребта в цілому. З віком або під впливом патологій, таких як остеопороз, відбуваються дегенеративні зміни в мікроархітектурі трабекулярної тканини, що призводить до зменшення щільності кісткової тканини, підвищення ризику компресійних переломів хребців. Своєчасна та точна оцінка мікроструктури губчастої тканини є критично важливою як для діагностики, так і для прогнозування перебігу остеопоротичних змін [1].

У клінічній практиці оцінку мікроструктури трабекулярної тканини здійснюють за допомогою рентгенівських методів, як то двоенергетична рентгенівська абсорбціометрія (DEXA) та кількісна комп'ютерна томографія (QCT). Лабораторним методом дослідження мікроархітектури кісткових структур є мікро-КТ (μ СТ) [2–4]. Попри широке застосування DEXA як стандарту в оцінці мінеральної щільності кісткової тканини (МЩКТ), цей метод не дозволяє досліджувати зміни мікроархітектури трабекул. Натомість QCT надає тривимірні об'ємні дані, які дають змогу узагальнено аналізувати МЩКТ як у кортикальній, так і у трабекулярній компонентах, що широко використовується у клінічній діагностиці, включаючи скринінг та моніторинг остеопорозу [3–12]. Проте просторової роздільної здатності клінічної КТ недостатньо для відображення мікроструктурної організації трабекулярної тканини. Крім того, КТ характеризується наявністю шумів, пов'язаних із розсіянням рентгенівських фотонів, флуктуаціями сигналів в детекторах та артефактами реконструкції. Ці фактори призводять до розмиття границь трабекул, погіршення сегментації та значних похибок у морфометрії. Мікро-КТ вважається “золотим стандартом” для *in vitro* візуалізації мікроструктури кістки з просторовим розрізненням, яке дозволяє ідентифікувати окремі трабекули, їхню товщину, кількість та взаємне розташування. Така точність забезпечує надзвичайно високу інформативність при побудові цифрових моделей кісткової архітектури. Проте ця технологія не може бути застосована для рутинної клінічної діагностики через радіаційне навантаження, обмежений розмір зразка та неможливість сканування *in vivo*, мКТ має переважно дослідницьке застосування.

Спроби отримання кількісних характеристик кісткового статусу за результатами рутинної КТ потребують створення стандартизованих умов дослідження як на етапі сканування, так і при постобробці отриманих даних. Оцінка адекватності визначення кісткового статусу за реальними КТ-даними має проводитись на основі результатів обчислювальних експериментів з моделювання всіх стадій їх отримання. Це, в свою чергу, створює потребу в розробці морфологічно подібних цифрових 2D або 3D фантомів, що дозволяють моделювати трабекулярну структуру кістки та в подальшому вивчати вплив різних чинників процесу (шум, способи фільтрації, алгоритми реконструкції тощо) на точність визначення морфометричних показників.

Цифрові фантоми – це тестові об'єкти, що використовуються для початкового тестування та оптимізації методів медичної візуалізації, проте вони не можуть відображати усі складні властивості реальної біологічної тканини [5]. Такі фантоми широко застосовуються також в біомеханічному моделюванні, чисельних експериментах і тестуванні алгоритмів сегментації КТ-зображень.

Методологія створення цифрового фантому губчастої кістки

На першому етапі дослідження генерується бінарне зображення, яке відтворює типову мікроархітектуру губчастої кістки, якою вона відображається на мікро-КТ (рис. 1). Світлі пікселі позначають трабекули, а темні – міжтрабекулярний простір. Розмір зображення становить 512×512 пікселів, що еквівалентно площі 8.83×8.83 мм², з умовною просторовою роздільністю близько 20 мкм/піксель [13]. Це дозволяє детально відобразити варіативну форму, орієнтацію й густину розташування трабекулярних елементів кісткової тканини у перерізі (рис. 1).

Нормалізація зображення. Реконструйовані матриці інтенсивностей масштабували до діапазону $[0, 1]$:

$$Inorm(x, y) = (I(x, y) - Imin) / (Imax - Imin), \quad (1)$$

де $Imin$, $Imax$ – мінімальне та максимальне значення інтенсивності у зрізі. Це забезпечує співставність результатів та коректну візуалізацію гістограм.

Обрізання хвостів (кліпінг). Для зменшення впливу викидів застосовано обмеження значень пікселів на основі перцентилів:

$$Iclip(x, y) = \{ L, \text{ якщо } I(x, y) < L; U, \text{ якщо } I(x, y) > U; I(x, y) - \text{інакше}, \quad (2)$$

де L , U – зменшує вплив шумових піків та стабілізує вигляд гістограм.

Зображення було нормалізовано до діапазону $[0, 1]$ відповідно до стандартів MATLAB, де 1 відповідає щільній кістковій тканині, 0 – фоновій області. Такий підхід забезпечує повний контроль над геометричними характеристиками моделі до проведення КТ-моделювання, що критично для подальшого аналізу впливу чинників реконструкції. Отриманий фантом слугує еталонною моделлю для симуляцій, чисельного аналізу та порівняння з реальними мікро-КТ-знімками [11].

Радон-перетворення фантомного зображення

Перетворення Радона є математичною моделлю процесу проходження рентгенівського пучка через об'єкт під різними кутами. Воно дозволяє отримати синограму – 2D-матрицю, де кожен стовпчик відповідає сумарній щільності поглинання матеріалу вздовж відповідного напрямку в залежності від проєкційного кута. Математично процес описується як інтегральне перетворення [8]:

$$R_{\theta}(p) = \iint f(x, y) \delta(x \cos \theta + y \sin \theta - p) dx dy, \quad (3)$$

де $f(x, y)$ – функція, що описує щільність у точці (x, y) ; θ – кут проєкції; p – положення детектора; δ – дельта-функція Дірака.

У цифровому варіанті синограма $S(x, \theta)$ – це дискретна апроксимація інтегралу, яка описує проєкцію зображення на певному куті θ . Віртуальне сканування було здійснено у діапазоні кутів від 0° до 179° з кроком 1° з паралельним проєціюванням (рис. 2).

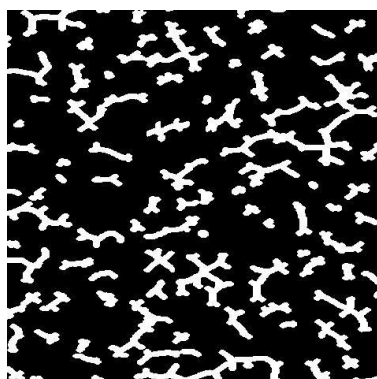


Рис. 1. Синтетично згенерований фантом мікро-КТ трабекулярної тканини хребця людини

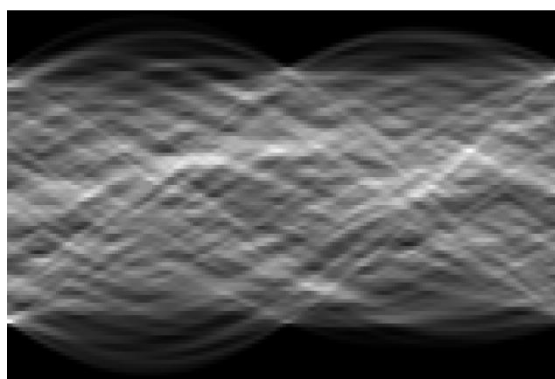


Рис. 2. Візуалізація синограми, отриманої при імітаційному скануванні фантомної трабекулярної структури у 180 проєкціях

Отже, маємо набір проєкційних даних для всіх пікселів вздовж променя під кутом θ :

$$S(x, \theta) \approx \sum f(x', y'). \quad (4)$$

Синограма є аналогом «сирих» проєкційних даних з детекторів КТ та слугує основою для подальшого моделювання реконструкції фантомного зображення.

Реконструкція фантомного зображення

Після моделювання синограми проходить реконструкція зображення шляхом оберненого Радон-перетворення. Цей процес імітує КТ-відновлення зрізів об'єкта з набору проєкцій під різними кутами. Для підвищення достовірності реконструкції застосовується фільтрація (фільтр Ram-Lak) [7], яка підсилює високочастотні компоненти, необхідні для точного відтворення меж структур. Також використовується лінійна інтерполяція для згладжування просторового відновлення та масштабування результату до початкового розміру зображення. Щоб надалі оцінити вплив шуму на якість реконструкції, спочатку виконується реконструкція референсного зображення без додавання шуму (рис. 3).

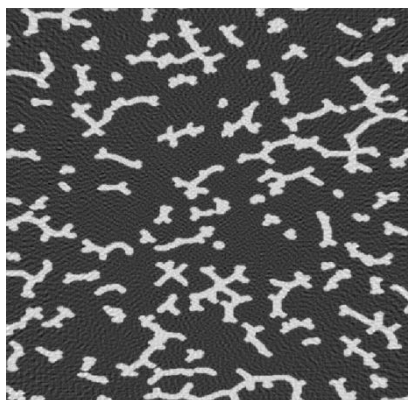


Рис. 3. Реконструкція фантомного зображення трабекулярної тканини без додавання шуму

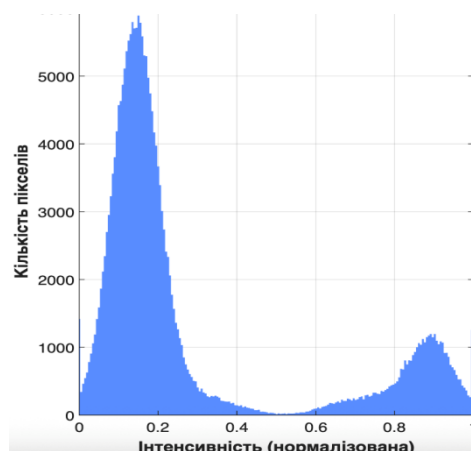


Рис. 4. Гістограма інтенсивностей для реконструкції без шуму

Аналіз реконструкції без шуму. На рис. 4 наведено гістограму інтенсивностей для реконструкції без шуму. Видно два основні піки: перший, біля низьких значень ($\approx 0.15-0.25$), відповідає фоновим областям, другий ($\approx 0.8-0.9$) відображає кісткову тканину. Чітке розділення фаз свідчить про високу якість реконструкції без впливу шуму. Між піками присутній мінімальний рівень значень, що відповідає перехідним зонам та артефактам згортки. Це розподіл надалі використовується для порівняння з даними, що містять шум. Математично реконструкція описується інтегральною формулою [7, 9]:

$$f(x, y) = \int_0^\pi [p\theta(t) * h(t)] d\theta, \quad (5)$$

де $p\theta(t)$ – проєкція при куті θ (елемент синограми); $h(t)$ – фільтр згортки (Ram-Lak).

Для моделювання шумів, наближених до реальної КТ-візуалізації, до синограми додався адитивний гаусівський шум. Шум визначався як випадкова змінна $n \sim N(0, \sigma^2)$, що додається до кожного значення проєкції:

$$S_{noisy}(x, \theta) = S(x, \theta) + n(x, \theta), \quad (6)$$

де $S(x, \theta)$ – інтенсивність синограми без шуму; $\sigma = k \cdot \max(S)$ – амплітуда шуму, пропорційна максимальному сигналу.

Така модель відображає флуктуації детекторів і квантовий шум рентгенівського випромінювання (рис. 4) [10]. Результат реконструкції наведено на рис. 5. Зображення містить рівномірний шум, характерний для реальних КТ-знімків, а трабекулярні елементи візуалізують-

ся узагальнено, із розмиттям через обмежену просторову здатність методу. Такий вигляд зображення є очікуваним, оскільки при клінічному КТ просторове розрізнення недостатнє для відображення окремих мікроструктур кістки, товщина яких становить лише кілька сотень мікрометрів. У моделі цей ефект посилюється шумом на етапі утворення синограми та попереднім зниженням роздільної здатності, що дозволяє реалістично відтворити умови сканування.

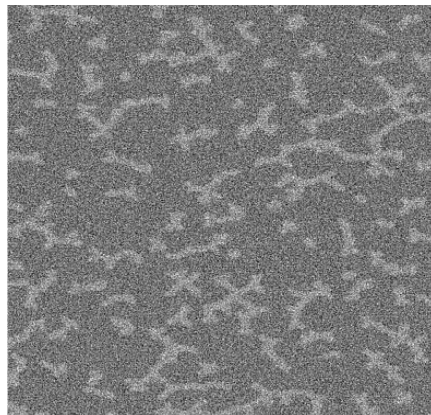


Рис. 5. Реконструйоване зображення фантома трабекулярної тканини після зворотного Радон-перетворення (з додаванням шуму)

Отримане реконструйоване зображення служить основою для подальшого аналізу морфометричних параметрів і демонструє, як зміна алгоритмів відновлення або рівня шуму впливає на якість візуалізації.

Побудова та інтерпретація гістограм

Розподіл інтенсивностей реконструйованого зображення аналізували за допомогою гістограм [11]. На рис. 6 показано сумарну гістограму інтенсивностей реконструйованого зображення (сині стовпчики) та криві для сегментованих фаз: «кістка» (червона) та «фон» (жовта). Видно, що розподіл інтенсивностей має широкий діапазон зі скупченням пікселів у ділянках низьких значень (фон) та локальним підйомом у середньо-високих значеннях (кісткова тканина). Чітке розмежування між цими фазами утруднене через накладання шуму та розмиття границь, що особливо помітно в діапазоні 0.4–0.6. Пікові значення біля 0 та 1 пояснюються фоновими ділянками та насиченими кістковими елементами відповідно.

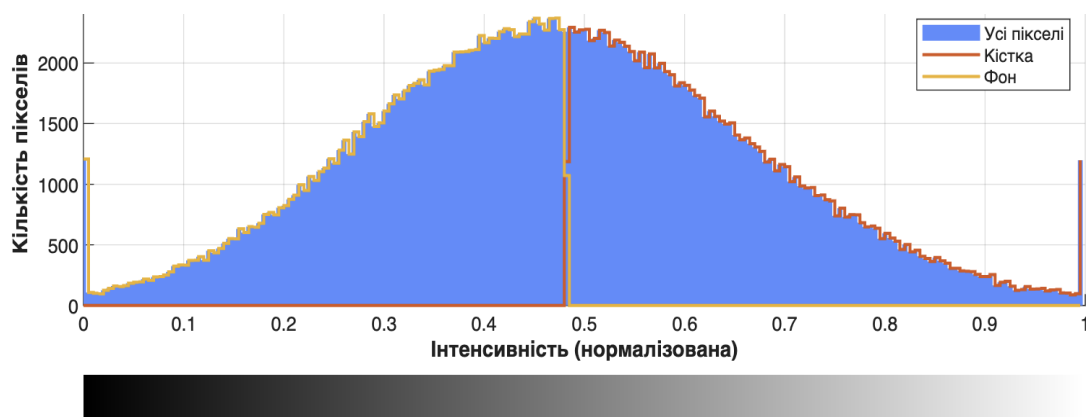


Рис. 6. Гістограма інтенсивностей реконструйованого зображення

Такий вигляд є типовим для моделювання КТ-зображень із шумом та відповідає реальним умовам, де завжди присутні флуктуації сигналу і часткове перекриття класів.

Порівняльна оцінка морфометричних показників

Специфічними показниками для оцінки змін мікроархітектури трабекулярної кісткової тканини на основі КТ є об'єм трабекулярної кістки (об'єм кістки/загальний об'єм BV/TV) та товщина трабекулярної кістки (Tb.Th) [2]. Отримані морфометричні параметри КТ-фантому було порівняно з результатами мікро-КТ [6, 15], де представлені усереднені показники трабекулярної кісткової архітектури поперекового відділу хребта (табл. 1).

Таблиця 1

Параметр	Мікро-КТ хребця [6]	Мікро-КТ фантома
BV/TV (%)	18.87 ± 1.6	19.51
Tb.Th (мм)	0.153	0.153

В порівнянні з реальною структурою мікро-КТ трабекулярної кістки в нормі, симульоване КТ-зображення мало показник BV/TV у межах інтервалу значень (17,27...20,47) для реальної мікро-КТ та точну відтворюваність показників Tb.Th [14].

Висновки

Представлено результати створення високоточного цифрового фантомного зображення трабекулярної тканини хребця людини на основі геометричних статистичних параметрів, отриманих із мікро-КТ. Реалізовано метод моделювання стандартного КТ-зображення кісткової структури на основі розробленого референсного фантома шляхом застосування Радон-перетворення та подальшої реконструкції.

Проведено порівняльний аналіз основних морфометричних показників фантомного та реального КТ-зрізів кістки. Цей результат підтвердив можливість застосування отриманого синтетичного КТ-фантому не тільки як об'єкту верифікації, але й готового інструменту для поточного використання в задачах подальшої кількісної оцінки точності морфометричного аналізу КТ-зображень кісткових структур. Використання такого підходу в подальшому відкриває можливість детально аналізувати ті аспекти стану кісткової тканини, які у клінічній практиці залишаються поза межами візуалізації.

Список літератури:

1. Molino, Giulia, Giorgia Montalbano, Carlotta Pontremoli, Sonia Fiorilli, and Chiara Vitale-Brovarone. Imaging Techniques for the Assessment of the Bone Osteoporosis-Induced Variations with Particular Focus on Micro-CT Potential // Applied Sciences. 2020. Vol. 10, no. 24. P. 8939. doi:10.3390/10248939
2. Filimonov S., Liliia A. and Tymkovych M. Analysis of CT Parameters of Trabecular Tissue Density of Vertebral Body // 2024 IEEE 5th KhPI Week on Advanced Technology (KhPIWeek), Kharkiv, Ukraine, 2024. P. 1–4. doi: 10.1109/KhPIWeek61434.2024.10878080.
3. Brett A.D., Brown J.K. Quantitative computed tomography and opportunistic bone density screening by dual use of computed tomography scans // J Orthop Translat, 2015. doi: 10.26044/ecr2020/C-00759.
4. Christiansen B.A. Effect of micro-computed tomography voxel size and segmentation method on trabecular bone microstructure measures in mice. Bone Rep, 2016. doi: 10.1016/j.jot.2015.08.006.
5. Manohar, Srirang, Ioannis Sechopoulos, Mark A. Anastasio, et al. Super phantoms: advanced models for testing medical imaging technologies // Communications Engineering. 2024. Vol. 3. P. 73. doi:10.1038/s44172-024-00218-z
6. Galassi F.M., Lorkiewicz W., Filipiak J. et al. Age- and sex-related changes in vertebral trabecular bone architecture in Neolithic and Mediaeval populations from Poland // Sci Rep. 2024. Vol. 14. P. 9977. <https://doi.org/10.1038/s41598-024-59946-z>
7. Tan X., Liu X., Xiang K., Wang J., Tan S. Deep Filtered Back Projection for CT Reconstruction // IEEE Access. 2024. Vol. 12. P. 20962–20972. doi:10.1109/ACCESS.2024.3357355.
8. Hwang G., Kim J., Lee Y. Inversion formulas for quarter-spherical Radon transforms // AIMS Mathematics. 2023. Vol. P. 1600. doi:10.3934/math.20231600.
9. Beckmann M., Nickel J. Optimized filter functions for filtered back projection reconstructions // Inverse Problems & Imaging. 2025. doi:10.3934/ipi.2025003

10. Hein D., Karchev P., Freichel S., et al. Noise suppression in photon-counting CT via posterior sampling in Poisson-flow generative models // Visual Computing for Industry, Biomedicine and Art. 2024. Vol. 7. P. 6. doi:10.1186/s42492-024-00175-6.
11. Koetzier L.R., Mastrodicasa D., Szczykutowicz T.P., et al. Deep Learning Image Reconstruction for CT: Technical Principles and Clinical Prospects // Radiology. 2023. Vol. 306(3). P. e221257. doi:10.1148/radiol.221257.
12. Oh S., Kang W.Y., Park H., et al. Evaluation of deep learning-based quantitative computed tomography for opportunistic osteoporosis screening // Scientific Reports. 2024. Vol. 14. P. 363. doi:10.1038/s41598-023-45824-7.
13. Lukova A., Dunmore C.J., Tsegai Z.J., et al. Technical note: Does scan resolution or downsampling impact the analysis of trabecular bone architecture? // American Journal of Biological Anthropology. 2024. Vol. 185(3). P. e25023. doi:10.1002/ajpa.25023.
14. Buyuksungur A., Turan B., Atik O., et al. The Effect of Micro-Computed Tomography Thresholding Methods on Bone Micromorphometric Analysis // Biomedicines. 2024. Vol. 12(11). P. 343. doi:10.3390/biomedicines15110343.
15. Kok J., Bevers M.S.A.M., van Rietbergen B., Oei E.H.G., Booi R. Quantification of bone microarchitecture using photon-counting CT at different radiation doses: A comparison with μ CT // European Journal of Radiology. 2024. Vol. 181. P. 111717. doi:10.1016/j.ejrad.2024.111717.

Надійшла до редколегії 10.10.2025

Відомості про авторів:

Філімонов Сергій Олександрович – Харківський національний університет радіоелектроніки, аспірант кафедри біомедичної інженерії, Україна; e-mail: serhii.filimonov@nure.ua; ORCID: <https://orcid.org/0009-0003-7609-9051>

Авер'янова Лілія Олександрівна – канд. техн. наук, доцент, Харківський національний університет радіоелектроніки, доцент кафедри біомедичної інженерії, Україна; e-mail: lilya.averyanova@nure.ua; ORCID: <https://orcid.org/0000-0003-0803-72220>

PHYSICS OF DEVICES, ELEMENTS AND SYSTEMS ФІЗИКА ПРИЛАДІВ, ЕЛЕМЕНТІВ І СИСТЕМ

УДК 621.383.5

DOI:10.30837/rt.2025.4.223.19

О.Д. МЕНЯЙЛО, канд. техн. наук, О.В. ГРИГОР'ЄВА, В.Г. МАХОНІН

ОПТИМІЗАЦІЯ ФЛУКТУАЦІЙНИХ ВЛАСТИВОСТЕЙ ДІОДНИХ ГЕНЕРАТОРІВ ВБУДОВАНИХ СИСТЕМ АВІОНІКИ

Вступ

Нагальна необхідність мініатюризації апаратури надвисоких частот, підвищення її економічності і надійності обумовила використання в якості активних елементів напівпровідникових приладів. Значні успіхи в напівпровідниковій технології та відкриття нових фізичних явищ зробили можливим широке застосування напівпровідників в надвисокочастотному діапазоні. Одним з перших явищ такого роду було надвисокочастотне випромінювання при ударній іонізації в р-п переходах, що послужило основою для створення в 1959 р. нового класу напівпровідникових приладів – лавино-пролітних діодів. На базі лавино-пролітних та подібних до них діодів створюються і швидко вдосконалюються різноманітні прилади та пристрої, в першу чергу генератори сантиметрового і міліметрового діапазонів.

Сучасні напівпровідникові діодні генератори НВЧ забезпечують досить велику вихідну потужність в безперервному режимі і можуть складати значну конкуренцію електровакуумним мікрохвильовим генераторам, особливо там, де потрібна конструктивна простота та надійність, що характерно для систем авіоніки. Одним з основних факторів, що обмежує максимальну потужність генератора на лавино-пролітних діодах (ГЛПД), є перегрів активної області діода, і як наслідок – незворотній тепловий пробій р-п переходу. Так, наприклад, кожні 100° С перевищення температури над 200° С зменшують середній час безвідмовної роботи діода на порядок, а при температурі вище 300° С відмови набувають випадкового характеру, оскільки одночасно включається кілька механізмів деградації.

Генератори на напівпровідникових діодах застосовуються в радіорелейних лініях, в системах сліпої посадки літаків, електронних вимірювачах висоти, стаціонарних та переносних радіолокаційних станціях. Такі генератори використовуються в якості задаючих в передавачах, гетеродинів в приймачах, як генератори шуму та інше.

Крім високої ефективності діодні генератори мають багато інших переваг, наприклад, невеликі габаритні розміри, високу надійність, не вимагають високовольтного джерела живлення та інше. Однак їх значним недоліком є досить високий рівень шуму. Особливо це відноситься до генераторів на лавино-пролітних діодах.

Існує багато методів досліджень флуктуаційних параметрів діодних генераторів. Так, наприклад, досліджуючи магнетронний генератор безперервних коливальних, ще Д. Міддлтон [1] показав, що найкращий спосіб охарактеризувати шумові властивості певних генераторів генератора – це розділити їх шуми на амплітудно модульовані та частотно модульовані компоненти. В цій роботі розглядаються та аналізуються деякі методи оптимізації флуктуаційних властивостей таких генераторів.

1. Механізм формування флуктуаційних шумових компонентів діодних генераторів НВЧ

Шум діодного генератора НВЧ, в основному, складається з двох компонент: флуктуації основної частоти (високочастотний шум) і компоненти, яка обумовлена шумовою модуляцією (низькочастотний шум). Розглянемо модель діодного генератора, яка безпосередньо дозволяє врахувати флуктуаційний шум $e(t)$ та модуляційний шум $U(t)$. Одна з таких можливих моделей наведена на рис. 1.

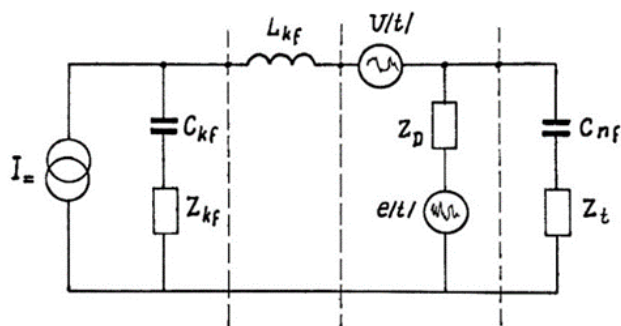


Рис. 1. Схема моделі генератора з урахуванням флуктуаційних та модуляційних шумів

На рисунку генератор напруги $e(t)$ моделює флуктуаційний шум. Модуляційний шум, що виникає в результаті флуктуацій постійного струму δI , може бути представлений генератором напруги $U(t)$, підключеним до ланцюга живлення. Таке представлення генератора дозволяє роздільно враховувати шуми, що породжені флуктуаціями джерела постійного струму та високочастотними флуктуаціями. Таке розділення можливе завдяки фільтру у вигляді ємності C_{kf} та індуктивності L_{kf} . Комплексний опір Z_{kf} моделює низькочастотний вхідний опір ланцюга живлення.

У випадку вузько смугового шуму ця шумова напруга може мати наступний вигляд:

$$e(t) = \operatorname{Re} [n(t) \exp j\omega t] = e_c(t) \cos \omega t - e_s(t) \sin \omega t, \quad (1)$$

де $e_s(t)$ та $e_c(t)$ – синусоїдальні та косинусоїдальні компоненти випадкової функції $n(t)$.

Напруга шуму $e(t)$, як випадковий процес, може бути представлена завдяки Фур'є-трансформації відповідною залежністю спектра густини потужності $S_{ee}(\omega)$.

Тобто

$$S_{cc}(\theta) = S_{ss}(\theta) = S_{ee}(\omega + \theta) + S_{ee}(\omega - \theta). \quad (2)$$

Зазначимо, що компоненти $e_c(t)$ та $e_s(t)$ є функціями, що повільно змінюються та характеризуються відповідними спектрами $S_{ee}(\theta)$ та $S_{ss}(\theta)$.

Модуляційний шум описується флуктуацією постійного струму $\delta i(t)$ і відповідає певному спектру потужності $S_{II}(\omega)$.

Механізм формування шуму лавинного осцилятора можна проілюструвати, виходячи з рис. 2.

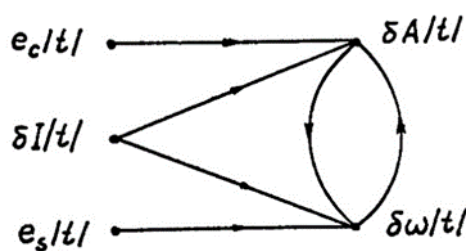


Рис. 2. Механізм формування шуму

Згідно з цим механізмом косинусоїдальна компонента флуктуаційного шуму викликає флуктуацію амплітуди, що призводить до послідовного відхилення частоти; в той час як синусоїдальна компонента флуктуаційного шуму викликає коливання частоти, що, в свою чергу, призводить до коливання амплітуди через частотно залежні елементи генератора.

Таким чином, модуляційний шум може безпосередньо спричинити шум, як амплітудно модульований (АМ), так і частотно модульований (ЧМ).

2. Аналіз шумових компонентів діодних генераторів

Використовуючи умови виникнення коливань, у випадку малих відхилень амплітуди $\delta A(t)$ та струму живлення $\delta I(t)$ можна записати рівняння для активної та реактивної складової комплексного опору генератора, що працює у безперервному режимі:

$$R_D = R_D(A_O I_-) - \frac{\partial R_D(A_O I_-)}{\partial A} \delta A(t) - \frac{\partial R_D(A_O I_-)}{\partial I} \delta I(t), \quad (3)$$

$$X_D(\omega) = X_D(A_O I_-) + \frac{\partial X_D(A_O I_-)}{\partial A} \delta A(t) + \frac{\partial X_D(A_O I_-)}{\partial I} \delta I(t). \quad (4)$$

З урахуванням умов генерації на основній частоті рівняння (3) та (4), що визначають амплітуду і фазу коливань генератора, набувають вигляду

$$\begin{aligned} & \frac{\partial R_D}{\partial A} X'_t \delta A(t) - \frac{\partial X_D}{\partial A} R'_t \delta A(t) + |Z'_t|^2 \frac{1}{A_O} \frac{d\delta A(t)}{dt} = \\ & = \frac{1}{A_O} (X'_t e_c(t) + R'_t e_s(t)) - \frac{\partial R_D}{\partial I} X'_t \delta I(t) + \frac{\partial X_D}{\partial I} R'_t \delta I(t). \end{aligned} \quad (5)$$

Наведені вище рівняння є стохастичними функціями часу. Випадкові процеси $\delta A(t)$, $\delta \omega(t)$, $\delta I(t)$ та $e(t)$ – частково характеризуються своїми автокореляційними функціями. Зафіксувавши значення функції в певний момент часу t , а потім здвинувши її на $t+\tau$, перемноживши та проінтегрувавши по t , отримаємо наступні співвідношення:

$$\begin{aligned} & \left[\frac{\partial R_D}{\partial A} X'_t - \frac{dX_D}{dA} R'_t \right]^2 R_A(t) - \frac{1}{A_O^2} (Z'_t)^4 \frac{d^2}{d\tau^2} R_A(\tau) = \\ & = \frac{1}{A_O^2} (Z'_t)^2 R_e(\tau) + \left[\frac{\partial R_D}{\partial I} X'_t - \frac{\partial X_D}{\partial I} R'_t \right]^2 R_I(\tau), \end{aligned} \quad (6)$$

$$\begin{aligned} & \left[\frac{\partial R_D}{\partial A} R'_t + \frac{\partial X_D}{\partial A} X'_t \right]^2 R_A(\tau) + (Z'_t)^4 R_\omega(\tau) = \\ & = \frac{1}{A_O^2} (Z'_t)^2 R_e(\tau) + \left[\frac{\partial R_D}{\partial I} R'_t + \frac{\partial X_D}{\partial I} X'_t \right]^2 R_I(\tau), \end{aligned} \quad (7)$$

де введено скорочення:

$$R_A(\tau) = \lim_{\tau \rightarrow \infty} \frac{1}{2T} \int_{-T}^T \delta A(t) \delta A(t + \tau) dt, \quad (8)$$

$$R_\omega(\tau) = \lim_{\tau \rightarrow \infty} \frac{1}{2T} \int_{-T}^T \delta \omega(t) \delta \omega(t + \tau) dt. \quad (9)$$

Слід зазначити, що ці рівняння справедливі при умові, що джерела флуктуаційного та модуляційного шуму будуть незалежними, некорельованими, тобто їх коефіцієнт кореляції дорівнює нулю.

Як відомо, автокореляційна функція і спектр щільності потужності утворюють Фур'є-пару. Таким чином, після певних математичних перетворень можемо отримати вираз для спектру флуктуацій частоти у наступній, досить складній формі:

$$\begin{aligned} S_{\omega\omega}(\Omega) = & \frac{\left[(Z'_t)^2 \Omega^2 + A_O^2 \left(\frac{\partial Z_D}{\partial A} \right)^2 \right] S_{ee}(\Omega)}{A_O^2 \left[\Omega^2 (Z'_t)^4 + A_O^2 \left(\frac{\partial R_D}{\partial A} X'_t - \frac{\partial X_D}{\partial A} R'_t \right)^2 \right]} + \frac{A_O^2 \left[\frac{\partial R_D}{\partial A} R'_t + \frac{\partial X_D}{\partial A} X'_t \right]^2 \left[\frac{\partial R_D}{\partial I} X'_t + \frac{\partial X_D}{\partial I} R'_t \right]^2}{(Z'_t)^4 \left[\Omega^2 (Z'_t)^4 + A_O^2 \left(\frac{\partial R_D}{\partial A} X'_t - \frac{\partial X_D}{\partial A} R'_t \right)^2 \right]} + \\ & + \frac{\left[\frac{\partial R_D}{\partial I} R'_t + \frac{\partial X_D}{\partial I} X'_t \right]^2}{(Z'_t)^4} S_{II}(\Omega). \end{aligned} \quad (10)$$

Для спрощення рівняння скористуємось графічним представленням робочої точки генератора (рис. 3). На комплексній площині зображено криву $Z_D(A)$ комплексного опору діода та

$Z_t(\omega)$ – комплексного опору коливальної системи генератора. Умови генерації показують, що точки перетину цих кривих представляють собою можливі робочі точки. Складний петле-подібний характер кривої навантаження обумовлений можливістю застосування багаторезонансної коливальної системи.

Припустимо, що генератор працює в стабільній робочій точці (наприклад, точка В на рис. 3).

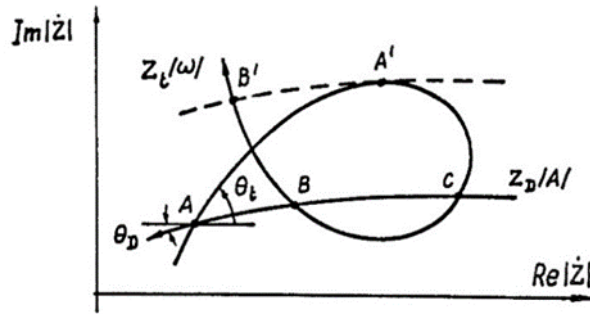


Рис. 3. Графічне представлення робочої точки генератора

Коливання амплітуди та струму живлення приводять до того, що робоча точка буде переміщуватися на комплексній площині. Припускаючи, що кути, які визначають положення кривих залежності комплексного навантаження від частоти $Z_t(\omega)$, комплексного опору діода від амплітуди коливань $Z_D(A)$ та струму живлення $Z_D(I)$ будуть незмінними та дорівнюватимуть θ, ψ, Θ , отримуємо наступні спрощені рівняння:

$$\frac{dZ_t}{d\omega} = \frac{dR_t}{d\omega} + j \frac{dX_t}{d\omega} = \left[\frac{dZ_t}{d\omega} \right] \exp(j\theta), \quad (11)$$

$$\frac{\partial Z_D}{\partial A} = \frac{\partial R_D}{\partial A} + j \frac{\partial X_{Dt}}{\partial A} = \left[\frac{\partial Z_D}{\partial A} \right] \exp(j\eta), \quad (12)$$

$$\frac{\partial Z_D}{\partial I} = \frac{\partial R_D}{\partial I} + j \frac{\partial X_{Dt}}{\partial I} = \left[\frac{\partial Z_D}{\partial I} \right] \exp(j\psi). \quad (13)$$

Беручи до уваги ці рівняння, амплітудно модульований та частотно модульований спектри можна представити у вигляді

$$S_{AA}(\Omega) = \frac{S_{ee}(\Omega)}{\Omega^2 \left[\frac{dZ_t}{d\omega} \right]^2 + \left[\frac{\partial Z_D}{\partial A} \right]^2 A_0^2 \sin^2(\Theta - \eta)} + \frac{S_0^2 \left[\frac{\partial Z_D}{\partial I} \right]^2 \sin^2(\psi - \Theta)}{\Omega^2 \left[\frac{dZ_t}{d\omega} \right]^2 + \left[\frac{\partial Z_D}{\partial A} \right]^2 A_0^2 \sin^2(\Theta - \eta)} S_{II}(\Omega), \quad (14)$$

$$S_{\omega\omega}(\Omega) = \frac{\left[\Omega^2 \left(\frac{dZ_t}{d\omega} \right)^2 + \left(\frac{\partial Z_D}{\partial A} \right)^2 A_0^2 \right] S_{ee}(\Omega)}{\left[\frac{dZ_t}{d\omega} \right]^2 A_0^2 \left[\Omega^2 \left(\frac{dZ_t}{d\omega} \right)^2 + \left(\frac{\partial Z_D}{\partial A} \right)^2 A_0^2 \sin^2(\Theta - \eta) \right]} + \frac{\left[A_0^2 \left(\frac{\partial Z_D}{\partial A} \right)^2 \cos^2(\eta - \Theta) \left[\frac{\partial Z_D}{\partial I} \right]^2 \sin^2(\psi - \Theta) \right]}{\left[\frac{dZ_t}{d\omega} \right]^2 \left[\Omega^2 \left(\frac{dZ_t}{d\omega} \right)^2 + \left(\frac{\partial Z_D}{\partial A} \right)^2 A_0^2 \sin^2(\Theta - \eta) \right]} + \frac{\left(\frac{\partial Z_D}{\partial I} \right)^2 \cos^2(\psi - \eta)}{\left(\frac{dZ_t}{d\omega} \right)^2} S_{II}(\Omega) \quad (15)$$

або в спрощеній формі:

$$S_{AA}(\Omega) = S_{ee}(\Omega) K_{AM}^{o2} + S_{II}(\Omega) K_{AM}^2, \quad (16)$$

$$S_{\omega\omega}(\Omega) = S_{ee}(\Omega) K_{AM}^{o2} + S_{II}(\Omega) K_{AM}^2, \quad (17)$$

де

$$K_{AM}^{o2} = \frac{1}{\Omega_m^2 \left(\frac{dZ_t}{d\omega} \right)^2 + \left(\frac{\partial Z_D}{\partial A} \right)^2 A_0^2 \sin^2(\Theta - \eta)}, \quad (18)$$

$$K_{AM}^2 = \frac{A_0^2 \left(\frac{\partial Z_D}{\partial I} \right)^2 \sin^2(\psi - \Theta)}{\Omega_m^2 \left(\frac{dZ_t}{d\omega} \right)^2 + \left(\frac{dZ_D}{dA} \right)^2 A_0^2 \sin^2(\Theta - \eta)}, \quad (19)$$

$$K_{FM}^{o2} = \frac{\Omega_0^2 \left(\frac{dZ_t}{d\omega} \right)^2 + \left(\frac{\partial Z_D}{\partial A} \right)^2}{A_0^2 \left[\Omega_m^2 \left(\frac{dZ_t}{d\omega} \right)^2 + \left(\frac{\partial Z_D}{\partial A} \right)^2 A_0^2 \sin^2(\Theta - \eta) \right]}. \quad (20)$$

Аналізуючи схему заміщення лавинно-пролітного генератора, можна помітити, що низькочастотні коливання постійного струму значною мірою залежать від вхідного опору ланцюга джерела живлення. Модуляційний шум буде максимальним, коли вхідний опір ланцюга джерела живлення дорівнює нулю і зменшується по мірі його росту.

Щоб з'ясувати додаткові способи зменшення рівня шуму діодного генератора, проаналізуємо вирази (15) та (16). Якщо знехтувати модуляційним шумом, то можна спостерігати ще один параметр, який сильно впливає на шумові компоненти генератора, а саме – кут $(\theta - \eta)$, під яким перетинаються криві комплексного опору діода та комплексного опору коливальної системи.

Амплітудно та частотно модульовані компоненти шумових флуктуацій будуть оптимальними, якщо $(\theta - \eta)$ прямує до $\pi/2$, і досягнуть свого максимуму при $(\theta - \eta) = 0$. Зазначимо, що це справедливо тільки в стійких робочих точках.

Взаємозалежність флуктуацій амплітуди та частоти тим сильніша, чим під меншим кутом пересікаються криві $Z_t(\omega)$ і $Z_D(A)$. Цю залежність можна охарактеризувати за допомогою коефіцієнта кореляції $\gamma_{A\omega}$, який може бути записаний у вигляді

$$\gamma_{A\omega} = -\cos(\Theta - \eta). \quad (21)$$

Теоретичний вид залежності коефіцієнта кореляції амплітуди та частоти $\gamma_{A\omega}$ разом із нормованим АМ спектром показаний на рис. 4.

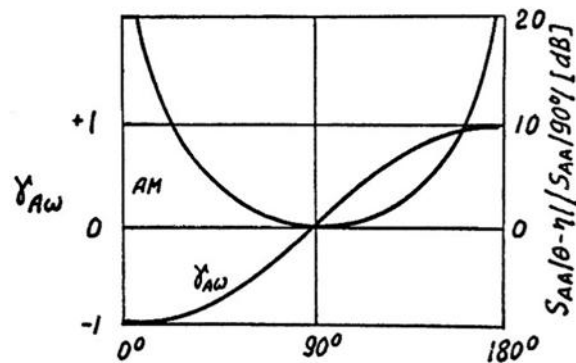


Рис. 4. Залежності $\gamma_{A\omega}$ та нормованого АМ спектру

Таким чином, чим більш складним є навантаження (наприклад, декілька резонаторів), тим більше можливостей впливу на кут θ , наслідком чого може бути оптимізація шумових параметрів генератора.

Висновки

Шумові флуктуації діодного генератора доцільно аналізувати як такі, що складаються з двох компонент – модуляційної та флуктуаційної.

При умові невеликих відхилень, що справедливо для більшості випадків, шум модуляції, при відповідному вхідному опорі схеми живлення, можна зробити мінімальним.

Високочастотний шум визначається трьома основними параметрами: безпосередньо шумом активного елементу генератора, нелінійністю активної та пасивної частин діода, частотною залежністю коливальної системи генератора.

Враховуючи це, маємо можливість оптимізувати рівень шумових флуктуацій або регулювати його.

Теоретичний аналіз шумових компонентів діодних генераторів свідчить, що в загальному випадку рівень частотно модульованого шуму діодних генераторів більш значний ніж амплітудно модульований шум, що підтверджують і практичні дослідження.

Список літератури:

1. Misawa T. Multiple uniform laguer approximation in analysis of negativ resistance in p-n junction in breakdown // IEEE Tran. Electron Devices vol. ED-14 1967. P. 795–808.
2. Misawa T. Negative Resistance in p-n Junctions Under Avalanche Breakdown Conditions, pts. I and II // IEEE Trans. Electron Devices. 1966. Vol. ED-13. P. 137–151. Jan. 1966.
3. Бондаренко М. Мікроелектроніка НВЧ. Ч. 2 : навч. посіб. Харків, 2019.
4. Олейник В.Ф., інші. Електронні прилади міліметрового та субміліметрового діапазонів на основі нанотехнологій. Київ : ООО ДВ, 2004.
5. Мельников А. И., Кобельков Г.И. Генерация та посилення радіохвиль сантиметрового та міліметрового діапазонів за допомогою напівпровідникового діода в області позитивного нахилу його статичної вольт-амперної характеристики. Диплом на открытие N24, приоритет 27.X.
6. Карушкин Н. Ф. Синхронізація генераторів на ЛПД імпульсної і безперервної дії в міліметровому діапазоні довжин хвиль. 2021. № 110–20 <http://dx.doi.org/10.15222/TKEA2021.1-2.10>
7. Micorsemi (Hrsg.): GaAs IMPATT DIODES MI5001 – MI5022. 19. Januar 2009 (archive.org [PDF; abgerufen am 5. September 2021] Datenblatt).
8. IMPATT – Diode – Radar Basics // radartutorial.eu. Christian Wolff, abgerufen am 5. September 2021.

Надійшла до редколегії 04.10.2022

Відомості про авторів:

Меняйло Олександр Дмитрович – канд. техн. наук, доц., Харківський національний університет радіоелектроніки, доцент кафедри проектування та експлуатації електронних апаратів, Україна; e-mail: oleksandr.meniailo@nure.ua; ORCID: <https://orcid.org/0000-0001-8969-2143>

Григор'єва Ольга Володимирівна – Харківський національний університет радіоелектроніки, старший викладач кафедри проектування та експлуатації електронних апаратів, Україна; e-mail: olha.hryhorieva@nure.ua; ORCID: <https://orcid.org/0000-0002-5759-8897>

Махонін Віктор Геннадійович – Харківський національний університет радіоелектроніки, асистент кафедри проектування та експлуатації електронних апаратів, Україна; e-mail: viktor.makhonin@nure.ua; ORCID: <https://orcid.org/0009-0003-5608-0513>

І.М. БОНДАРЕНКО д-р фіз.-мат. наук, *О.С. ГНАТЕНКО*, канд. фіз.-мат. наук,
О.В. ГРИЦУНОВ, д-р фіз.-мат. наук, *О.Г. ПАЩЕНКО*, канд. фіз.-мат. наук,
Г.М. БЕНДЕБЕРЯ, *М.А. КОПОТЬ*, *С.В. ГРИШКОВ*

СПЕКТРАЛЬНЕ МОДЕЛЮВАННЯ КОНКУРЕНЦІЇ ВИДІВ КОЛИВАНЬ В МАГНЕТРОНІ З СУТТЄВИМ ВПЛИВОМ ПРОСТОРОВОГО ЗАРЯДУ

Вступ

Проблема придушення та знищення малих безпілотних літальних апаратів (БПЛА) в умовах їх масового застосування здобула чималу актуальність під час російсько-української війни. Серед радіотехнічних та електронних методів її вирішення виділяють основні:

- перевантаження нелінійних електронних схем постійним мікрохвильовим випромінюванням достатньої потужності;
- незворотне пошкодження електроніки БПЛА короткими електромагнітними імпульсами потужного генератора мікрохвиль [1, 2].

У попередній роботі [3] розглянуто загальні питання комп'ютерного моделювання та оптимізації параметрів і характеристик вакуумних НВЧ приладів, що можуть бути використані в системах протидії малим та середнім БПЛА, а також в інших застосуваннях, де потрібна генерація електромагнітних НВЧ імпульсів великої інтенсивності. Програмний комплекс TULIPgm призначено для нестационарного та спектрального моделювання НВЧ приладів методом «частка в комірці» (PIC). Але окрім проєктно-конструкторського призначення, комплекс TULIPgm може бути використаний для дослідження фізичних процесів при взаємодії сповільнених електромагнітних хвиль з електронними потоками, як у схрещених полях, так і поздовжньої. Наприклад, однією з областей застосувань може бути аналіз процесів «перескоку» (зміни) видів коливань в приладах М-типу, що є одними з найбільш негативних явищ, які обмежують електронні параметри цих приладів та погіршують їх електромагнітну сумісність (ЕМС), особливо під час інтенсивного використання електромагнітного спектру НВЧ в умовах бойових дій.

Стаціонарна робота магнетронів, як і інших приладів М-типу з катодом у просторі взаємодії, на побічних модах достатньо досліджена, у тому числі шляхом чисельного моделювання (див., наприклад, [4 – 7]). Однак сам процес переходу з виду на вид вивчений неповністю, особливо це стосується еволюції спектрів збуджуючих струмів і вихідних сигналів в нестационарному режимі. Враховуючи практичну важливість цього питання з точки зору проблем ЕМС, наведемо результати чисельного аналізу зазначених явищ за допомогою спектральних моделей, що входять до складу пакету TULIPgm.

Метою статті є комп'ютерне моделювання перехідних процесів та спектрів сигналів при зміні робочого виду коливань для одного з типових різновидів приладів М-типу – магнетрона середньої потужності. Особливістю фізичних процесів взаємодії у таких генераторах є значний вплив полів просторового заряду електронної втулки та спиць (порівняно з магнетронами великої потужності) на механізм формування електронної конфігурації («хмари»), її форму та стабільність і, опосередковано, на вольтамперні характеристики (ВАХ) приладу.

Причини і види побічних коливань у магнетронах

Магнетрон є типовим представником класу НВЧ приладів М-типу з замкнутим (циліндричним) електронним потоком і катодом в просторі взаємодії. Така конструкція (замкнутий простір взаємодії) визначає не лише характер енергообміну електронного потоку з високочастотним полем на робочому виді коливань, а й специфічність побічних коливань. Основні джерела цих коливань у приладах з розподіленим катодом пов'язані з багатомодовістю періодичної (сповільнюючої) резонансної системи, властивостями електронного потоку та конструктивними особливостями простору взаємодії.

1. Електродинамічна система, яка використовується для уповільнення електромагнітної хвилі, як і будь-яка періодична система на НВЧ, є багатомодовою. У такій системі можуть збуджуватись різні види коливань (моди) як в основній, так і у вищих смугах пропускання. Ці види відрізняються один від одного власною частотою, структурою ВЧ поля у просторі взаємодії, а також напрямом поширення просторової гармоніки, з якою взаємодіє електронний потік. Зазвичай для взаємодії використовується той вид коливання, одна з просторових гармонік якого виявляється в синхронізмі з електронним потоком. Однак з різних причин у просторі взаємодії можуть збуджуватися й інші види коливань у резонансній структурі, причому частоти збудження можуть виявитися як у робочій смузі пропускання приладу, так і за її межами. Коливання на цих частотах вважаються побічними.

Побічні коливання можуть виникати також на просторових гармоніках у вищих смугах пропускання резонансної системи. Збудження просторових гармонік полегшується тим, що в приладах М-типу електронний потік є багатошвидкісним, і якась частина електронів потоку може виявитися в синхронізмі з неробочою просторовою гармонікою, причому взаємодія може здійснюватися як на прямих, так і на зворотних хвилях.

2. Іншим джерелом побічних коливань є безпосередньо електронний потік у просторі взаємодії. При взаємодії електронів із полем резонансної системи у схрещених полях форма електронного потоку суттєво інша, ніж у статичному режимі приладу. Виникає угруповання спиць: потік стає не лише багатошвидкісним з епітрохоїдальними траєкторіями електронів, що перетинаються, а різко змінюються й межі потоку. З'являються гармоніки конвекційного струму, спектр яких значною мірою визначаються формою електронних спиць. Істотними виявляються також коливання електронного потоку у напрямку осі приладу (вздовж силових ліній постійного магнітного поля). Епітрохоїдальний характер руху електронів є джерелом інтенсивних шумових коливань, властивих приладам М-типу з катодом у просторі взаємодії. І, нарешті, у замкнутому електронному потоці з'являється додаткова нестійкість, обумовлена механізмом позитивного зворотного зв'язку. Електронний потік набуває властивостей електронного багатомодового резонатора, в якому можуть збуджуватися власні коливання.

3. Збудження побічних коливань може бути внаслідок існування паразитних резонансних областей, пов'язаних з пристроями енергії, торцевими або бічними порожнинами, що примикають до робочого простору взаємодії, і залежать від особливостей конструктивного виконання приладу. Коливання можуть виникати і під дією інших факторів (форми живлячої електричної напруги, неоднорідності статичних електричного і магнітного полів тощо).

Внаслідок суттєвої нелінійності процесів у схрещених полях і відносно складних граничних умов, дослідження збудження побічних коливань у приладах М-типу з катодом у просторі взаємодії аналітичними методами принципово неможливо (навіть у стаціонарних режимах). Натомість, існуючі на сьогодні чисельні моделі РІС (обчислювальний експеримент) дозволяють відносно легко виконати такий аналіз, включаючи нестационарні режими приладів. Особливо широкі можливості щодо цього є у так званих спектральних моделей [8, 9], спеціально розроблених для вирішення подібних задач.

Далі на прикладі відносно розповсюдженого типу приладів зі схрещеними полями з катодом у просторі взаємодії – магнетрона для мікрохвильового нагріву – буде проаналізовано процеси збудження та руйнування побічних коливань і відповідні спектри вихідного сигналу, типові для більшості приладів М-типу.

Загальний опис перехідних процесів при конкуренції видів коливань

Дослідження конкуренції видів коливань в схрещених полях проводиться на чисельній моделі реального магнетронного приладу: 0,7-кіловатного магнетрона для побутових мікрохвильових печей М-136, конструктивні дані якого наведено в табл. 1. Використовується Задача Magnol (MAGNetron Oscillator) для двовимірного моделювання звичайних та інвертованих магнетронів зі складу пакета програм TULIPgm, детально описаного в публікації [3]. Алгоритми Задачі аналогічні розглянутим в роботах [10 – 14].

Таблиця 1

Параметр	Позначення	Значення
Радіус катода, мм	R_c	2,3
Радіус анода, мм	R_a	4,45
Висота анодного блока, мм	H_a	10,0
Кількість резонаторів	N	10
Товщина ламелей, град	θ	20,6
Матеріал катоду	—	Оксид
Власна частота нормального виду $N/2$, ГГц	$f_{N/2}$	2,45
Власна частота нормального виду $N/2-1$, ГГц	$f_{N/2-1}$	4,4
Власна частота нормального виду $N/2-2$, ГГц	$f_{N/2-2}$	5,3
Власна добротність нормального виду $N/2$	$Q_{intN/2}$	1400,0
Власна добротність нормального виду $N/2-1$	$Q_{intN/2-1}$	1000,0
Власна добротність нормального виду $N/2-2$	$Q_{intN/2-2}$	750,0
Внесена добротність нормального виду $N/2$	$Q_{extN/2}$	140,0
Внесена добротність нормального виду $N/2-1$	$Q_{extN/2-1}$	400,0
Внесена добротність нормального виду $N/2-2$	$Q_{extN/2-2}$	600,0
Ємність нормального виду $N/2$, пФ	$C_{N/2}$	6,84
Ємність нормального виду $N/2-1$, пФ	$C_{N/2-1}$	12,1
Ємність нормального виду $N/2-2$, пФ	$C_{N/2-2}$	15,0
Індукція постійного магнітного поля, Тл	B_0	0,157

Початкова робоча напруга магнетрона М-136 (напруга Хартрі [15, 16]) становить 2,97 кВ; максимальна робоча напруга (згідно з технічною документацією) – близько 3,9 кВ. При анодній напрузі приблизно 4,2 кВ відбувається перехід приладу з $N/2$ (основного, π) нормального виду резонансної системи (рис. 1) на сусідній ($N/2-1$) нормальний вид (рис. 2), напруга Хартрі якого становить 4,05 кВ. Перехідний процес при цьому триває приблизно 80 ... 120 нс (200 ... 300 періодів робочого виду, рис. 3). Видно, що протягом цього часу амплітуда коливання основного виду згасає приблизно за експоненціальним законом, а амплітуда коливання виду $N/2-1$ збільшується, досягаючи насичення (A/A_{max} – нормовані на стаціонарні значення амплітуди $N/2$ та $N/2-1$ видів).

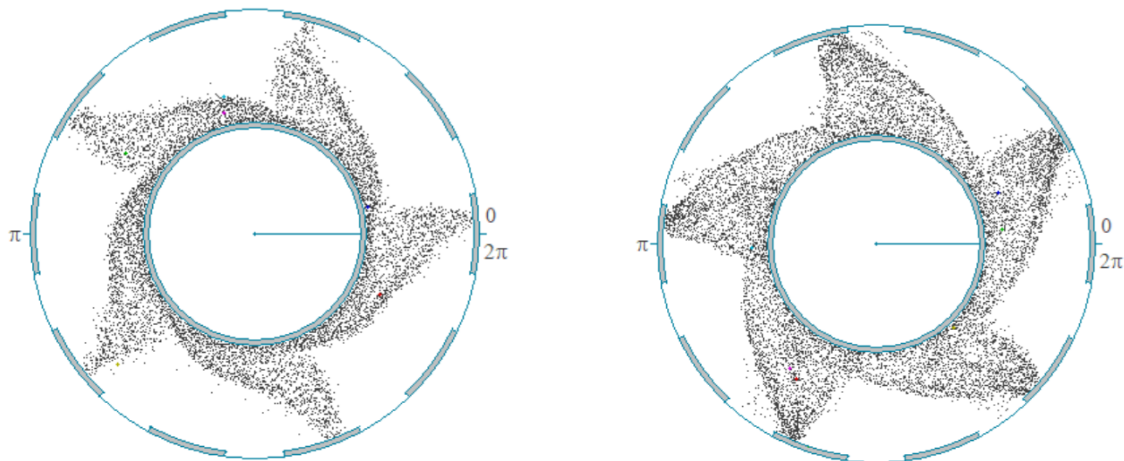


Рис. 1. Розподіли просторового заряду поблизу низьковольтної межі основного ($N/2$) виду коливань ($U_a = 3,05$ кВ, зліва) та на високовольтній межі основного виду коливань ($U_a = 4,0$ кВ, справа)

Протягом перехідного процесу конфігурація електронної хмари формується обома видами коливань з порівнянними амплітудами і є досить складною (рис. 4). Загальна тривалість транзитного періоду при зміні видів коливань визначається не інерційністю електронної хмари (з цього погляду її можна вважати практично безінерційною), а енергією, накопиченою в попередній моді коливальної системи, і енергією кінцевої моди, тобто, навантаженими добротностями обох мод. Для параметрів електродинамічної системи, наведених в

табл. 1, практичне закінчення перехідного процесу відбувається приблизно через 250 періодів основного виду коливання з моменту стрибкоподібної зміни анодної напруги з 4,1 до 4,2 кВ. До цього моменту формується стійка конфігурація електронної хмари з шістьма спицями (мінус перша просторова гармоніка нормальної моди $N/2-1$, рис. 2).

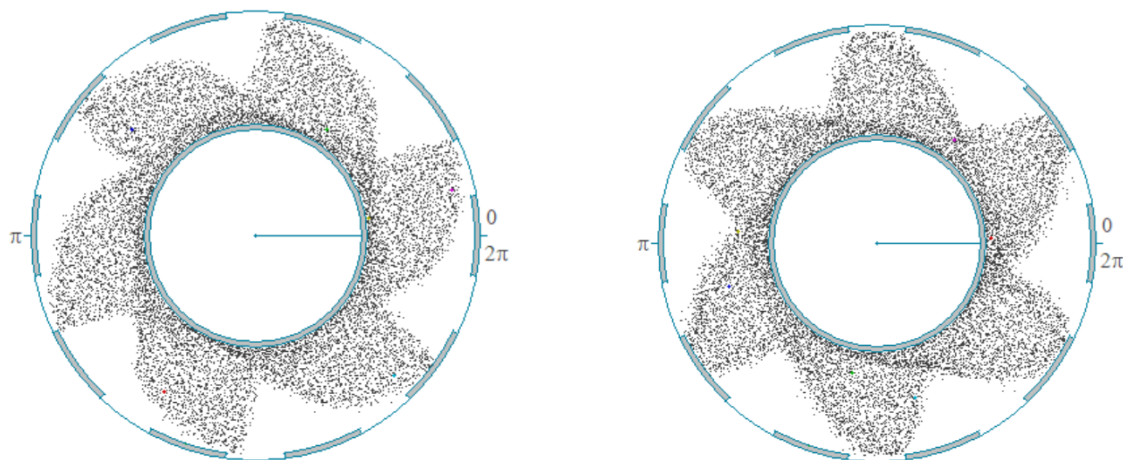


Рис. 2. Розподіли просторового заряду поблизу низьковольтної межі побічного ($N/2-1$) виду коливань ($U_a = 4,1$ кВ, зліва) та на високовольтній межі побічного виду коливань ($U_a = 4,4$ кВ, справа)

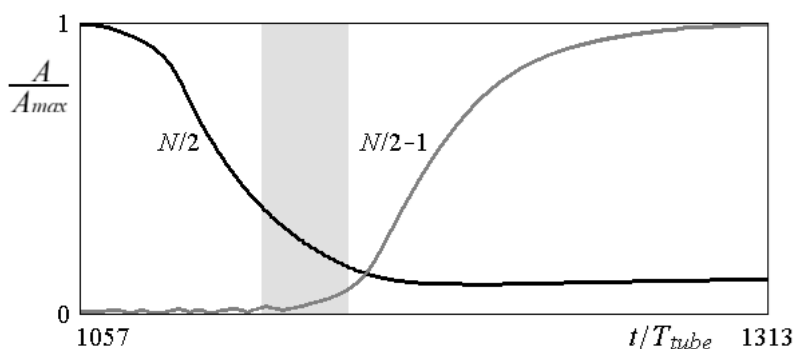


Рис. 3. Процес переходу від основного ($N/2$) виду коливань до сусіднього ($N/2-1$) виду ($U_a = 4,2$ кВ).
 A/A_{max} – нормовані амплітуди $N/2$ та $N/2-1$ видів

Специфікою приладів М-типу зі суттєвим впливом просторового заряду на процес взаємодії (як, наприклад, в магнетронах малої та середньої потужності) є гістерезисний характер ВАХ окремих видів коливань (рис. 5), що свідчить про підвищену нелінійність процесу взаємодії між електромагнітною хвилею та електронною хмарою. Гістерезис виявляється у відмінності анодних напруг, при яких має місце перехід приладу від певного типу коливань до сусіднього і навпаки. Наприклад, у дослідженому випадку при поступовому підвищенні анодної напруги при роботі на основному виді цей вид зберігається аж до напруг, близьких до $U_{12} \approx 4,2$ кВ. Лише при вказаному значенні запускається процес руйнування конфігурації електронної хмари з п'ятьма спицями. Навпаки, при зниженні анодної напруги під час роботи на ($N/2-1$) виді конфігурація з шістьма спицями продовжує існувати до аж напруг, близьких до $U_{21} \approx 4,0$ кВ, тобто руйнування її починається лише при вказаному значенні. Вочевидь, ступінь «затягування» моди визначається відносною різницею напруг перескоку $\delta U = 2|U_{21} - U_{12}| / (U_{12} + U_{21}) \approx 5\%$ для приладу, що моделюється.

З фізичного погляду описане явище гістерезису можна пояснити тим, що в суттєво нелінійних електронно-хвильових системах при наявності двох чи більше видів коливань переважуючий вплив на електронну хмару виявляє електромагнітне поле з найбільшою амплітудою. Воно «підтягує» конфігурацію угруповання спиць під вид коливання резонансної

системи, який збуджено в поточний момент, тим самим необмежено подовжуючи час його існування в області ВАХ, яка «належить» вже іншому виду.

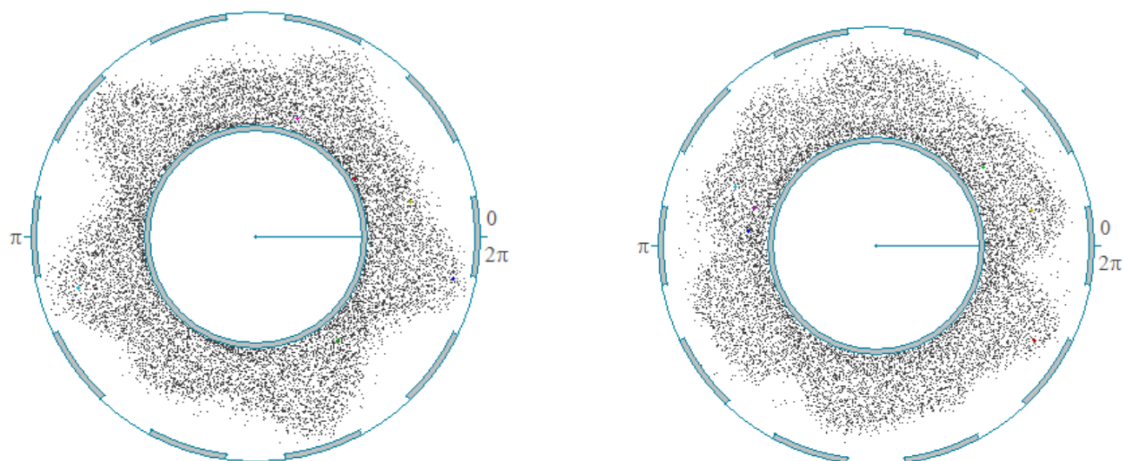


Рис. 4. Розподіли просторового заряду протягом переходу від основного ($N/2$) виду коливань до сусіднього ($N/2-1$) виду ($U_a = 4,2$ кВ, зліва) та зворотного переходу ($U_a = 4,0$ кВ, справа)

Є припущення, що δU має зменшуватися з підвищенням потужності приладу, оскільки у високоенергетичних магнетронів відносний вплив просторового заряду і, відповідно, нелінійність електронно-хвильового угруповання, зазвичай менші. Щоб це підтвердити чи спростувати, необхідні додаткові дослідження.

Поряд з дослідженням переходу між видами $N/2$ та $N/2-1$ було проведено спробу моделювання транзиту режиму роботи приладу М-136 від $N/2-1$ до $N/2-2$ виду. Напруга Хартрі виду $N/2-2$ становить 4,14 кВ, тобто лише незначно перевищує відповідну напругу моди $N/2-1$. Можливо, це є причиною того, що збудження виду $N/2-2$ не вдається спостерігати. При збільшенні анодної напруги до значень понад 4,4 кВ відбувається необоротне руйнування спицевого угруповання $N/2-1$ з відповідним поступовим зникненням анодного струму (рис. 5). Спроби досягти «штучної» переваги моди $N/2-2$ над модою $N/2-1$ (наприклад, шляхом зменшення навантаженої добротності другої) також не призводять до очікуваного результату.

Спектральні характеристики високочастотних полів та струмів

Дослідження частотних характеристик НВЧ приладів у спектральних моделях пакета TULIPgm ґрунтується на понятті так званої базової частоти приладу f_{tube} . Це не обов'язково власна частота якогось із видів коливань резонансної системи, а умовна частота, яка визначає часовий масштаб еволюції приладу, що моделюється, а також вихідні дані алгоритмів спектрального та гармонічного аналізу. Базова частота – особливість спектральних моделей [8, 9], які не «прив'язуються» до апіорі заданих частот вхідних сигналів чи очікуваних коливань потоку, як їх попередні одно- та багаточастотні аналоги. Тут використовується значення $f_{tube} = 2,3$ ГГц (нагадаємо, що

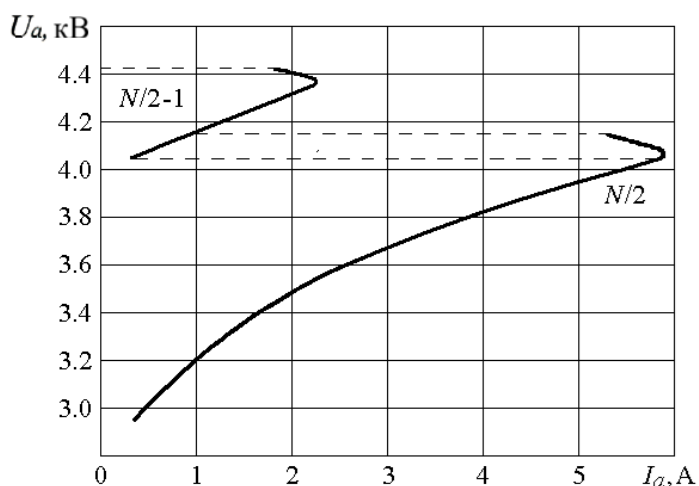


Рис. 5. ВАХ основного ($N/2$) і сусіднього ($N/2-1$) видів коливань та явище їх гістерезису

власна частота π -виду резонансної системи дорівнює 2,45 ГГц). Базову частоту завжди рекомендується вибирати дещо відмінною від частот усіх можливих видів коливань приладу, оскільки в іншому випадку деякі важливі для дослідження спектральні компоненти можуть потрапити на межу між частотними вікнами. Інколи використовується також термін «період приладу» $T_{tube} = 1 / f_{tube}$.

Гармонічний і спектральний аналіз полів і струмів НВЧ приладів у пакеті TULIPgm здійснюється за допомогою сучасних параметричних алгоритмів спектрального моделювання. Використовуються процедури спектрального аналізу дійсних і комплексних часових рядів за допомогою модифікованого коваріаційного методу [17], а також гармонічного розкладання в ряди Фур'є за допомогою первинних методів Проні і методів найменших квадратів Проні (включаючи змішаний підхід [18]) та всіх подальших їх удосконалень.

Априорі очевидно, що при зміні виду коливання магнетрона спектр збуджуючого струму (спицевого угруповання) та, відповідно, наведеного ним в резонансній системі електромагнітного поля еволюціонує від відповідного стаціонарного режиму приладу на виді $N/2$ до стаціонарного спектру цього ж приладу на виді $N/2-1$, проходячи через змішаний перехідний стан з великою кількістю комбінаційних складових. Саме в цей період виникає найбільша небезпека «засмічення» електромагнітного спектру навколишнього середовища неприпустимими для сусідніх радіотехнічних та електронних систем випромінюваннями, особливо якщо «перескоки» виду коливань відбуваються систематично (так зване «дрижання імпульсу»). Нагадаємо, що навіть у мікрохвильовій печі магнетрон, як правило, працює в імпульсному режимі [19].

Як вихідний, виберемо стаціонарний режим роботи магнетрона М-136 на виді $N/2$. Анодна напруга дорівнює 3,05 кВ (поблизу низьковольтної межі основного виду коливань). Розподіл об'ємного заряду в приладі для цього режиму показано на рис. 1, зліва. Спектр гармонік вихідного сигналу, отриманий методом найменших квадратів Проні, зображено на рис. 6. Довжина вибірки становить 256 періодів приладу. Добре просліджується домінуюча компонента основного сигналу з частотою виду $N/2$ ($1,065f_{tube}$ або 2,45 ГГц) та її друга гармоніка ($2,13f_{tube}$ або 4,9 ГГц, не показана). Також простежується частота виду $N/2-1$ ($1,91f_{tube}$ або 4,4 ГГц). Спектри вихідних сигналів при роботі магнетрона з більшими анодними напругами принципово не відрізняються від описаного, доки має місце стабільна генерація на моді $N/2$. Зокрема, відносні амплітуди бічних складових (по відношенню до основного сигналу) практично не змінюються.

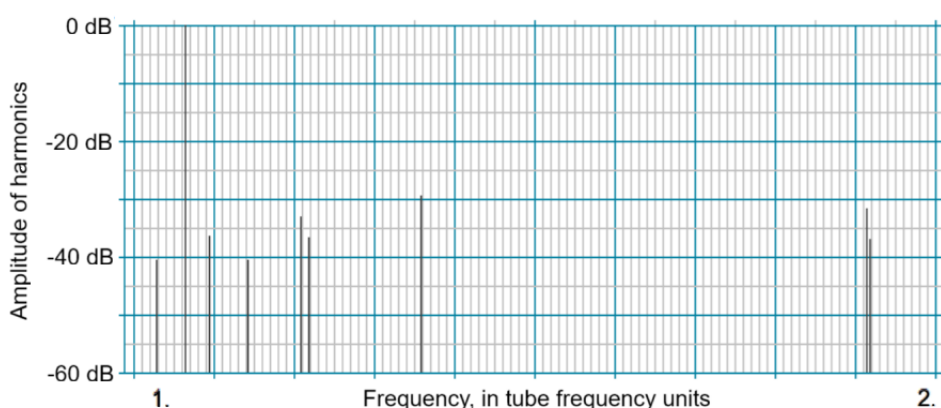


Рис. 6. Спектр вихідного сигналу поблизу низьковольтної межі основного ($N/2$) виду коливань ($U_a = 3,05$ кВ)

При збільшенні анодної напруги до 4,2 кВ починається поступове руйнування спицевого угруповання виду $N/2$ і зменшення амплітуди відповідної моди резонансної системи. Одночасно зростає амплітуда $N/2-1$ виду, злегка збудженого і раніше (при роботі приладу на π -виді). Часова залежність цієї амплітуди в загальних рисах аналогічна до наростання амплітуди робочого виду при включенні магнетрону [20] (рис. 3). Однак є суттєві відмінності у

конфігурації електронного потоку, обумовлені одночасним існуванням протягом тривалого часу обох видів коливань сумісної амплітуди. Протягом цього періоду електронна втулка піддається впливу електромагнітних полів двох нормальних мод резонансної системи з різними частотами і хвильовими числами. Як наслідок нелінійності електронного потоку в схрещених полях, структура електронної хмари стає цілком нерегулярною (рис. 4). Звідси впливає ймовірність наявності у спектрі вихідного сигналу великої кількості комбінаційних складових частот обох нормальних мод та їх гармонік, а також компонент, пов'язаних із власними коливаннями електронної хмари. На рис. 7 наведено спектр вихідного сигналу у перехідному режимі системи, отриманий в межах затемненого часового інтервалу на рис. 3. Помітно розширення смуги складових обох нормальних мод (з частотами $1,065f_{tube}$ і $1,913f_{tube}$). Крім того, спостерігається велика група спектральних компонент в околиці частоти $1,5f_{tube} = 3,45$ ГГц. На рис. 4 неможливо зіставити цим компонентам певне угруповання електронного потоку, проте складова з такою частотою чітко простежується і в спектрі наведеного струму зонда. За межами зображеного на рис. 7 діапазону з'являються також інші компоненти.

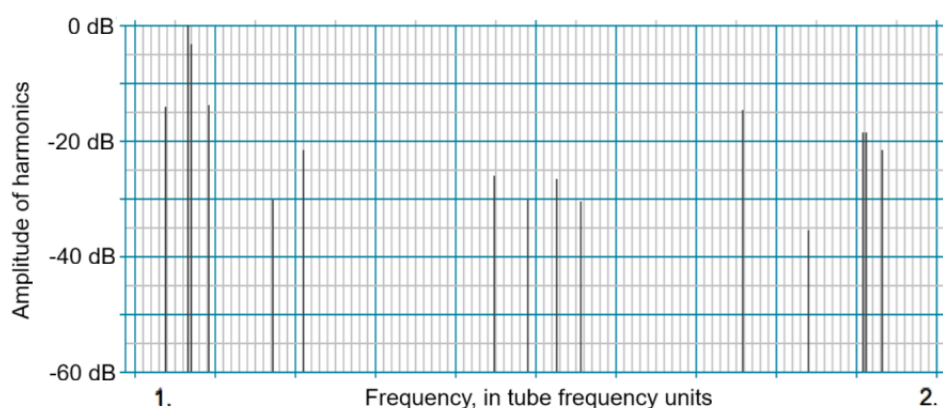


Рис. 7. Спектр вихідного сигналу у перехідному режимі системи ($U_a = 4,2$ кВ)

На момент закінчення перехідного процесу формується стійка конфігурація електронної хмари з шістьма спицями (рис. 2). Спектр вихідного сигналу «очищується» (рис. 8). Крім домінуючої складової з частотою $N/2-1$ моди ($1,91f_{tube}$ або 4,4 ГГц), в ньому присутня несподівано велика гармоніка π -виду з амплітудою близько $-(5 \dots 7)$ дБ від амплітуди високовольтної моди. Причина сильного збудження виду $N/2$ електронним потоком, конфігурація якого на перший погляд ортогональна просторовій структурі цього виду, залишається поки що нез'ясованою. Спостерігаються стабільна гармонійна компонента з частотою близько $0,85f_{tube}$ або 1,95 ГГц, що є, очевидно, різницевою частотою між видами $N/2$ та $N/2-1$, а також складова з частотою приблизно $2,74f_{tube}$ або 6,3 ГГц (обидві не показані), яка утворюється, імовірно, в результаті нелінійної взаємодії другої гармоніки виду $N/2-1$ з π -видом. Походження ще однієї порівняно стійкої гармоніки на частоті приблизно $1,74f_{tube}$ або 4,0 ГГц (також не показана) не встановлено. Можливо, вона є інтермодуляційним компонентом між іншими гармоніками зазначених видів коливань.

Для порівняння можливих спектральних оцінок, на рис. 9 показано спектр збуджуючого струму у приладі, що працює на стаціонарному $N/2$ виді (анодна напруга також дорівнює 3,05 кВ). Спектр отримано за допомогою «прозорого» зонда малого розміру, розміщеного посередині між катодом і анодом. «Прозорий» зонд генерує наведений струм, на зразок реального металевого електрода, розташованого в тому ж місці, проте, на відміну від нього, не впливає на рух електронів. Гармонічний аналіз наведеного на зонд струму здійснюється модифікованим коваріаційним методом. Довжина вибірки дорівнює $256T_{tube}$. Порівняно з рис. 6, спектр на рис. 9 містить більше гармонічних компонент, але значна частина їх – малоінформативні шуми моделі. Тому завжди бажано використання різних методів оцінки спектрів.

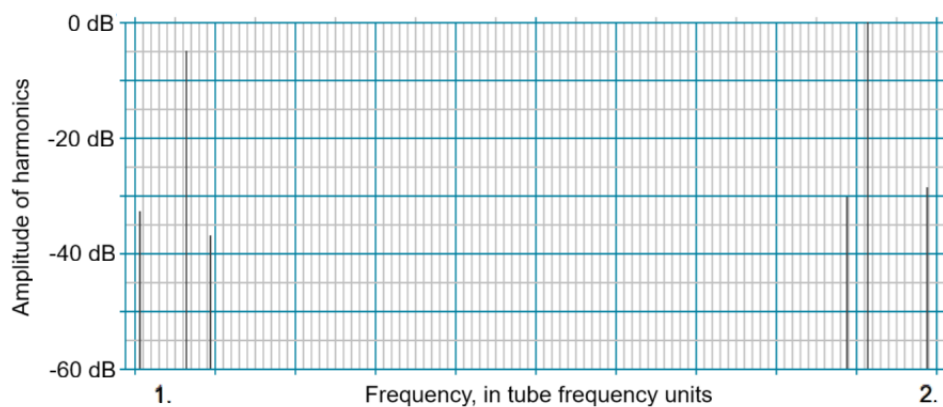


Рис. 8. Спектр вихідного сигналу на високовольтній межі побічного ($N/2-1$) виду коливань ($U_a = 4,4$ кВ)

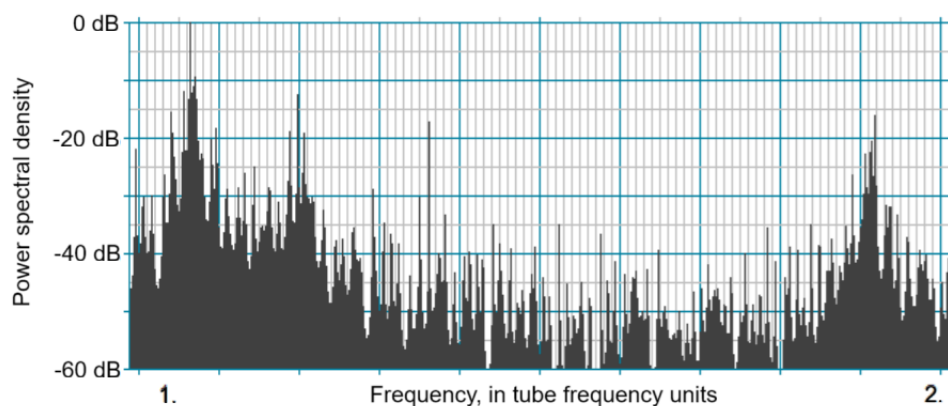


Рис. 9. Спектр збуджуючого струму поблизу низьковольтної межі основного ($N/2$) виду коливань ($U_a = 3,05$ кВ)

Висновки

1. Спонтанна (незапланована) зміна видів коливань є одним з найбільш неприємних явищ, які обмежують електронні параметри приладів М-типу як малої, так і великої потужності, негативно впливають на якість сигналу та погіршують електромагнітну сумісність з іншими радіоелектронними системами, особливо під час інтенсивного використання електромагнітного спектру НВЧ в умовах бойових дій.

2. Повноцінне комп'ютерне моделювання процесів конкуренції видів коливань у принципово нелінійних приладах зі схрещеними полями стало можливим лише після появи спеціально розроблених для цієї мети алгоритмів, відомих під назвою «спектральні моделі».

3. Особливості зміни видів коливань у магнетронних приладах з розподіленим катодом визначаються, серед іншого, впливом об'ємного заряду електронного угруповання. При суттєвій (порівняно з соленоїдними полями електродинамічної системи) ролі кулонівської взаємодії в електронному потоці ВАХ конкуруючих видів набувають гістерезисного характеру.

Список літератури:

1. Atherton K.D. (2023) The Air Force Used Microwave Energy to Take Down a Drone Swarm. Available at: <https://www.popsci.com/technology/thor-weapon-drone-swarm-test/>
2. Nikolov B. (2025) UK's new microwave weapon neutralizes drone swarms for pennies, Bulgarian Military Industry Review. Available at: <https://bulgarianmilitary.com/2025/04/17/uks-new-microwave-weapon-neutralizes-drone-swarms-for-pennies/>
3. Бондаренко І.М., Гнатенко О.С., Грицунов О.В., Пашенко О.Г., Карнаушенко В.П., Копоть М.А. Архітектура програмної системи TULIPgm для проєктування вакуумних підсилювачів і генераторів НВЧ-діапазону // Радіотехніка. 2025. Вип. 221. С. 113–126.
4. Churyumov G.I., Frolova T.I., Gritsunov A.V., Nikitenko O.M., Prokopchik V.A. Analysis of mode competition in magnetrons // Proc. Fifth IEEE Int. Vacuum Electronics Conf. (IVEC 2004), Monterey, California (USA). P. 232–233.

5. Baiburin V.B., Eremin V.P., Sysuev A.V. et al. Numerical modeling of magnetron generators with allowance for the mode competition // *Tech. Phys. Lett.* 2000. Vol. 26. P. 153–155.
6. Neculaes, V.B., Gilgenbach R.M., Lopez M. et al. Mode Competition in Relativistic Magnetrons and Injection Locking in KW Magnetrons // *AIP Conference Proceedings*. 2003. Vol. 691, No. 1. P. 301.
7. Zheng Q., Bi L., Li H. and Shen D. Suppression of Mode Competition in High-efficiency Phase-locking between High-power Magnetrons // *2024 Photonics & Electromagnetics Research Symposium (PIERS)*, Chengdu, China. P. 1–4.
8. Gritsunov A.V. On Spectral Modeling of Microwave Devices // *Telecomm. and Radio Engineering*. 2001. Vol. 55, No. 8. P. 98–102.
9. Gritsunov A.V. On a spectral approach to simulation of microwave devices // *Journal of Communications Technology and Electronics*. 2004. Vol. 49, No. 7. P. 829–832.
10. Hockney R.W., Eastwood J.W. *Computer Simulation Using Particles* / R.W. Hockney. McGraw-Hill, Inc., 1981. 562 p.
11. Vasyanovich A.V., Gritsunov A.V., Nikitenko A.N., Horunzhii M.O. General principles of spectral modeling of microwave devices // *Telecommunications and Radio Engineering*. 2003. Vol. 60, No. 1-2. P. 88–99.
12. Bilotserkivska A.I., Bondarenko I.M., Gritsunov A.V., Babychenko O.Yu., Sviderska L.I., Vasianovych A.V. Decomposition of electromagnetic potentials in partial functions of dispersive electrodynamic lines // *Ukrainian J. of Physics*. 2024. Vol.69, No. 6. P. 382–394.
13. Gritsunov A.V. Methods of calculation of nonstationary nonharmonic fields in guiding electrodynamic structures // *Journal of Communications Technology and Electronics*. 2007. 52, No. 6. P. 601–616.
14. Gritsunov A.V. About simulation of fields in large particles model // *Proc. 1997 SBMO/IEEE MTT-S Int. Microwave and Optoelectronics Conf.* 1997. Vol. 2, Natal (Brazil). P. 517–519.
15. Carter R.G. *Microwave and RF Vacuum Electronic Power Sources* / R.G. Carter. Cambridge Univ. Press, 2018. 808 p.
16. Tsimring S.E. *Electron Beams and Microwave Vacuum Electronics* / S.E. Tsimring. Wiley-Interscience, 2006. 574 p.
17. Marple S.L., Jr., *Digital Spectral Analysis with Applications*. / S.L. Marple, Jr. Prentice-Hall, Inc. 1987. 492 p.
18. Gritsunov A.V., Turenko L.Y. Harmonic decomposition of an exciting current in simulation of the electron devices // *Telecommunications and Radio Engineering*. 2002. Vol. 58, No. 11–12. P. 56–67.
19. Chernousov Y., Novel high power pulsed mode operation of commercial continuous-wave magnetron / *IEEE Trans. on Electron Devices*. 2023. Vol. 70, no. 2. P. 826–829.
20. Грицунов О.В. Збудження електромагнітних коливань довільного спектрального складу замкненими електронними потоками в системах зі схрещеними полями : дис. ... д-ра фіз.-мат. наук: 01.04.04. Харків, 2006. 374 с.

Надійшла до редколегії 27.09.2025

Відомості про авторів:

Бондаренко Ігор Миколайович – д-р фіз.-мат. наук, професор, Харківський національний університет радіоелектроніки, завідувачий кафедрою мікроелектроніки, електронних приладів та пристроїв, Україна; e-mail: ihor.bondarenko@nure.ua; ORCID: <https://orcid.org/0000-0003-3907-6785>

Гнатенко Олександр Сергійович – канд. фіз.-мат. наук, доцент, Харківський національний університет радіоелектроніки, завідувачий кафедрою фізичних основ електронної техніки, Україна; e-mail: oleksandr.hnatenko@nure.ua; ORCID: <https://orcid.org/0000-0001-7722-0923>

Грицунов Олександр Валентинович – д-р фіз.-мат. наук, професор, Харківський національний університет радіоелектроніки, професор кафедри мікроелектроніки, електронних приладів та пристроїв, Україна; e-mail: alexander.gritsunov@nure.ua; ORCID: <https://orcid.org/0000-0002-2258-4006>

Пашченко Олексій Георгійович – канд. фіз.-мат. наук, доцент, Харківський національний університет радіоелектроніки, доцент кафедри мікроелектроніки, електронних приладів та пристроїв, Україна; e-mail: olexiy.pashchenko@nure.ua; ORCID: <https://orcid.org/0000-0001-8927-3811>

Бендеберя Геннадій Миколайович – Харківський національний університет радіоелектроніки, старший викладач кафедри мікроелектроніки, електронних приладів та пристроїв, Україна; e-mail: hennadii.bendeberia@nure.ua; ORCID: <https://orcid.org/0000-0002-0070-4927>

Копоть Михайло Андрійович – Харківський національний університет радіоелектроніки, завідувачий навчальною лабораторією кафедри програмної інженерії, Україна; e-mail: mykhaylo.kopot@nure.ua; ORCID: <http://orcid.org/0000-0002-7163-8904>

Гришков Святослав В'ячеславович – Харківський національний університет радіоелектроніки, аспірант кафедри мікроелектроніки, електронних приладів та пристроїв, Україна; e-mail: sviatoslav.hryshkov@nure.ua.

*D.V. SLIUSAR, O.M. CHUGAI, I.V. KOLODIY, S.V. OLIYNYK, O.O. POLUBOIAROV,
Y.A. VOLOSHYN, S.M. KULISH*

COMPOSITION, STRUCTURE AND MICROHARDNESS OF MULTICOMPONENT TUNGSTEN CARBIDE BASED COATINGS FORMED USING THE INVERSE MAGNETRON SPUTTERING SYSTEM

Introduction

Composition of crystalline materials is known to be one of the factors determining their physical properties. Therefore, it is not surprising that in recent decades there has been a sharp increase in interest in multicomponent materials. A special place among such materials is occupied by high-entropy alloys (HEAs) containing five or more components [1]. This feature of the composition, causing distortions of the crystal lattice, has a significant influence on many physical properties of materials, especially mechanical ones. For this reason, early studies of VPPs were mainly devoted to their mechanical properties [2]. However, in recent years, the range of problems related to the creation of new materials of this type has significantly expanded. Accordingly, prospects for their wider practical application have emerged.

One of the promising practical applications of these alloys is related to the creation of highly efficient thermoelectric energy converters [3-5]. It should be noted in this connection that the existence of a fundamental possibility to change the material structure, the solubility limit of specific elements in it, as well as thermal and electrical properties by varying the composition has served as a basis for the introduction of a new term "entropic materials engineering" [3].

Additional opportunities for controlling the thermal and electrical properties of HESs arise when semiconductor compounds are used for their creation. Thus, it was shown in [4] that the optimal combination of thermal and electrical properties in the $(\text{GeTe})_1-(\text{MnZnCdTe}_3)_x$ system can be achieved by doping with the donor impurity Sb.

An important practical aspect of the fabrication of HPPs of a particular composition is the choice of appropriate technology and equipment. It is well known that not only the composition and total concentration of background impurities, but also distortions of the crystal lattice depend on this choice.

Traditional methods of forming multi-component coatings are characterized by preliminary production of material of the same composition with subsequent transfer to the surface of the product. This significantly complicates the process of coating formation and makes it inflexible due to the need to form coatings of different composition. Therefore, there is an urgent need to develop new technologies for the formation of multicomponent coatings.

One of the concepts for solving the mentioned problem is to use technologies based on simultaneous sputtering (co-sputtering) of individual components of the coating by corresponding controlled sources [6]. It should be noted that in recent years there has been a significant increase in interest in such technologies and corresponding equipment [7]. At the same time, when implementing any of the mentioned technologies, it is problematic to ensure the uniformity of the composition of the coating over the area of the product [8].

A natural way to solve this problem is to increase the number of sources of individual coating components while simultaneously reducing their size. However, a significant reduction in the size of traditional sources runs into fundamental limitations of both a physical and constructive character. So, the development of such a sputtering system for the formation of multi-component coatings, which on the one hand would have in its composition a sufficiently large number of independent sources of coating components, which sizes can be varied within wide limits, and on the other hand would provide the possibility of controlling the mode of operation of each of these sources is actual today.

A new ion-plasma sputtering system was created at Kharkiv National Aerospace University «Kharkiv Aviation Institute» [9], which is a type of inverse magnetron systems [10]. The system provides sputtering of a large number of target cathodes of a simple design, made of individual coating components. Due to the absence of fundamental restrictions on the size of target cathodes, there is a possibility of forming homogeneous coatings of almost any composition.

At the same time, our experience of operating the specified ion-plasma system indicates that the process of target cathodes sputtering with accelerated ions is affected by a number of interrelated parameters (electrical potentials on the electrodes of the sputtering system, current through the solenoids of the magnetic system, pressure of the plasma-forming gas, etc.). The consequence may be the sputtering of other structural elements of the technological chamber, and therefore uncontrolled alloying of the coating with additional components. Therefore, the objective of our work is to study the influence of metals from the composition of its structural elements on the structure and microhardness of WC coatings formed using a sputtering system.

Specimens and methods of research

Multicomponent coatings were formed on substrates made of 14X17 steel using inverse magnetron sputtering systems with a virtual anode, sectioned cathode assemblies with radial plasma flows. Segmented target cathodes made of pure tungsten and graphite were used to form tungsten carbide coatings. The thickness of the coatings was 3-6 microns.

The content of additional elements in the composition of the obtained coatings is due to the scattering of elements of the technological compartment, namely electrical screens. The sputtering process of these screens was controlled by changing the electrical potential on them during the formation of the coatings. The composition of the obtained coatings was studied using a scanning electron microscope REM-106.

X-ray structural analysis was performed on a DRON-4-07 diffractometer in copper Cu-K α radiation using a nickel selective absorption filter. The rays reflected from the specimen were recorded by a scintillation detector. Instrumental conditions for recording diffractograms were the same for all specimens.

The diffractograms were subjected to standard processing (background separation, selection of the K α 1-doublet, approximation of the diffraction peaks by the pseudo-Voigt function), which is necessary for the calculation of the coatings structure parameters.

The calculation of the specimen's coherent-scattering region (CSR) was carried out according to Scherer's formula [11]

$$D = \frac{\lambda}{\beta \cos(\theta)}, \quad (1)$$

where D is the size of the CSR; λ – X-ray radiation wavelength; β – the actual physical expansion, and θ – the diffraction angle.

It should be noted that Scherer's formula gives an approximate size of the CSR, since it takes into account only the broadening of the diffraction peaks due to dimensional effects.

But since not all diffractograms have lines of two orders, the calculation was carried out by this method, and not by Williamson-Hall's [12].

The analysis was performed for the line due to the (111) plane. Annealed silicon powder had been used as a sample for determining instrumental line expansion.

Using the value of the integral half-width of the reference sample lines, we had obtained an instrumental function that has been used to extract the true expansion β from the total expansion of the specimen lines.

The microhardness of the specimens was measured using a PMT-3 microhardness tester, the weight of the load was 20 g.

Results and Discussion

The composition of the studied coating specimens is given in the table 1. From it, we can see that in addition to the main components of the coatings – W and C – a large number of other elements are observed in their composition, in particular: Fe, Mo, Cr, Ni, Ti and O. The content of the last component in the composition of the coatings is probably due to the adsorption of water vapor by the surface of the specimens during their fitting in the technological compartment of the electron microscope. At the same time, the absence of H in the composition of coatings can be explained by the low sensitivity of the microscope analyzer sensor to light elements.

According to the data presented in the table, the content of tungsten in the specimens varies widely. Moreover, as the content of this element decreases, the content of iron increases. At the same time, the chromium content does not change significantly from specimen to specimen. Nickel and titanium were found only in some specimens. It should be noted that the content of these two elements is relatively small.

In our opinion, the presence of Fe, Cr, Ni and Ti in the coatings is due to the fact that, in addition to the target cathodes, only electric shields made of 12X18N9T steel, which includes these elements, were sprayed in a controlled manner during the formation of the coatings.

Typical X-ray diffractogram for studied coatings is shown on Figure 1. According to the results of structural and substructural characteristics calculation, only cubic tungsten carbide WC (structural type B1, space group #225 [13]) with a rather small size of the DKR was found in the coatings. At the same time, in all specimens, the tungsten carbide lattice parameter significantly exceeds the value known from literary sources ($a = 4.215\text{\AA}$ [14]). Most likely, this is due to the presence of mechanical macrostresses in the coatings.

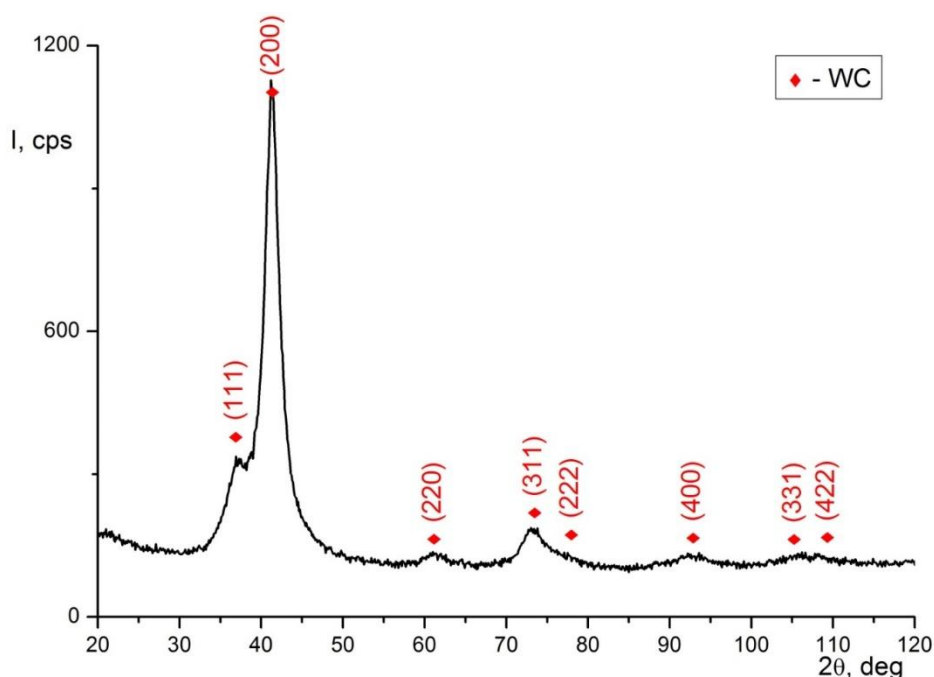


Fig. 1. Typical X-ray diffractogram for WC coatings

A comparative analysis of the CSR size, lattice period, and microhardness of coating specimens have shown (Fig. 2) that with an increase in the first parameter, there is a tendency for decrease of the other two. Moreover, the microhardness of one of the coating specimens reaches 17 GPa, which is a completely acceptable value for protective coatings based on tungsten carbide [15].

An important feature of the studied coating specimens is the presence of texture (200) in most of them. This is consistent with the results of our previous studies of WC coatings structure, which were also formed by the method of magnetron sputtering [16].

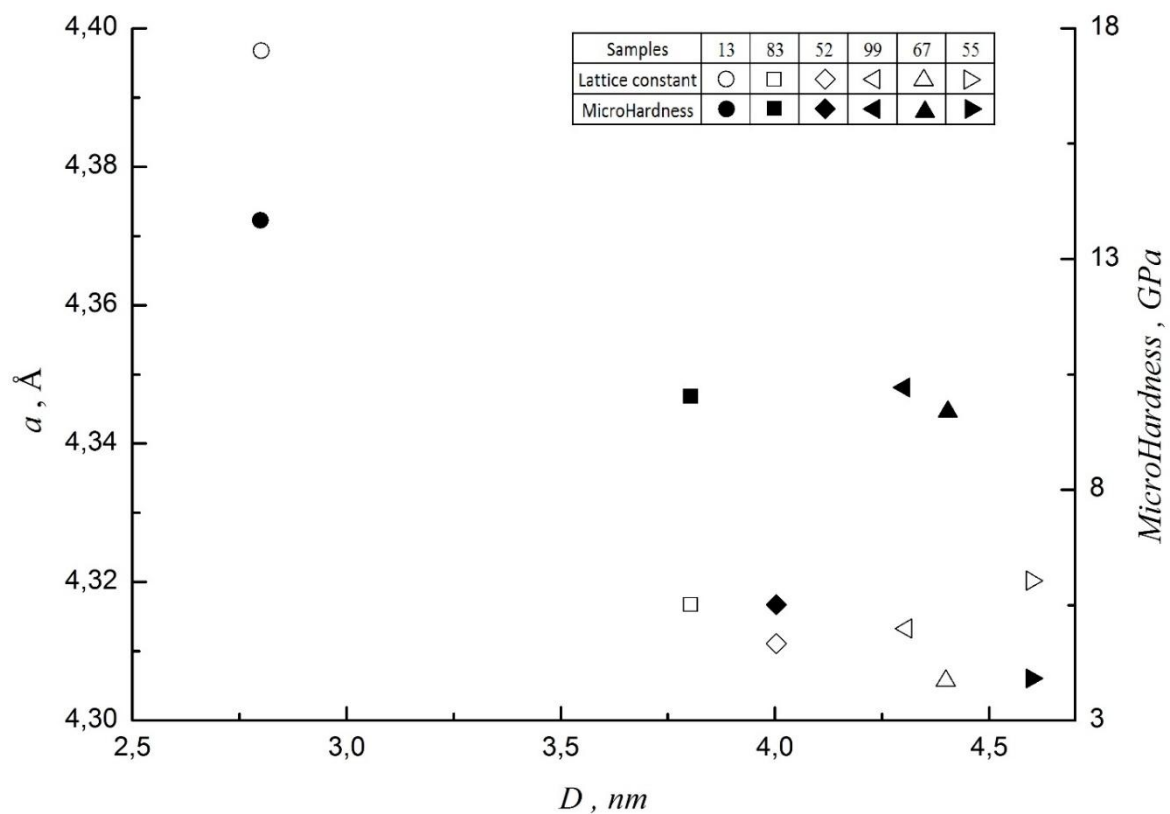


Fig. 2. Dependence of the lattice parameter and microhardness of WC coating specimens on the size of the co-herent-scattering region

Table 1

Content of elements in coating specimens

# of specimen	Mass content of elements in the coating, at. %								Microhardness,
	W	Fe	Mo	Cr	C	Ni	Ti	O	
13	75,6	6,5	9,2	1,3	4,8	-	-	2,6	17,5
67	72,4	6,9	11,9	1,2	4,5	-	2,8	0,3	5,0
83	68,6	8,6	11,9	1,4	4,3	-	3,2	2,0	5,5
52	63,7	15,2	9,3	4,8	4,2	1,6	-	1,2	4,7
99	61,8	15,2	10,8	3,1	4,3	0,9	3,4	0,5	3,9
55	43,5	32,1	5,9	9,8	2,9	4,1	-	1,7	6,0

The given data obviously testify to the determining influence not only of the composition, but also of significantly non-equilibrium formation conditions on the structure and microhardness of the investigated coatings. It is the non-equilibrium conditions of atoms condensation, the nature of their interaction both with each other and with the substrate that causes the appearance of texture [17] and the substructure of coatings. The point of the maximal weakening of impurities influence on the structure and mechanical properties of WC coatings requires further research.

Conclusions

As a result of additional sputtering of metals from the structural elements of the inverse magnetron sputtering system with sectioned cathode assemblies, multicomponent coatings based on tungsten carbide were formed. For the first time, the influence of the mentioned metals composition on the period of the crystal lattice, the size of X-rays coherent scattering region and the microhardness of coatings based on tungsten carbide have been determined. For the entire set of coating specimens, the specified parameters are related to each other. It is assumed that the listed features of the crystal structure and the presence of texture are determined not only by additional components in the composition of coatings, but also by significantly non-equilibrium conditions of their formation.

The obtained data, in our opinion, indicate the prospects of managing a wide range of physical and technical properties, including tribological, of multicomponent coatings based on tungsten carbide during their formation using inverse magnetron sputtering systems with sectioned cathode assemblies

References:

1. Huang Y., Zhi S., Zhang S., Yao W., Ao W., Zhang C., Liu F., Li, J. and Hu L. (2022). Regulating the Configurational Entropy to Improve the Thermoelectric Properties of $(\text{GeTe})_{1-x}(\text{MnZnCdTe}_3)_x$ Alloys. *Materials* [Electronic resource]. 15(19), 6798. doi: 10.3390/ma15196798.
2. Li W., Xie D., Li D., Zhang Y., Gao Y. and Liaw P. K. (2021). Mechanical behavior of high-entropy alloys. *Progress in Materials Science* [Electronic resource]. 100777. doi: 10.1016/j.pmatsci.2021.100777.
3. Jiang B., Yu Y., Cui J., Liu X., Xie L., Liao J., Zhang Q., Huang Y., Ning S., Jia B., Zhu B., Bai S., Chen L., Pennycook S. J. and He J. (2021). High-entropy stabilized chalcogenides with high thermoelectric performance. *Science* [Electronic resource]. 371(6531), 830–834. doi: 10.1126/science.abe1292.
4. Huang Y., Zhi S., Zhang S., Yao W., Ao W., Zhang C., Liu F., Li J. and Hu L., (2022). Regulating the Configurational Entropy to Improve the Thermoelectric Properties of $(\text{GeTe})_{1-x}(\text{MnZnCdTe}_3)_x$ Alloys. *Materials* [Electronic resource]. 15(19), 6798. doi: 10.3390/ma15196798.
5. Xia M., Record M.C. and Boulet P. (2022). Investigation of p-type high-entropy thermoelectric alloy: A DFT approach. *Materials* [Electronic resource]. 16(1), 235. doi: 10.3390/ma16010235.
6. Yan X. H., Li J. S., Zhang W. R. and Zhang Y. (2018). A brief review of high-entropy films. *Materials chemistry and physics* [Electronic resource]. 210, 12–19. doi: 10.1016/j.matchemphys.2017.07.078.
7. Nagy P., Rohbeck N., Roussely G., Sortais P., Lábár J. L., Gubicza J., Michler J. and Pethő L. (2020). Processing and characterization of a multibeam sputtered nanocrystalline CoCrFeNi high-entropy alloy film. *Surface and coatings technology* [Electronic resource]. 386, 125465. doi: 10.1016/j.surfcoat.2020.125465.
8. Zhang W., Liaw P. K. and Zhang Y. (2018). Science and technology in high-entropy alloys. *Science china materials* [Electronic resource]. 61(1), 2–22. doi: 10.1007/s40843-017-9195-8.
9. Isakov A.V., Kolesnik V.P., Olshrimovskyy A.M., Stepanushkin N.P. and Taran A.A. Numerical simulation of abnormal glow discharge processes in crossed electric and magnetic fields. *V: International Conference-School on Plasma Physics and Controlled Fusion and the Adjoint Workshop 'Nano- and micro-sized structures in plasmas', KhFTI NAS, Ukraine. C.* 171–174.
10. Thornton J. A. (1978). Substrate heating in cylindrical magnetron sputtering sources. *Thin solid films* [Electronic resource]. 54(1), 23–31. doi: 10.1016/0040-6090(78)90273-0.
11. Vinila V. S., Isac J. Synthesis and structural studies of superconducting perovskite $\text{GdBa}_2\text{Ca}_3\text{Cu}_4\text{O}_{10.5+\delta}$ nanosystems. *Design, Fabrication, and Characterization of Multifunctional Nanomaterials*. 2022. P. 319–341. URL: <https://doi.org/10.1016/b978-0-12-820558-7.00022-4>.
12. Nath D., Singh F. and Das R., (2020). X-ray diffraction analysis by Williamson-Hall, Halder-Wagner and size-strain plot methods of CdSe nano-particles- a comparative study. *Materials chemistry and physics* [Electronic resource]. 239, 122021. doi: 10.1016/j.matchemphys.2019.122021.
13. Cenizal, K., Gladyshevskii, R. and Villars, P., (2014). *Handbook of inorganic substances*. De Gruyter, Inc.
14. Shanenkov I., Nikitin D., Ivashutenko A., Rahmatullin I., Shanenkova Y., Nassyrbayev A., Han W. and Sivkov A. (2020). Hardening the surface of metals with WC_{1-x} coatings deposited by high-speed plasma spraying. *Surface and coatings technology* [Electronic resource]. 389, 125639. doi: 10.1016/j.surfcoat.2020.125639.
15. Winarto W., Sofyan N. and Rooscote D. (2017). Porosity and wear resistance of flame sprayed tungsten carbide coatings/ GREEN PROCESS, MATERIAL, AND ENERGY: A SUSTAINABLE SOLUTION FOR CLIMATE CHANGE: Proceedings of the 3rd International Conference on Engineering, Technology, and Industrial Application (ICETIA 2016), Surakarta, Indonesia [Electronic resource]. doi: 10.1063/1.4985482.
16. Kolesnyk V. P., Chuhai O. M., Slyusar D. V., Kalakhan O. S., Voloshyn O. O., Oleinyk S. V. and Veselivska H. H. (2019). Structure and properties of ionic plasma WC coatings. *Materials science* [Electronic resource]. 55(2), 220–224. doi: 10.1007/s11003-019-00292-1.
17. Bochulia T.V. and Sobol O.V. (2017). The use of structural engineering for obtaining superhard coatings based on nitrides transition metals. *Machines. technologies. materials* [Electronic resource]. 10(2), 77–83. <https://stumejournals.com/journals/mtm/2017/2/77.full.pdf>.

Надійшла до редакції 12.10.2025

Відомості про авторів:

Слюсар Денис Віталійович – канд. техн. наук, Національний аерокосмічний університет «Харківський авіаційний інститут», доцент кафедри космічної техніки та нетрадиційних джерел енергії, Україна; e-mail: d.sliusar@khai.edu; ORCID: <https://orcid.org/0000-0002-8314-6587>

Чугай Олег Миколайович – д-р. техн. наук, Національний аерокосмічний університет «Харківський авіаційний інститут», професор кафедри фізики, Україна; e-mail: oleg.chugai@khai.edu; ORCID: <https://orcid.org/0000-0002-2857-6592>

Колодій Ігор Вікторович – Національний науковий центр "Харківський фізико-технічний інститут" (ННЦ ХФТІ), молодший науковий співробітник, Україна; ORCID: <https://orcid.org/0000-0001-8598-9732>

Олійник Сергій Володимирович – д-р. техн. наук, Національний аерокосмічний університет «Харківський авіаційний інститут», доцент кафедри фізики, Україна; e-mail: sergey.oliynick@khai.edu; ORCID: <https://orcid.org/0000-0001-6073-8531>

Полубояров Олексій Олександрович – канд. техн. наук, Національний аерокосмічний університет «Харківський авіаційний інститут», старший викладач кафедри фізики, Україна; e-mail: o.poluboiarov@khai.edu, ORCID: <https://orcid.org/0000-0002-8587-8669>

Волошин Юлія Андріївна – PhD, Національний аерокосмічний університет «Харківський авіаційний інститут», доцент кафедри радіоелектронних та біомедичних комп'ютеризованих засобів та технологій, Україна; e-mail: y.voloshyn@khai.edu; ORCID: <https://orcid.org/0000-0003-4138-6731>

Куліш Сергій Миколайович – канд. техн. наук, Національний аерокосмічний університет «Харківський авіаційний інститут», професор кафедри радіоелектронних та біомедичних комп'ютеризованих засобів та технологій, Україна; e-mail: s.kulish@khai.edu; ORCID: <https://orcid.org/0000-0002-5506-2714>

BLDC MOTOR CONTROL SYSTEMS ANALYSIS

Introduction

The use and performance of brushless direct current (BLDC) motors are significantly related to the electronic switching and control system that is required to operate these motors. Therefore, in the past, the use of BLDC motors was limited by the additional cost of the motor controller and its dependence on the control quality indicators and the complexity of the algorithms. Now the use of these motors is constantly increasing due to the evolution in the field of semiconductors and the rapid growth of computing capabilities of microprocessor systems and their reduction in their cost. This allows the implementation of compact devices with high performance while maintaining low costs.

BLDC motors have long been used in industrial applications such as electric drives, feed drives for CNC machines, industrial robots, extruder drives, etc. Due to such characteristics as compact size, constant mechanical torque, long service life, reduced weight, high speed range and the absence of sparks and noise, BLDC motors are successfully used in a wide range of applications.

The main areas of application of BLDC [1]: industry, automotive, HVAC systems, semiconductor industry, computer technology, home appliances, quadcopters and drones, robotics, medical industry, prosthetics.

In addition, the design features of BLDC motors, compared to other types of motors, allow for better heat dissipation, thus further expanding their application areas. A detailed overview of applications in these industries is given in article [1].

A brushless direct current (BLDC) motor is a synchronous AC motor with permanent magnets on the rotor (moving part) and windings on the stator (stationary part). The permanent magnets create the rotor flux, and the energized stator windings create the poles of the electromagnet.

The motor's work of converting electrical energy into mechanical energy is based on the attraction or repulsion between magnetic and electro-magnetic poles. In the simplified structure of a three-phase motor [2], shown in fig. 1, the process begins when current flows through one of the three stator windings and creates a magnetic pole that attracts the nearest permanent magnet of the opposite pole.

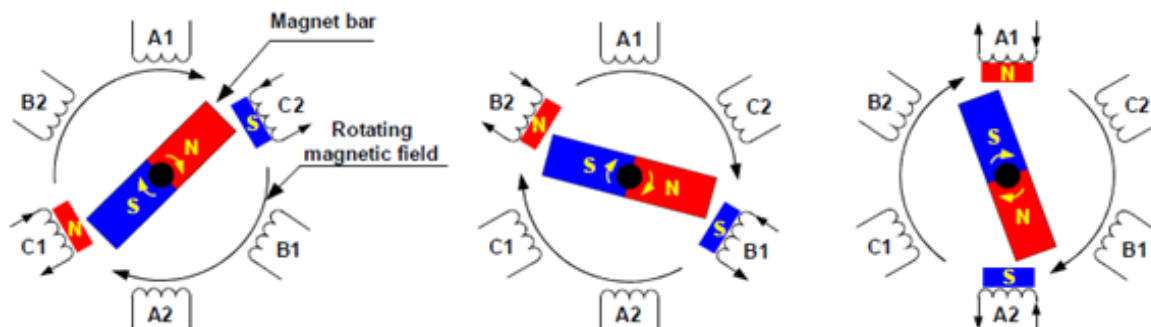


Fig. 1. Simplified diagram of a BLDC motor rotation

An important feature and characteristic of BLDC motor is the trapezoidal shape of the back EMF, which is created by a certain way of connecting the stator coils.

BLDC motor is a symmetrical three-phase system, where BEMF phase voltages are shifted by one third of field angle period ($2\pi/3$). BEMF voltage depends on rotor angle as shown in fig. 2.

This feature allows to implement very simple methods to control the motor with rectangular pulses. A BLDC motor with permanent magnets and trapezoidal back EMF then consumes rectangular currents.

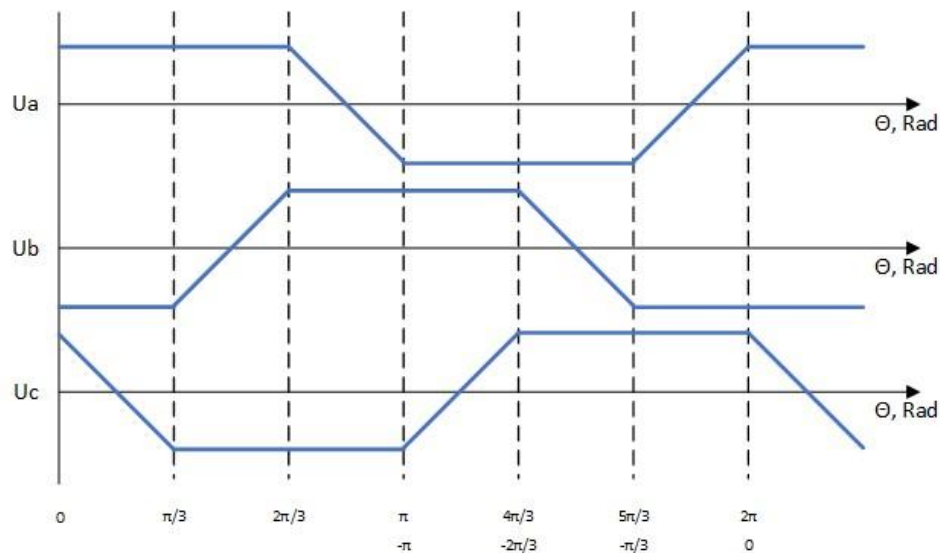


Fig. 2. BLDC motor phase Back EMF voltages

The line-to-line BEMF shape of the motor is calculated as the difference between phase voltages and this is shown in fig. 3.

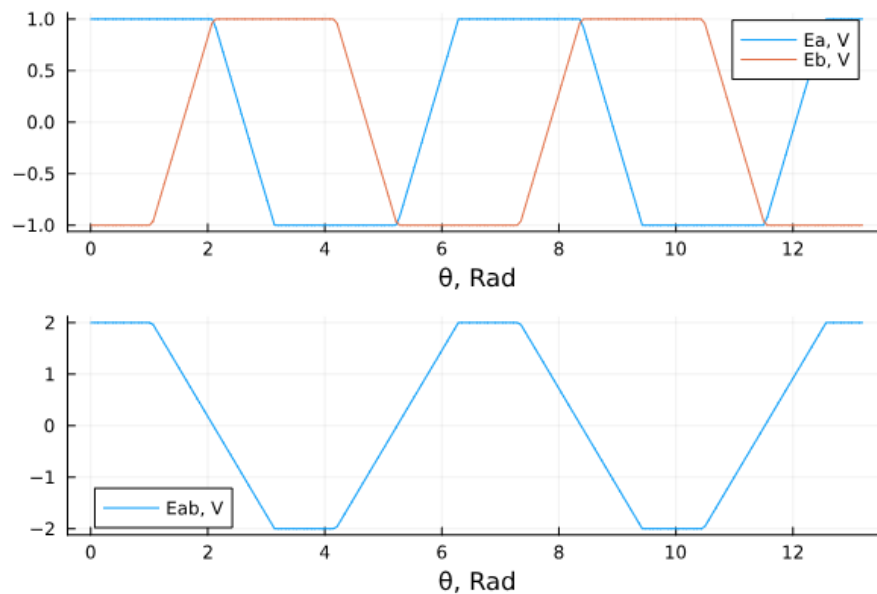


Fig. 3. BLDC motor line-to-line Back EMF voltage

In the classic motor design, the trapezoidal shape of the BEMF is determined by different coil connections and air gap distances. This winding configuration requires fewer windings compared to synchronous motors with a sinusoidal BEMF shape (PMSM motors) and, accordingly, BLDCs have a lower cost.

Real BLDC motors can have BEMF shape different from trapezoidal. It is smoother due to construction features and the influence of the stator resistance and inductance during rotor rotation. Example of BEMF shape of real motors is shown in fig. 4.

Some BLDC motors have BEMF close to sinusoidal shape; it makes them relatively close to PMSM motors. So, it is possible to use advanced control techniques developed for PMSM motors to control BLDC. In many cases, due to winding configuration or decreasing cost of the motor, its BEMF shape has significant differences from trapezoidal and sinusoidal.

BLDC motor simulation [3] shows that difference between the BEMF shape of the motor and shape of the stator voltage plays a significant role in forming motor currents under the load modes and reduces efficiency of the system. So, it is necessary to consider the BEMF shape in choosing the best control method for a given BLDC motor.

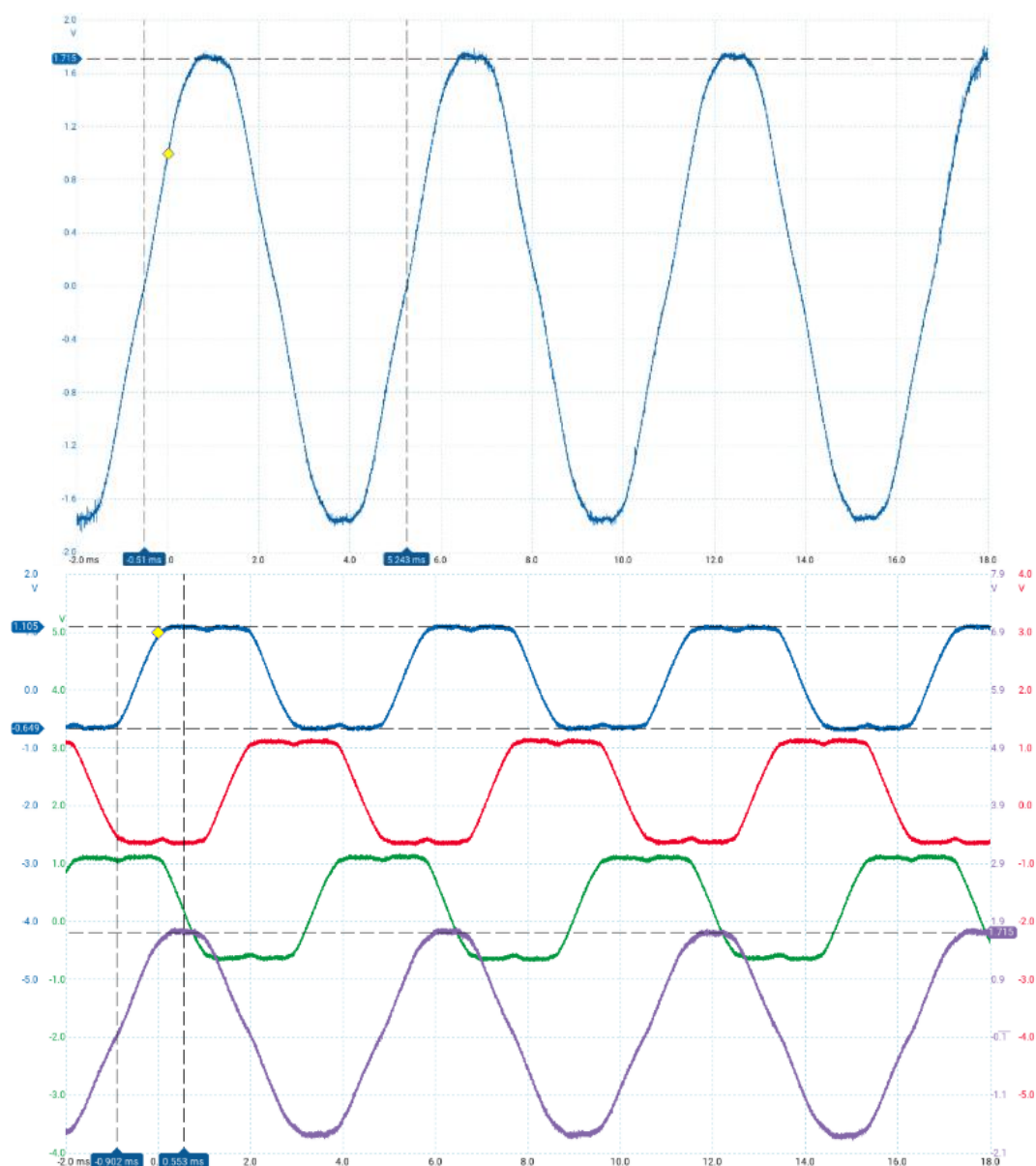


Fig. 4. Experimental Back EMF shapes of BLDC motors

Some BLDC motors have BEMF close to sinusoidal shape; it makes them relatively close to PMSM motors. So, it is possible to use advanced control techniques developed for PMSM motors to control BLDC. In many cases, due to winding configuration or decreasing cost of the motor, its BEMF shape has significant differences from trapezoidal and sinusoidal.

BLDC motor simulation [3] shows that difference between the BEMF shape of the motor and shape of the stator voltage plays a significant role in forming motor currents under the load modes and reduces efficiency of the system. So, it is necessary to consider the BEMF shape in choosing the best control method for a given BLDC motor.

The aim of the article is to analyse generally used and latest methods of BLDC motor control to use these approaches in combine with developing prediction control system of the BLDC motor. Control methods analysed from point of stator voltage shapes passed to the motor from the power converter; methods of synchronisation with the rotor position and motor speed control techniques.

1. Power converter switching

To control the voltage and current in the windings of brushless DC motors, switching semiconductor electronic devices are generally used. The most common and universal power converter circuit

for controlling BLDC motors is a three-phase bridge autonomous voltage inverter, the structure of which is shown in fig. 5.

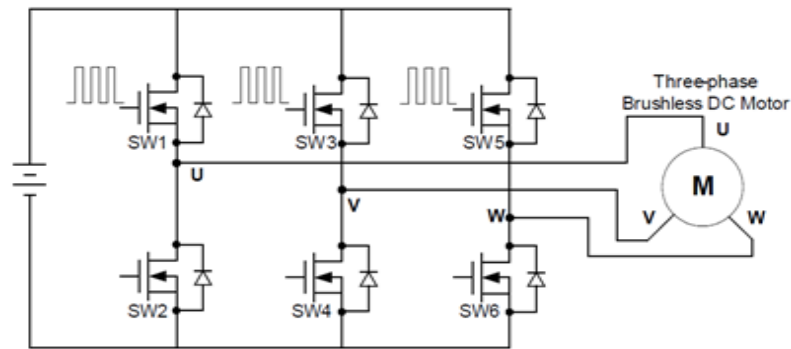


Fig. 5. Simplified circuit of 3-phase power inverter for BLDC motor control

The inverter circuit [4] uses fully controlled switches: FET or IGBT transistors that are turned off by the control circuit. Inverter is powered by a DC source.

3-phase inverter converts the DC voltage from a battery or a rectifier with a storage capacitor into a three-phase AC voltage with a sinusoidal or rectangular or other frequency-variable shape.

The main approaches to generate voltage for BLDC control motors are:

- autonomous voltage inverter in amplitude control
- 6-step commutation;
- sinusoidal 3-phase PWM;
- space Vector PWM;
- hysteresis control (relay switching).

First three techniques generate different variations of rectangular AC voltage shape. They are used for simple and fast control applications such as fans, quadcopter motors and drones, where the motors have close to trapezoidal BEMF shape. In general, it is used to simplify control system and when exact BLDC motors.

In advanced control systems which use SVPWM inverter control it is possible to adopt output voltage to BEMF shape of the motor. Such systems will be reviewed later in the article. These methods are reviewed in the next section.

2. Voltage shapes for motor control

2.1. Autonomous voltage inverter in amplitude control

This technique is classic form of the 3-phase inverter control and can be used to drive BLDC motor. The output voltage period is divided into six intervals. Each of the switches in the half-bridge is turned on for half the output frequency period. The diagrams of the operation of an autonomous voltage inverter in amplitude control mode are shown in fig. 6.

The linear voltage has a rectangular shape, its half-wave duration, the amplitude is full DC-link voltage. But the effective value of line-to-line voltage is 0.816 of DC-link voltage [4]. But such shape of stator voltage does not correspond to motor BEMF shape and simulation shows that motor currents lead to sufficient pulsations in the motor torque in steady state modes. Dependency of motor torque from 3-phase currents was simulated used setup from [3] and shown in fig. 7.

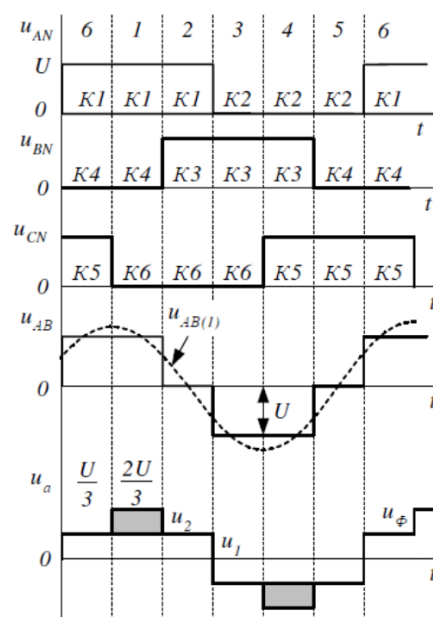


Fig. 6. Three-phase inverter operation with amplitude control

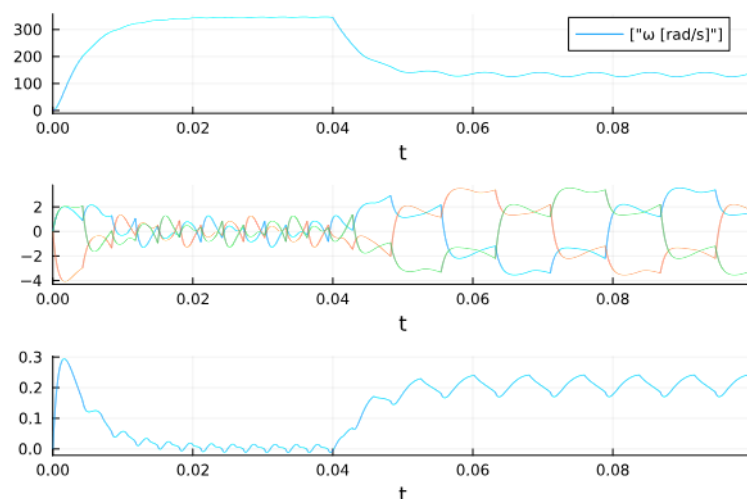


Fig. 7. Motor torque ripple

This sufficient disadvantage of simple amplitude control leads to the current and torque oscillations which cause speed disturbances. This control type is rarely used in practical applications.

2.2. 6-step commutation

This mode also known as 2-phase current injection. Trapezoidal commutation (also known as 6-Step commutation) follows the principle that current should flow in only two of the three phases at the same time. According to this method, a pulse with a width of 120 electrical degrees is applied to 2 phases of the motor and the third phase remains disconnected from the voltage source. This means that at the same moment one phase of the motor is connected to positive voltage, another phase is connected to 0 (GND) and third phase is left floating. All this three state generates by inverter half-bridges. Fig. 8 shows the control signals for inverter gates and output voltage at the one half-bridge (phase of inverter). Floating state (Hi-Z) it shown as half oh DC-link voltage. Separate control of the half-bridge keys required to create floating state – in this mode both FETs should be turned off (low level at the gate).

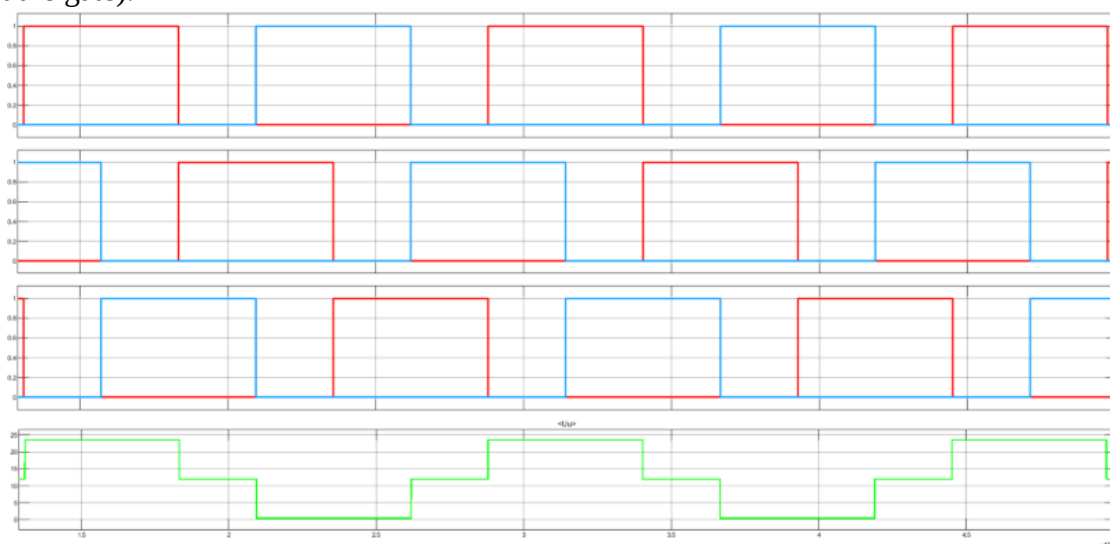


Fig. 8. 6-step commutation control signals

To change the voltage on the motor, PWM is used at the half-bridge inverter, which generates a positive voltage. The operation diagram is shown in fig. 9.

When a BLDC motor connected to inverter, the shape of the voltages at the inverter output changes because the rotating motor is a source of BEMF. At times when a phase remains disconnected from the voltage source, there is a back EMF of the motor phase on it.

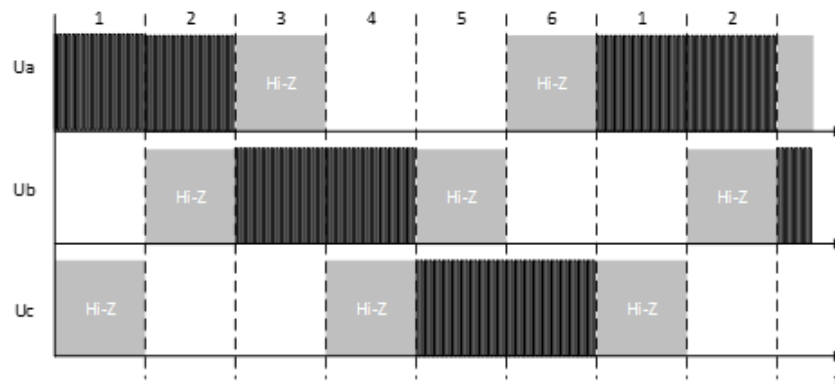


Fig. 9. Motor phase voltages in 6-step commutation mode with PWM voltage control

Motor phase and line-to-line voltages and motor current shown in fig. 10.

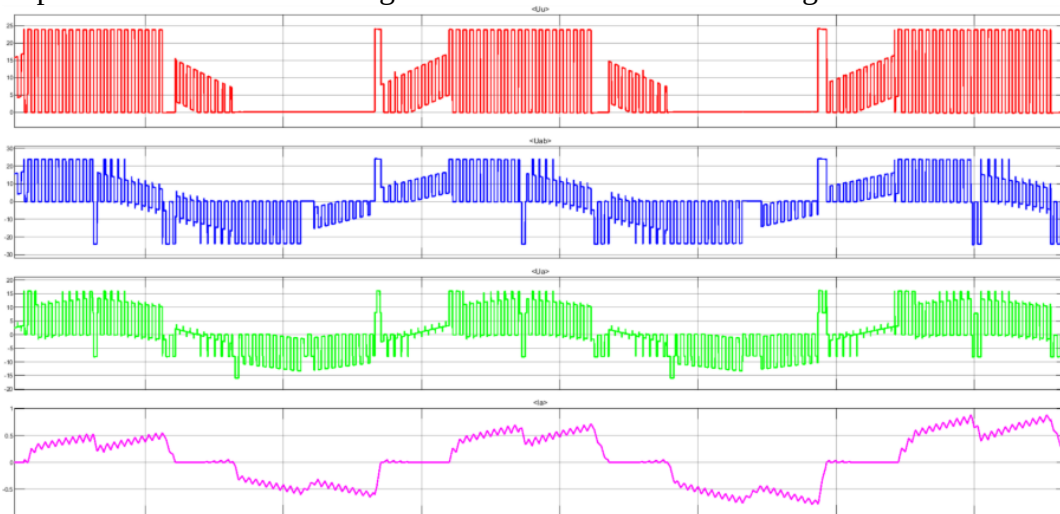


Fig. 10. Voltage and current diagrams of a BLDC motor with 6-step commutation

In this mode motor currents flows only through 2 phases, and this derives mostly linear shape of current and motor torque. One of the advantages of this technique – possibility to measure motor BEMF in real time at the phase which is left in Hi-Z state (floating).

Also, the shape of phase voltage is much closer to trapezoidal motor BEMF, and this mode delivers the minimal average torque required to rotate the load.

6-step commutation required synchronisation between inverter voltage and BEMF of the motor. The BEMF value should be synchronised with moments of current injection as shown in fig. 11.

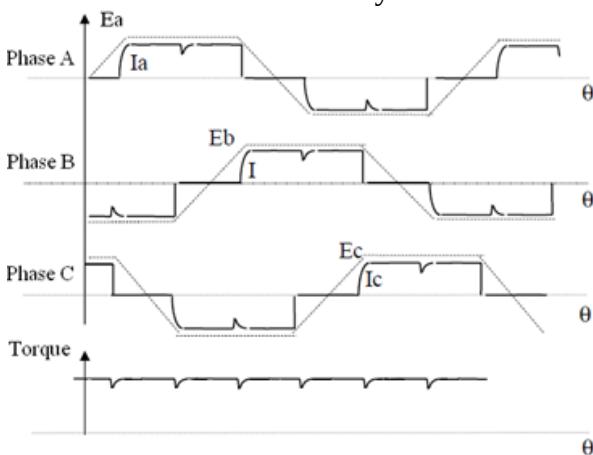


Fig. 11. BEMF and currents synchronization during 6-step commutation

The synchronisation techniques considered in more detail in the next section of article.

Disadvantage of this 6-step method is in sufficient torque cogging, when current switched from one phase to another. The torque and its ripples shown at bottom axis of fig. 11. At high loads also leads to sufficient commutation disturbances which can decrease EMI parameters of the system.

Also exists 12-step commutation methods that allow to form more than 6 output states which corresponds to more positions of the field flux vector. They are usually used to increase motor rotation performance at the low speeds.

2.3. Sinusoidal 3-phase PWM (SPWM technique)

If the BLDC motor has a back EMF shape close to a sinusoidal one, the 6-step mode can be used for commutation, but in this case the next problems appear:

- torque consists of a fragment of a sine wave and is a combination of the trapezoidal current strategy and sinusoidal back EMF;
- the torque value is smaller.

In this case, the 3-phase sinusoidal voltage at the inverter output is used and the motor will create a constant torque without ripples.

The most common for analogue and digital control systems is the method of formation based on reference signals [4] and the tabular method of

voltage formation. These methods to control an autonomous voltage inverter to generate sine voltage have been significantly studied and have been used for a significant number of years, and therefore they will not be considered in detail in this review.

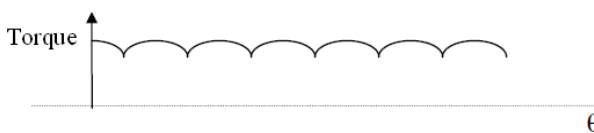


Fig. 12. Torque ripple in a sinusoidal motor controlled as BLDC

2.4. Space vector PWM (SVPWM)

This method of the 3-phase voltage generation allows to orient the instantaneous value of the voltage vector and its rotational speed in accordance with the required voltage frequency and magnitude in real time.

For the circuit of an autonomous voltage inverter (Fig. 5), there are eight possible discrete states of the power switches, and the output voltages of the inverter can be composed of these eight switch states.

The given voltage vector is formed during the PWM period from three consecutive states among which it is located at a given moment of time.

The diagram of the operation of this algorithm [5] is shown in fig. 13.

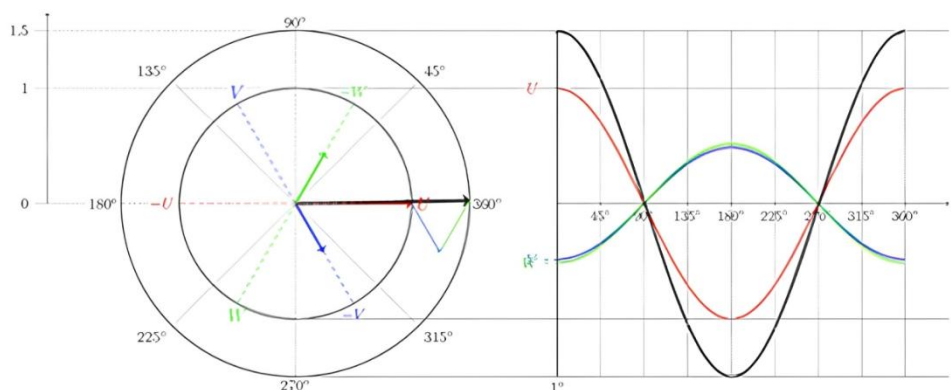


Fig. 13. Visualization of Space vector PWM generation

The advantages of this method are:

- fast control of the voltage vector, and thereby changing set the amplitude and frequency in real time;
- the ability to generate a constant voltage on the stator with any orientation
- easy integration into the motor vector control system
- possible to create non-sine voltage and adopt it to BEMF voltage shape of the motor

The disadvantages are relatively high requirements for the computing system and not full use of the inverter DC-link voltage. But the second disadvantage is neglecting by the compensation method by adding the third harmonic.

3. Rotor position measurement

While BLDC are synchronous AC motors, it is always necessary to adjust the position of the rotor with the voltages generated by the inverter, i.e. to sync control voltages with actual motor BEMF.

Therefore, information about the current position of the rotor is required.

Depends on the source of data about the rotor position, control methods and systems are divided into sensors position measurement and sensorless.

3.1. Hall-sensors control

Since most BLDC motors have a trapezoidal back EMF and the voltage waveform in these cases requires rectangular control signals, the most common position sensors are Hall effect sensors. The sensors are installed on the stationary stator of the motor and output a logic signal about the position opposite the south or north pole of the rotor magnet. For a three-phase BLDC motor, three Hall sensors are required to determine the rotor position.

Depends on the physical location of the Hall sensors on the stator, there are two types of sensor positioning: 60° phase shift and 120° phase shift. The combination of signals from the 3 sensors determines the exact sequence of commutation signals.

Fig. 14 shows the connection between Hall-sensors signals and motor BEMF for BLDC motor. Based on it the switching sequence for 3-phase inverter can be created. If 6-step commutation is used it is necessary to align current injection periods with BEMF which can be calculated from Hall sensor signals as shown in fig. 15 and in [2].

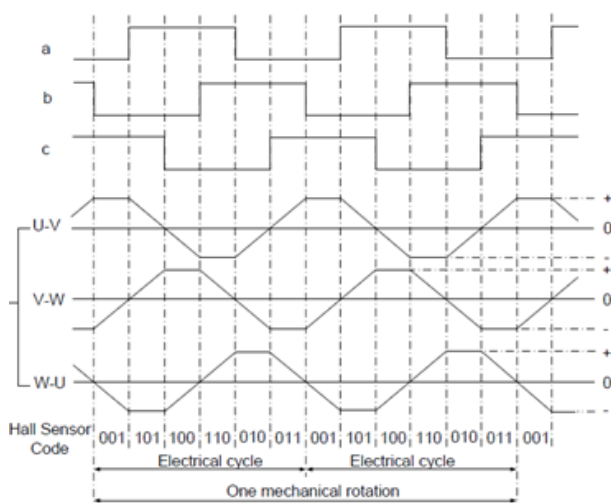


Fig. 14. Correlation of Hall sensor signals and BEMF signals

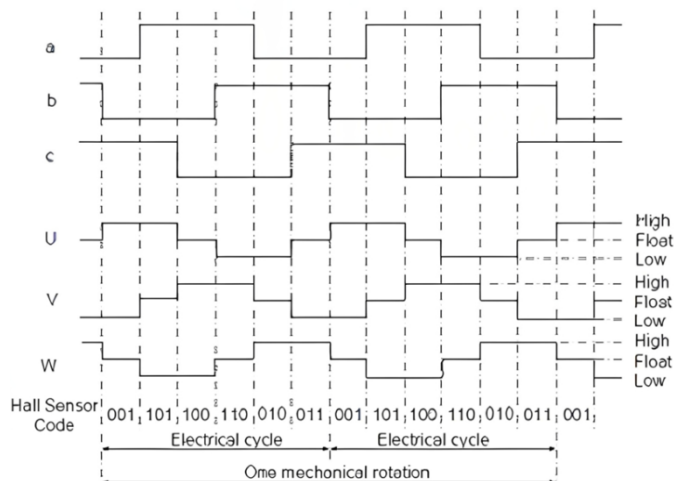


Fig. 15. Timing diagram of motor commutation using Hall sensors

For each 60° rotation angle, one of the Hall sensors changes its state. Six steps are required to complete a full electrical cycle. When the motor is running, the phase current switching is updated every 60° . For each step, one motor terminal is switched high, the other low, and the third remains floating (6-step commutation). Fig. 16 shows the block diagram of the motor control with Hall sensors and location correction system.

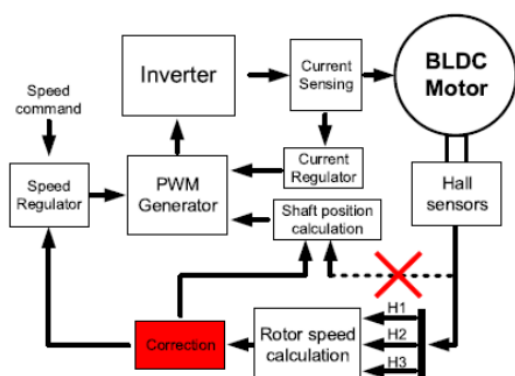


Fig. 16. Block diagram of the motor control with Hall sensors and location correction system

Controlling motors with Hall sensors provides high-quality motor control over the entire speed range and requires a simple, inexpensive control system that can be implemented without the use of a microprocessor.

However, when using cheap mass-produced motors, there is an error in the location of the Hall sensors. Signals from incorrectly shifted sensors lead to asymmetric operation of the inverter, which in turn leads to electromagnetic torque pulsation, an increase in the amplitude of the motor current and acoustic noise [6]. A higher current amplitude increases electrical losses, as well as electromagnetic interference, in addition to forcing manufacturers to use inverter transistors with a higher nominal current.

In [6] was proposed to correct the switching points based on the difference in the periods of the sensor output signal during motor rotation.

3.2. BLDC motor control w/o sensors

Hall sensors cannot be used in systems where the rotor is in a closed housing and requires minimal electrical inputs, or the system is designed to be as cheap as possible.

To obtain information about the rotor position, the following can be used:

- motor BEMF signals;
- rotor position estimation from motor current and voltage signals.

3.2.1. BEMF zero crossing measurement

When using back-EMF signals, the control system monitors the BEMF signals instead of the position determined by the Hall sensors [2] for signal switching. The relationship between the sensor output and the BEMF was 14 shown is used.

Common method for BLDC motor control w/o sensors is BEMF zero-crossing detection. As sensors are commonly used electronic comparators – to detect moment of BEMF zero cross. The sensor signal changes state when the polarity of the BEMF voltage changes from positive to negative or from negative to positive. The BEMF zero crossing provides accurate position data for switching.

Sensorless commutation significantly simplifies the design of the motor and its cost. The disadvantage of the system is that since BEMF is proportional to the speed of rotation, at low speeds the signal value is minimal and cannot be used for commutation. In such cases, the motor is forcibly accelerated to the minimum operating speed by forced rotation of the stator field, and the starting currents of the motor are increased even without load.

3.2.2. Rotor position estimation

With development computing power of motor controllers sensorless rotor position estimation became basic. In general, these techniques of estimation of the rotor position based on measurement motor currents and voltages (optionally) and calculation of actual rotor angle in real time. Basic block diagram of control system with motor angle observer given in [8] and shown in fig. 17.

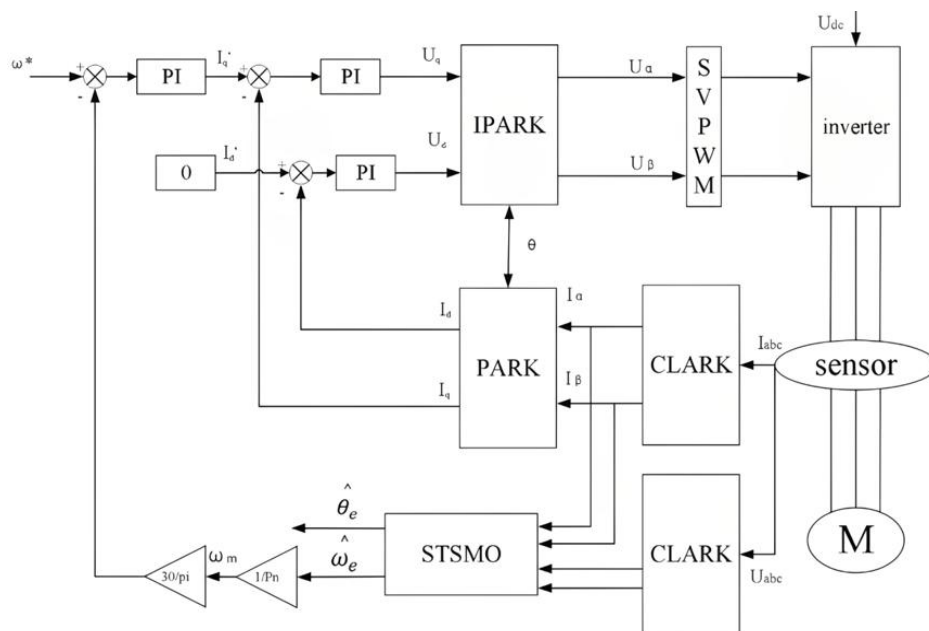


Fig. 17. Block diagram of the motor control with Hall sensors and location correction system

Control system uses information about angle, derived from observer for function of Park transformations, speed calculation, torque calculation and for calculation of SVPWM which is used in given control system to form 3-phase motor voltage.

Review and comparison of common techniques of BLDC angle estimation is given in [7]. The most common methods of motor angle estimation are: Flux linkage observers; BEMF observers; Sliding mode observers (SMO); Super-twisting SMO (ST SMO); Extended Kalman Filters (EKF);

Luenberger observers; Frequency-adaptive observers; Machine-parameters adaptive observers; PLL based angle observers.

Flux linkage observers are most simple from computational recourses and used for high-speed applications. They estimate rotor flux linkage using stator voltage and current measurements and don't include differential parts in model. However, they are sensitive to motor parameters accuracy and load conditions.

BEMF angle observers are Nonlinear-model-based observers and effective at medium and high speeds [7]. They estimate rotor position using BEMF induced in the stator windings, which directly correlates with rotor flux. Observer structure estimates the BEMF, which is then used to derive rotor angle with arctangent function. To improve range of speeds for BEMF observers one considered motor coils parameters (resistance and inductances) and calculates BEMF based on motor electrical model.

More robust solution is Sliding Mode Observer (SMO) - nonlinear state observer based on the principles of sliding mode control (SMC), designed to reconstruct unmeasured system states by enforcing a sliding condition on the estimation error dynamics. Common block diagram of the sliding mode observer shown in fig. 18.

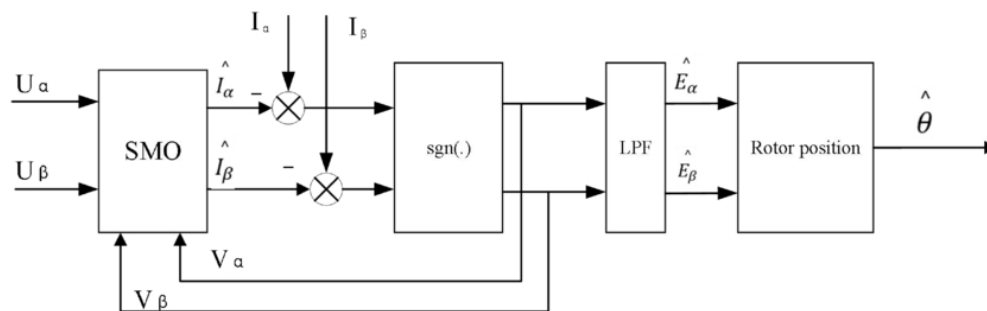


Fig. 18. Block diagram of Sliding Mode Observer

SMO is using internal simple motor model and compares its output signal with measured signal to create sliding condition. Mostly all simple observers are computationally efficient but fail at low speeds due to the diminishing back-EMF amplitude, which compromises observability. Open-loop I-f control is typically used for startup. To enlarge speed range are used more advanced estimations but with high computational complexity.

4. Motor speed control

Motor control systems mainly maintain speed because most applications require constant velocity under varying loads. Speed control ensures stable operation, energy efficiency, and process reliability, while torque control serves as a lower-level mechanism that supports speed regulation. In most industrial, automotive, and robotic applications, the output variable of interest is mechanical speed rather than torque or current. A review of various speed control methods is provided, including PID controllers, adaptive control, fuzzy systems, and others. The advantages and limitations of each method are investigated. As a result, an overview of the current state of research in this area is provided for further study of the prospects for the development and implementation of new BLDC motor speed control systems.

4.1. PID controller-based automatic control system

Proportional-integral control systems are the most widely used speed control technique for BLDC and all other types of motors. It can be easily implemented on analogue and digital components because it is well understood, simple and has been used in practice for a long time. Improving performance or reducing cost has been the subject of development for a long time.

The block diagram of a PID controller [9] is shown in fig. 19.

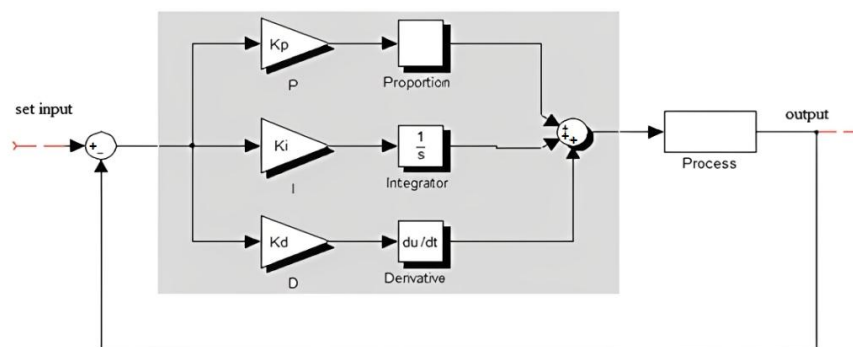


Fig. 19. Structure of the PID controller

Control systems using the PID controller are well studied and in the scientific community there is a huge amount of scientific research in this area, therefore, from the standpoint of scientific innovation, research in this area is not promising. But PID controllers are widespread as a component of more effective BLDC motor control systems.

For speed control of BLDC motors, the most common is the classic speed and current PI control in which the speed controller generates tasks for the motor current PI-controller (fig.20).

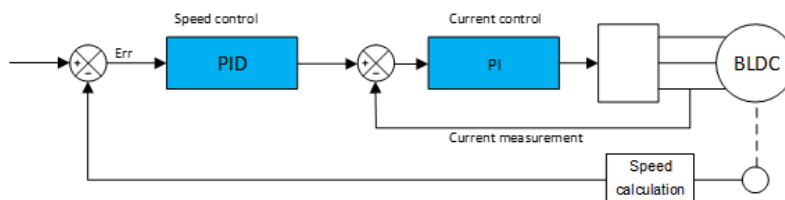


Fig. 20. 2-loop speed control system of a BLDC motor

The current regulator compensates the electrical component of the motor circuit and provides support for the motor torque, and the speed regulator compensates the mechanical component of the motor rotation with feedback.

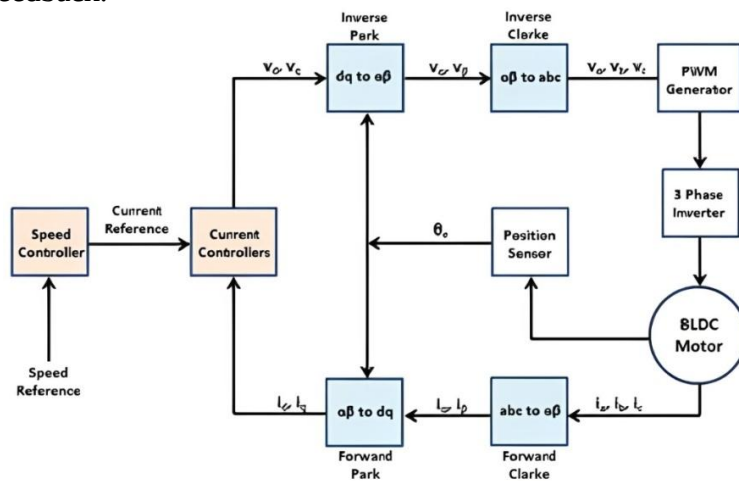


Fig. 21. Block diagram of BLDC vector control system

The current controller can be replaced by a hysteresis (relay) regulator, which increases the accuracy of current support and system dynamics, but may require high switching frequencies when working with low-power motors or high-speed motors.

The algorithm of a conventional PID regulator is simple, stable, easy to calculate parameters when the exact mathematical model of the system in differential equations is known. The disadvantage of implementing the system is that most industrial processes with varying degrees of nonlinearity, parameter variability and uncertainty of the mathematical model of the system. Setting the parameters of PID regulation is very complicated, so it is difficult to achieve stable regulation in field conditions and in actual production. Therefore, with the increase in the computing power of microprocessor systems and the emergence of high-speed parallel processing systems, classical PID control systems are replaced with more advanced control systems.

4.2. Field oriented control (FOC)

The most common control method for sensorless speed maintain of BLDC motors is 6-step trapezoidal control, which was described above. Although this method is easy to implement, it has several disadvantages, such as large torque ripple, high speed limitations, requirements for precise sensor positioning, speed ranges, and high noise levels.

The Field Oriented Control (FOC) methodology overcomes these limitations while providing increased efficiency by maximizing torque per unit current [11]. Accurate measurement of the rotor angular position is essential for the FOC algorithm and can be implemented in two ways. The first method is to use sensors, such as Hall effect sensors, to determine the rotor position, known as sensor-based FOC. This approach provides higher measurement accuracy, but is generally undesirable due to cost, installation issues, and limited application ranges. The second method, sensorless FOC, involves estimating the rotor position using state observers mentioned in 3.2.2 section. In this method, rotor position is estimated by measuring instantaneous motor parameters such as voltage and current and then mathematically calculating the rotor position vector. This eliminates the need for physical position sensors and requires only the use of motor current sensors, thus reducing cost and increasing reliability, albeit at lower levels of accuracy.

The principle of operation of the FOC algorithm is as follows. The three-phase power supply of the motor creates a rotating magnetic field of the stator. The permanent magnets in the rotor try to align themselves along this field, which leads to continuous rotation. The maximum torque is created when the fields are perpendicular. The FOC algorithm achieves this condition by dividing the stator field into two perpendicular components and then driving the component along the rotor field (without torque) to zero. The axes along and perpendicular to the rotor field are called the direct (d) and quadrature (q) axes, respectively. The adjustment of the stator field components is carried out using PID controllers that maintain the corresponding d and q components of the motor current.

Maintenance of reference speed is implemented by a speed PID controller that generates the motor torque command and affects the perpendicular component of the stator field.

Advantages of the method are [12] increased accuracy of maintaining speed in steady-state operation, minimal level of motor torque pulsations, low energy consumption. This method in combination with SVPWM allows to calculate instantaneous values of the motor voltage and adopts inverter output voltage to actual BEMF shape of the motor.

Disadvantages of this type of control include slow response to changes in load torque or set speed; relatively high computational cost of the algorithm; sensitivity to motor parameters used to calculate PID controllers of the FOC system.

4.3. Direct torque control (DTC)

The basic idea of Direct Torque Control (DTC) [13] is to select the appropriate stator voltage vector from eight possible inverter states to ensure that the stator flux linkage vector rotates as it produces the desired torque.

- Motor torque – using a torque observer based on phase current data;
- Rotor position – using Hall sensors or using a rotor position observer.

Depends on the rotor position and the ratio of the reference and measured torque - the inverter voltage vector is selected, which increases or decreases the torque in the set direction (fig. 22).

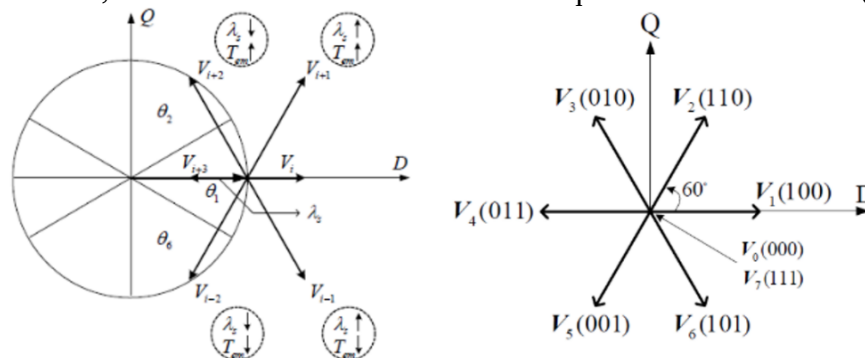


Fig. 22. Calculation of the inverter voltage vector depending on the current rotor position from 8 possible states

For this selection, a simple hysteresis switch is used as shown in the block diagram in fig. 23.

The advantages of this methodology are high accuracy of motor torque support, high dynamics of speed control and especially high speed of motor torque generation, which is limited only by the electrical motor constant.

Disadvantages are high computational complexity of the algorithm in sensorless control, requirement for small sampling times, reduced stability of speed support in sensorless motor control.

To improve the performance of sensorless torque measurement, a complex observer of motor parameters based on Sliding Mode Control (SMC) was proposed in [14]. In control systems, Sliding Mode is a nonlinear control method that changes the dynamics of a nonlinear system by applying an intermittent control signal (or, more precisely, a setpoint control signal), which causes the system to “slide” along the cross section of the normal behaviour of the system. The proposed Sliding Mode observer allows you to obtain the values of torque and speed simultaneously.

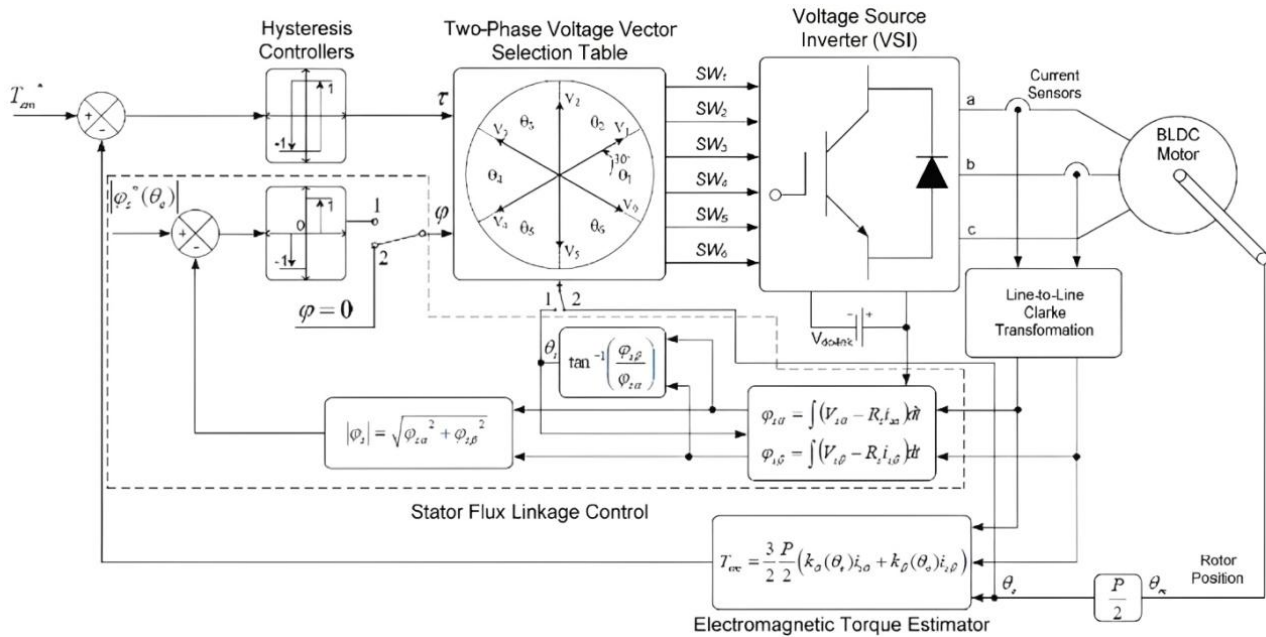


Fig. 23. DTC block diagram

To compensate for the shortcomings of DTC and FOC systems, a hybrid control system was proposed in [12] that combines the advantages of both systems. It uses an algorithm switch depending on the speed error as shown in fig.24.

4.3. Fuzzy logic controllers

In the applications of BLDC motor control, fuzzy logic systems are effectively used, while they have advantages in terms of calculation speed.

In the article [15], an adaptive control system with a fuzzy logic controller is proposed. The block diagram of the system is shown in fig. 25. The approach of combining a PID controller with a fuzzy logic controller is used in [16]. This allows one to improve the quality of regulation and the dynamics of the system by changing the controller coefficients in real time.

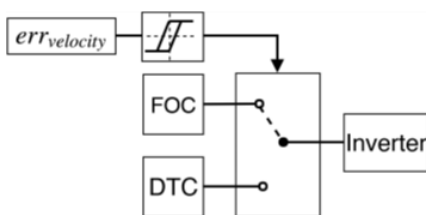


Fig. 24. Block diagram of a hybrid control system using DTC-FOC

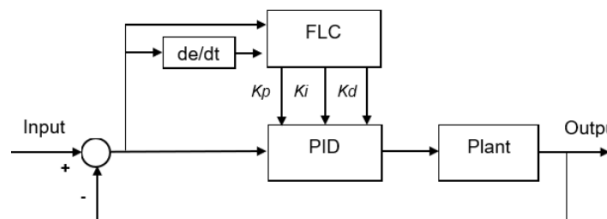


Fig. 25. Adaptive control system based on PID regulator with fuzzy logic controller

4.4. Model prediction control (MPC)

Predictive control or Model Predictive Control is one of the modern methods of dynamic systems control theory, based on prior knowledge of the dynamic characteristics of processes. The controller relies on an empirical model of the controlled process to predict its further behaviour, based on the previous values of state variables. With the increase in the computing power of microcontrollers, it becomes possible to apply predictive control methods for BLDC motors [17]. In addition to improving the parameters of the classical speed control structure (fig. 19), these systems allow direct control of the motor power and the use of the most economical motor operation mode by reducing reactive power to 0. The system structure of the BLDC predictive control system with power control is shown in fig. 25 and fig. 26.

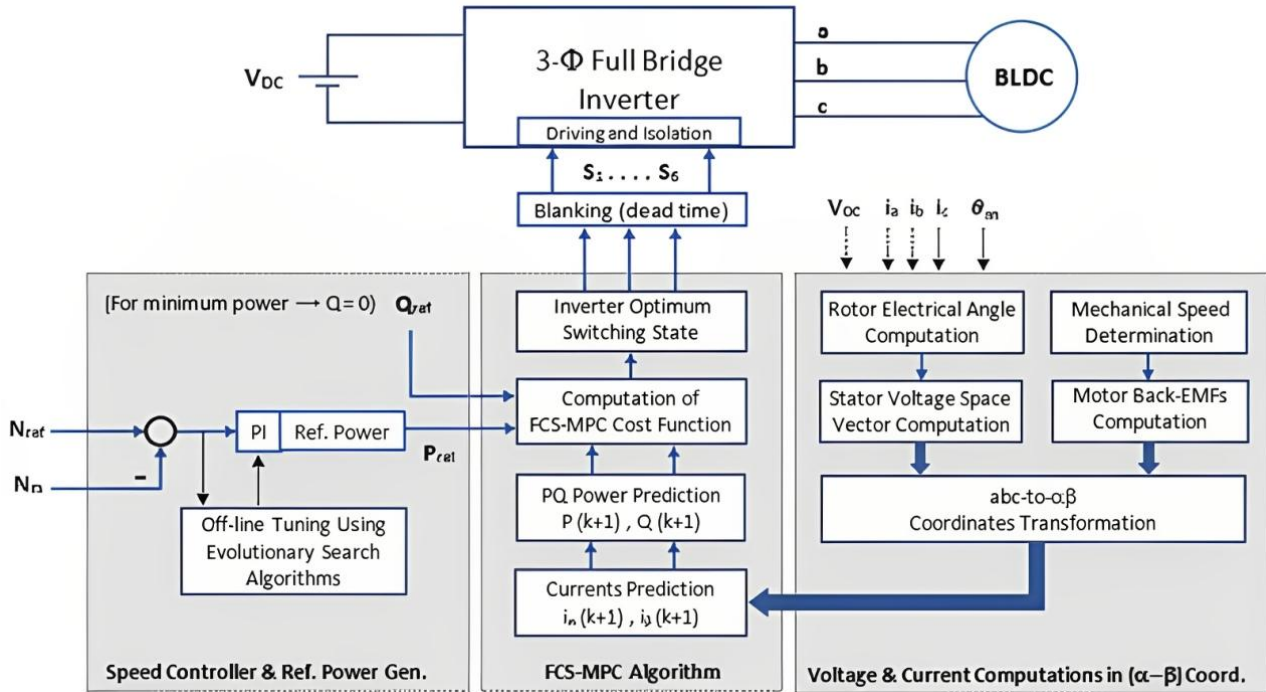


Fig. 25. Structure of a predictive control system with active power regulation

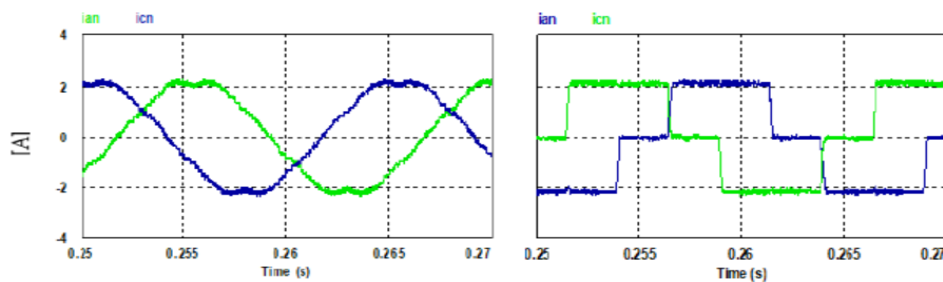


Fig. 26. Comparison of motor currents with reactive power reduction and current control

The disadvantage of the methodology is the significant computational cost and, accordingly, the limitation on maximum motor speeds

4.5. Adaptive control systems

With the development of the computing power of microcontrollers, so-called adaptive BLDC control methods are being introduced that can adapt to change the system according to unknown motor parameters or changing load parameters. Adaptive control methods for BLDC motors usually include complex algorithms and feedback mechanisms that constantly monitor the behaviour of the motor and adjust the control signals accordingly. These methods can use various sensors, such as Hall effect sensors or encoders, to provide feedback on the rotor position, speed and other relevant variables.

The control algorithms then use this feedback information to optimize the motor operation in real time, ensuring optimal performance under different conditions.

In [18], an adaptive controller is proposed that is used to compensate for the non-ideal shape of the BEMF of the motor, thereby improving the quality of speed regulation and minimizing losses during motor operation.

Adaptive systems allow to adjust the power consumed from the electrical network by jointly controlling the inverter for driving the BLDC motor and the power factor corrector [19].

4.6. Deep learning in BLDC motor control

With the creation of machine learning systems capable of working as part of embedded systems, it has become possible to use these flexible innovative algorithms for motor control.

When controlling the speed of a motor, a neural network can be used as a controller that includes all the functions of the control system and includes forward and inverse mathematical models of the system (just as a PID controller is an inverse function for the controlled system) [20]. The structure of such a system is given in fig. 27.

In addition to direct speed control, the neural network allows to implement optimization algorithms depending on the load and motor parameters changing. Also, in control systems, ANFIS (Adaptive Neuro Fuzzy Interference System) systems are used, which are a combination of neural networks and fuzzy logic systems [21, 22].

An ANFIS controller is a neural model that operates on fuzzy logic values and adjusts itself through training. An example of such an adaptive controller [21] for motor speed control is given in fig. 28.

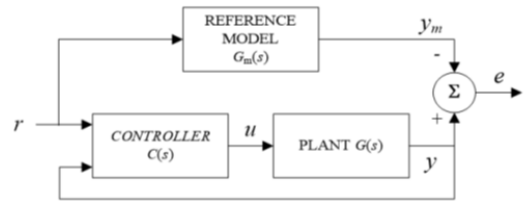


Fig. 27. Using ANN for motor speed control

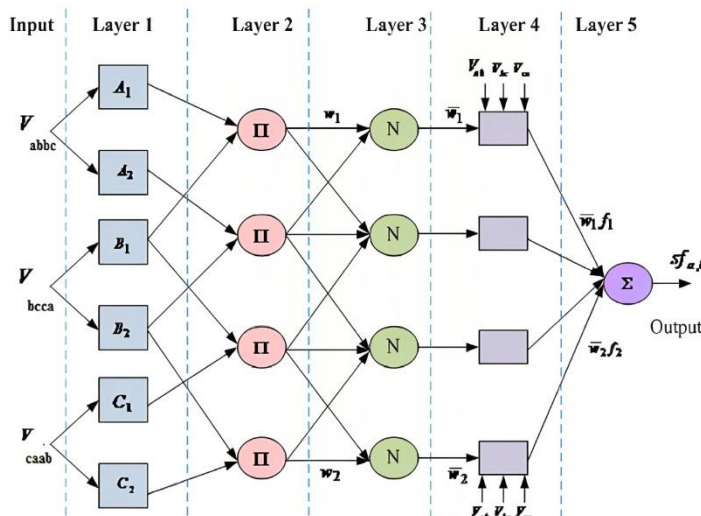


Fig. 28. ANFIS controller architecture for BLDC motor control

The main areas of application of neural networks in the field of BLDC control are:

- adjusting the motor speed depending on the load conditions, temperature and other;
- artificial neural networks (ANNs) can estimate the position and speed of the rotor without using physical sensors;
- improving the accuracy of back EMF estimation;
- adaptive controllers, reinforcement learning and fuzzy logic can improve the performance of speed control;
- optimizing the efficiency of the control system and extending the battery life;
- motor fault prediction, fault detection and diagnosis.

The disadvantages of the systems are high computational complexity and lack of training examples for training the network to handle dynamic operating modes. But using logic or FPGA based systems, where much easily to implement NN structures it is possible to create efficient and cheap BLDC motor control system.

Conclusions

Modern research focuses on the development of sensorless control methods, energy consumption optimization, enhancement of fault prediction algorithms, and improvement of the overall adaptability of systems to varying operating conditions. These directions play a key role in the advancement of electromobility and automated technologies, contributing to the creation of more efficient, reliable, and resilient electric drives.

References:

1. Visconti P., Primiceri P. An overview on state-of-art and future application fields of BLDC motors: design and characterization of a PC-interfaced driving and motion control system // *ARNP Journal of Engineering and Applied Sciences*. 2017. Vol. 12, No. 17. P. 4913–4926.
2. Zhao J., Yu Y. Brushless DC Motor Fundamentals // *Monolithic Power Systems*. Application Note AN047 Rev. 1.0. 2014.
3. Trofimov P., Sokol E. BLDC motor simulation model with configurable BEMF in Julia // *Bulletin of the National Technical University “KhPI”*. Series: New solutions in modern technology. 2025. No 1(23). P. 62–69. <https://doi.org/10.20998/2413-4295.2025.01.08>
4. Шавьолкін О. О. Енергетична електроніка : навч. посіб. Київ : КНУТД, 2017. 396 с.
5. Solbakken Y. SPACE VECTOR PWM INTRO // Internet resource. 2017. <https://www.switchcraft.org/learning/2017/3/15/space-vector-pwm-intro>
6. Kolano K. Improved Sensor Control Method for BLDC Motors // *IEEE Access*. 2019. Vol. 7. P. 186158–186166. <https://doi.org/10.1109/ACCESS.2019.2960580>
7. Saha B., Sen A., Singh B., Mahtani K., Sánchez-Fernández J. A. Quadrature-Phase-Locked-Loop-Based Back-Electromotive Force Observer for Sensorless Brushless DC Motor Drive Control in Solar-Powered Electric Vehicles // *Appl. Sci*. 2025. Vol. 15, No 2. P. 574. <https://doi.org/10.3390/app15020574>
8. Wen H., Yao X. Sensorless control of BLDCM based on STSMO // *Proc. SPIE*. 2024. Vol. 13445. P. 1344507. <https://doi.org/10.1117/12.3054414>
9. Patel V. K. R. S., Pandey A. K. Modeling and Performance Analysis of PID Controlled BLDC Motor and Different Schemes of PWM Controlled BLDC Motor // *International Journal of Scientific and Research Publications*. 2013. Vol. 3, Issue 4. P. 1–12.
10. Rajinith S., Abeykoon C., Maithripala D. H. S. Design of a Sensorless Field Oriented Control Drive for Brushless DC Motors // *Proc. 9th Int. Conf. Control, Dynamic Systems, and Robotics (CDSR 2022)*. Niagara Falls, Canada, 2022. P. 1–9. <https://doi.org/10.11159/cdsr22.180>
11. Carey K. D., Zimmerman N., Ababei C. Hybrid field oriented and direct torque control for sensorless BLDC motors used in aerial drones // *IET Power Electron*. 2019. Vol. 12, No 3. P. 438–449. <https://doi.org/10.1049/iet-pel.2018.5231>
12. Ozturk S. B. Direct Torque Control of Permanent Magnet Synchronous Motors with Non-Sinusoidal Back-EMF. Istanbul Technical University ; Texas A&M University, 2008.
13. Ghule A. B., Sankeshwari S. S. Sliding Mode Observer for Torque Control in Sensorless BLDC Motor // *IOSR J. Electr. Electron. Eng*. 2015. Vol. 10, Issue 5, Ver. I. P. 16–20. <https://doi.org/10.9790/1676-10511620>
14. Praptodiyono S., Maghfiroh H., Hermanu C. BLDC Motor Control Optimization Using Optimal Adaptive PI Algorithm // *J. Elektronika dan Telekomunikasi*. 2020. Vol. 20, No 2. P. 47–52. <https://doi.org/10.14203/jet.v20.47-52>
15. Rehman A., Kumar Singh A. Mamdani and Sugeno Fuzzy Logic Approach of PID Controller // *Int. J. Res. Appl. Sci. Eng. Technol*. 2022. Vol. 10, Issue V. <https://doi.org/10.22214/ijraset.2022.43542>
16. Azab M. Comparative Study of BLDC Motor Drives with Different Approaches: FCS-Model Predictive Control and Hysteresis Current Control // *World Electr. Veh. J*. 2022. Vol. 13, No 7. P. 112. <https://doi.org/10.3390/wevj13070112>
17. Adıgüzel F., Türker T. A periodic adaptive controller for the torque loop of variable speed brushless DC motor drives with non-ideal back-electromotive force // *Automatika*. 2022. Vol. 63, No 4. P. 732–744. <https://doi.org/10.1080/00051144.2022.2065802>
18. Praveen Kumar L., Sreepal Reddy K. Adaptive Variable Speed Control Scheme for Wind Based on PFC of BLDC Drive Applications // *Int. J. Mod. Trends Sci. Technol*. 2016. Vol. 2, No 9. P. 142–148. <https://doi.org/10.29126/ijmtst.2.9.142>
19. Utomo D. S. B., Rizal A., Fanany A., Gaffar O. Model Reference Neural Adaptive Control Based BLDC Motor Speed Control // *Academia.edu*. 2019. P. 1–6. <https://doi.org/10.13140/RG.2.2.36694.73283>
20. Hemalatha N., Venkatesan S., Kannan R. Sensorless speed and position control of permanent magnet BLDC motor using particle swarm optimization and ANFIS // *Measurement: Sensors*. 2024. Vol. 31. P. 100960. <https://doi.org/10.1016/j.measen.2023.100960>
21. Mopidevia S., Kiransai D. Design, control and performance comparison of PI and ANFIS controllers for BLDC motor driven electric vehicles // *Measurement: Sensors*. 2024. Vol. 31. P. 101001. <https://doi.org/10.1016/j.measen.2023.101001>
22. Rajinith S., Abeykoon C., Maithripala D. H. S. Design of a Sensorless Field Oriented Control Drive for Brushless DC Motors // *Proc. 9th Int. Conf. Control, Dynamic Systems, and Robotics (CDSR 2022)*. Niagara Falls, Canada, 2022. P. 1–9. <https://doi.org/10.11159/cdsr22.180>

Received 20.10.2025

Відомості про автора:

Трофімов Павло Володимирович – аспірант, Національний технічний університет «Харківський політехнічний інститут», кафедра промислової і біомедичної електроніки; Україна; e-mail: pavlo.trofimov@iee.khpi.edu.ua

SYSTEMS AND METHODS OF INFORMATION PROTECTION
СИСТЕМИ І МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ

UDC 004.056.55

Assessment of the effectiveness of international standards and regulatory acts governing artificial intelligence models for Ukraine / Y.O. Lohachova, M.V. Yesina, D.Yu. Holubnychiy // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2025. № 223. P. 7–17.

The article presents a comprehensive study of the effectiveness of international standards and regulatory acts in the field of artificial intelligence (AI) with the aim of determining the most appropriate model for their implementation in Ukraine. The aim of the work is to conduct a comparative assessment of the leading approaches to AI regulation developed in the EU, the US, Canada, the UK, South Korea, China and other countries, as well as recognised international ISO/IEC standards. The study is based on the comprehensive use of multi-criteria analysis methods: pairwise comparisons, determination of weight coefficients on the Fishburn scale, ranking methods, scoring and numerical evaluation. The assessment was carried out using a system of unconditional and conditional criteria, including validity, flexibility, ethics, complexity, progressiveness, level of transparency of algorithms, prospects for integration, availability of institutional support, and impact on innovative development. The use of the MathCad environment allowed for mathematical modelling and calculation of integral performance indicators.

The results showed that the most balanced and promising for implementation in Ukraine are the European approach (EU AI Act) and the Canadian approach (AIDA), which demonstrate a high level of regulatory maturity, transparency of regulatory procedures, the presence of an ethical component, and effective institutional support. The American approach (NIST AI RMF) and the ISO/IEC 23894 standard took intermediate positions due to their versatility and flexibility. In contrast, the Chinese model showed the lowest adaptability to Ukrainian conditions due to the dominance of centralised control principles. The proposed assessment methodology can be used to develop a national AI regulation strategy in Ukraine aimed at ensuring a balance between security, ethics and innovative technological development.

Key words: cybersecurity; security; artificial intelligence; technology; standardisation.

14 tab. 7 fig. Ref: 14 items.

УДК 004.056.55

Оцінка ефективності застосування міжнародних стандартів та регуляторних актів з регулювання моделей штучного інтелекту для України / Є.О. Логачова, М.В. Єсіна, Д.Ю. Голубничий // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2025. Вип. 223. С. 7–17.

Представлено комплексне дослідження ефективності застосування міжнародних стандартів і регуляторних актів у сфері штучного інтелекту (ШІ) з метою визначення найдоцільнішої моделі їх імплементації в Україні. Метою роботи є порівняльна оцінка провідних підходів до регулювання ШІ, розроблених у країнах ЄС, США, Канаді, Великій Британії, Південній Кореї, Китаї та інших державах, а також визначення міжнародних стандартів ISO/IEC. Дослідження базується на комплексному використанні методів багатокритеріального аналізу: попарних порівнянь, визначення вагових коефіцієнтів за шкалою Фішберна, методів ранжування, приписування балів і числового способу оцінювання. Оцінювання проводилось за системою безумовних та умовних критеріїв, серед яких – валідність, гнучкість, етичність, складність, прогресивність, рівень прозорості алгоритмів, перспективність інтеграції, наявність інституційної підтримки та вплив на інноваційний розвиток. Застосування середовища MathCad дозволило здійснити математичне моделювання та обчислення інтегральних показників ефективності.

Отримані результати показали, що найбільш збалансованими та перспективними для впровадження в Україні є європейський підхід (EU AI Act) та канадський (AIDA), які демонструють високий рівень нормативної зрілості, прозорість регуляторних процедур, наявність етичної складової та ефективну підтримку інституцій. Американський підхід (NIST AI RMF) і стандарт ISO/IEC 23894 посіли проміжні позиції завдяки своїй універсальності та гнучкості. Натомість китайська модель виявила найнижчу адаптивність до українських умов через домінування принципів централізованого контролю. Запропонована методика оцінювання може бути використана для розроблення національної стратегії регулювання ШІ в Україні, спрямованої на забезпечення балансу між безпекою, етикою та інноваційним розвитком технологій.

Ключові слова: кібербезпека; безпека; штучний інтелект; технології; стандартизація.

Табл. 14. Іл. 7. Бібліогр.: 14 назв.

UDC 004.056.5

Theoretical justification and practical implementation of entropy extractors based on national cryptographic algorithms / Ya.A. Derevianko D.Yu. Gorbenko // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2025. № 223. P. 18–30.

Improving the process of obtaining randomness requires special attention in modern cryptographic systems and primitives. This is because random data that does not meet the requirements can significantly weaken or compromise cryptographic applications. Therefore, it is necessary to calculate keys and parameters of cryptographic transformations based on the use of verified randomness, as well as to standardize and certify methods and means of generating random sequences and numbers.

Currently, there is a high demand not only for new sources of randomness, but also for methods and means that can obtain sequences with good randomness properties from samples from such sources. This task is accomplished by entropy extractors. The NIST Special Publication 800-90B defines the procedure for collecting and evaluating entropy from relevant noise sources, as well as the procedure for applying entropy extraction to the obtained data so that the result meets certain requirements for entropy per bit, uniformity, and unpredictability.

The most important step in building an entropy extractor is choosing the proper noise source, as it contains a non-deterministic process that provides entropy and is essentially the basis of security for the entropy source and for the RNG as a whole. If the non-deterministic activity of the NS produces something other than binary data, the sampling process includes a digitization process.

Other essential steps in building an extractor include evaluating the entropy at the output of the selected noise source and then applying trusted cryptographic primitives to obtain uniform data with the required amount of entropy based on the noise source outputs.

The paper analyzes existing recommendations for constructing entropy extractors based on cryptographic primitives, provides a theoretical justification for the possibility of using national algorithms as such extractors, and gives examples of practical implementation of extractors based on national cryptographic algorithms.

Further research plans include developing a block_cipher_df extraction algorithm based on the Kalyna block cipher algorithm mentioned in this study, verification of the compliance of extractor outputs based on national cryptographic algorithms with the entropy requirements, as well as the application of extractor output extension components based on national algorithms to obtain sequences of arbitrary length.

Key words: extractors; entropy extraction; noise source; random sequences; symmetric encryption; hash functions; entropy estimation.

2 tab. 7 fig. Ref: 11 items.

УДК 004.056.5

Теоретичне обґрунтування та практична реалізація екстракторів ентропії на основі національних криптографічних алгоритмів / Я.А. Дерев'янюк, Д.Ю. Горбенко // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2025. Вип. 223. С. 18–30.

Покращення процесу отримання випадковості потребує особливої уваги у сучасних криптографічних системах та примітивах. Це пов'язано з тим, що невідповідність випадкових даних встановленим вимогам може значно послабити чи скомпрометувати криптографічні застосунки. Отже необхідним є обчислення ключів та параметрів криптографічних перетворень на основі використання перевіреної випадковості, а також стандартизація та сертифікація методів та засобів генерування випадкових послідовностей та чисел.

Існує висока необхідність не тільки у нових джерелах генерації випадковості, а і у методах та засобах, які можуть отримати послідовності з хорошими властивостями випадковості з вибірок з таких джерел. Цю функцію виконують екстрактори ентропії. У NIST Special Publication 800-90B визначається порядок збору та оцінки ентропії з відповідних джерел шуму, а також порядок застосування екстракції ентропії з отриманих даних, щоб результат відповідав певним вимогам щодо ентропії на біт, рівномірності та непередбачуваності.

Найбільш важливим кроком під час побудови екстрактора ентропії є правильний вибір джерела шуму, оскільки воно містить недетермінований процес, що і надає ентропію і по суті є основою безпеки для джерела ентропії і для RNG в цілому. Якщо недетермінована активність ДШ виробляє щось інше, ніж двійкові дані, процес відбору зразків включає в себе процес оцифрування.

Також невід'ємними кроками при побудові екстрактора є оцінка ентропії на виході обраного джерела шуму і подальше застосування довірених криптографічних примітивів для отримання рівномірних даних з необхідною кількістю ентропії на основі виходів джерела шуму.

У роботі наведено аналіз існуючих рекомендацій щодо побудування екстракторів ентропії на основі криптографічних примітивів, виконано теоретичне обґрунтування можливості застосування національних алгоритмів у якості подібних екстракторів, а також наведено приклади практичної реалізації екстракторів на основі національних криптографічних алгоритмів.

У подальших дослідженнях планується розробка алгоритму екстракції block_cipher_df на основі алгоритму блокового шифрування Калина, перевірка відповідності виходів екстракторів на основі національних криптографічних алгоритмів необхідним вимогам щодо ентропії, а також застосування компонентів розширення виходу екстракторів на основі національних алгоритмів для отримання послідовностей довільної довжини.

Ключові слова: екстрактори; екстракція ентропії; джерело шуму; випадкові послідовності; симетричне шифрування; функції ґешування; оцінка ентропії.

Табл. 2. Іл. 7. Бібліогр.: 11 назв.

UDC 004.056.5

Evolution of block symmetric cipher architectures / K.E. Lysytskyi, I.V. Lysytska, I.M. Galtseva, E.P. Kolovanova // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2025. № 223. P. 31–37.

The article presents an analysis of the evolution and design principles of block symmetric ciphers (BSCs), which are a direct implementation of the fundamental ideas of Claude Shannon.

A detailed comparative analysis of two classical iterative architectures is carried out, namely, the Feistel Network (FN) and the Substitution-Permutation Network (SPN), which have become the basis for most modern standards (including DES and AES). The key differences in their reversibility, requirements for the round function and diffusion rate are considered. Additionally, alternative designs such as the Leigh-Massey (LM) Network and the Generalized Feistel

(GFN) Network, ARX (Add-Rotate-XOR) ciphers are investigated, emphasizing their role in providing faster diffusion and flexibility.

Three main directions of modern adaptation of BSNs are highlighted:

Performance on powerful processors: dominance of ARX (Add-Rotate-XOR) designs that replace traditional S-blocks with operations efficient for 32/64-bit architectures (e.g., ChaCha20);

Post-quantum stability: it is substantiated that BSNs such as AES-256 remain resistant to Grover's attack by doubling the key length;

Minimalism and Lightweight Cryptography: changing priorities to energy efficiency and minimizing hardware costs for IoT devices. This has led to the development of ciphers with very small S-blocks (like PRESENT), which compensate for the weaker round function by significantly increasing the number of rounds.

Thus, the article demonstrates that the architecture of BSS is a dynamic field that successfully evolves, effectively adapting to both theoretical threats (quantum computing) and hard practical hardware limitations

Key words: cryptography; cryptanalysis; block symmetric ciphers; post-quantum cryptography; lightweight cryptography.

1 tab. 3 fig. Ref: 23 items.

УДК 004.056.5

Еволюція архітектур блокових симетричних шифрів / К.Є. Лисицький, І.В. Лисицька, І.М. Гальцева, С.П. Колованова // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2025. Вип. 223. С. 31–37.

Представлено аналіз еволюції та конструктивних принципів блокових симетричних шифрів (БСШ), що є прямою реалізацією фундаментальних ідей Клода Шеннона.

Проведено детальний порівняльний аналіз двох класичних ітеративних архітектур – Мережі Фейстеля (FN) та Мережі Підстановки-Перестановки (SPN), які стали базисом для більшості сучасних стандартів (включаючи DES та AES). Розглянуто ключові відмінності в їхній оборотності, вимогах до раундової функції та швидкості дифузії. Додатково досліджено альтернативні конструкції, як-от Мережа Лея – Мецці (LM) та узагальнена Мережа Фейстеля (GFN), ARX-шифри (Add-Rotate-XOR), підкреслюючи їхню роль у забезпеченні швидкої дифузії та гнучкості.

Виділено три основні напрями сучасної адаптації БСШ:

Продуктивність на потужних процесорах: домінування ARX-конструкцій (Add-Rotate-XOR), які замінюють традиційні S-блоки операціями, ефективними для 32/64-бітних архітектур (наприклад, ChaCha20);

Постквантова стійкість: обґрунтовано, що БСШ, такі як AES-256, залишаються стійкими до атаки алгоритмом Гровера за рахунок подвоєння довжини ключа;

Мінімалізм і Легка Криптографія: зміна пріоритетів на енергоефективність та мінімізацію апаратних витрат для пристроїв IoT. Це призвело до розробки шифрів із дуже маленькими S-блоками (як PRESENT), які компенсують слабшу раундову функцію значним збільшенням кількості раундів.

Стаття демонструє, що архітектура БСШ є динамічною галуззю, яка успішно еволюціонує, ефективно адаптуючись як до теоретичних загроз (квантові обчислення), так і до жорстких практичних обмежень апаратного забезпечення.

Ключові слова: криптографія; криптоаналіз; блокові симетричні шифри; постквантова криптографія; легка криптографія.

Табл. 1. Іл. 3. Бібліогр.: 23 назв.

UDC 004.056.55

Systematization of zero-knowledge proof methods / R.I. Mordvinov // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2025. № 223. P. 38 – 43.

The article systematizes modern methods of zero-knowledge proof (ZKP). Classification features are considered: protocol interactivity, algebraic or stochastic basis, need for trusted setup, type of zero-knowledge, and proof model. Classical schemes (Fiat-Shamir, Schnorr, Blum), modern zk-SNARK and zk-STARK, as well as novel approaches – PLONK, Halo 2, Bulletproofs, lattice-based ZKPs, and machine learning proofs are described. A comparative analysis is conducted according to efficiency, proof size, generation and verification complexity. It is shown that SNARKs provide compactness but require a trusted setup, while STARKs are transparent and post-quantum secure but large. Open problems are highlighted: recursive proofs, standardization, metadata protection, and applications in machine learning. It is concluded that further research in this field is aimed at creating scalable, secure, and quantum-resistant protocols for digital technologies.

Key words: zero-knowledge proof; zero-knowledge; interactive protocol; zk-SNARK; zk-STARK; cryptographic protocol.

1 tab. Ref: 22 items.

УДК 004.056.55

Систематизація методів доказу з нульовим розголошенням / Р.І. Мордвінов // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2025. Вип. 223. С. 38 – 43.

Систематизовано сучасні методи доказу з нульовим розголошенням (Zero-Knowledge Proof, ZKP). Розглянуто класифікаційні ознаки: інтерактивність протоколу, алгебраїчна чи стохастична основа, потреба у довірній установці, тип нульового знання та модель доведення. Описано класичні схеми (Фіата–Шаміра, Шнора, Блума), сучасні zk-SNARK та zk-STARK, а також новітні підходи – PLONK, Halo 2, Bulletproofs, ZKP на решітках та для машинного навчання. Проведено порівняльний аналіз за ефективністю, розміром доказів, складністю

генерації та перевірки. Показано, що SNARKи забезпечують компактність, але потребують trusted setup; STARKи є прозорими й постквантово стійкими, проте громіздкі. Висвітлено відкриті проблеми: рекурсивні докази, стандартизація, захист метаданих, застосування у сфері машинного навчання.

Зроблено висновок, що подальші дослідження у цій галузі спрямовані на створення масштабованих, безпечних і квантово-стійких протоколів для цифрових технологій.

Ключові слова: доказ з нульовим розголошенням; нульове знання; інтерактивний протокол; zk-SNARK; zk-STARK; криптографічний протокол.

Табл. 1. Бібліогр.: 22 назв.

UDC 621.3.095.221

Quantitative model of passive speech information concealment means using the nonlinear attenuators / V.I. Zabolotny, Y.M. Holoborodko, D.M. Zabolotny, D.O. Abrosymov // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2025. № 223. P. 44 – 50.

The application of nonlinear filters for protection against information reconnaissance is considered on the example of using the phenomenon of acousto-electrical conversion in auxiliary technical means at the object of information activity. The principle of operation of nonlinear filters, their characteristics, typical schemes of their application in the conditions of conducting intelligence of dangerous signals from outside the controlled territory are analyzed, with the development of a quantitative model.

It is shown that the reconnaissance operator is able to reduce the effectiveness of leakage protection by disconnecting the communication line from the telephone exchange. According to the results of the analysis, it is proposed to counteract this by shunting the communication line with a resistor within the controlled area. A quantitative model in the Python programming language allowed us to visualize the conclusions obtained.

Key words: nonlinear attenuators; technical information leakage channel; technical information protection; planar diode.

9 fig. Ref: 8 items.

УДК 621.3.095.221

Кількісна модель засобів пасивного приховування мовної інформації нелінійними атенюаторами / В.І. Заболотний, Ю.М. Голобородько, Д.М. Заболотний, Д.О. Абросімов // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2025. Вип. 223. С. 44 – 50.

Розглянуто застосування нелінійних фільтрів для захисту від розвідки інформації на прикладі використання явища акустоелектричного перетворення у допоміжних технічних засобах на об'єкті інформаційної діяльності. Проаналізовано, з розробкою кількісної моделі, принцип роботи нелінійних фільтрів, їхні характеристики, типові схеми їх застосування в умовах ведення розвідки небезпечних сигналів із-за меж контрольованої території.

Показано, що оператор розвідки здатний зменшувати ефективність захисту від витоку шляхом від'єднання лінії зв'язку від телефонної станції. Запропоновано протидіяти цьому шляхом шунтування лінії зв'язку резистором в межах контрольованої зони. Кількісна модель мовою програмування Python дозволила візуалізувати одержані висновки.

Ключові слова: нелінійні атенюатори; технічний канал витоку інформації; технічний захист інформації; площинний діод.

Іл. 9. Бібліогр.: 8 назв.

UDC 004.056.5

Creating information security systems based on open portable trusted execution environment (OP-TEE), KVM/QEMU and intel trust domain extensions / P.V. Shulik, Ph.D., D.S. Balagura, Ph.D., V.V. Prosolov, D.O. Viukhin // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2025. № 223. P. 51–56.

The purpose of the article is to study one of the approaches of OP-TEE framework integration with Intel-X86 platforms using intel trust domain extensions technology. The subject of research is the integration of OP-TEE framework with Intel-X86 VT-d/VT-x using Intel TDX, KVM and QEMU.

The solution proposed in the article is based on the isolation of the secure world into a separate TD. The solution is based only on Linux or Android used as the host OS, so Kernel-based Virtual Machine (KVM) is used as the virtualization system.

For the standard open-source implementation of OP-TEE, there is a QEMU implementation for ARM TrustZone platforms that integrate easily and run in a KVM environment. So, we can run OP-TEE/QEMU/KVM as TD.

The article will be useful to specialists in the field of information security, dealing with data protection in the operating systems of computer systems.

Key words: OP-TEE; Intel x86; trust domain extensions; KVM; QEMU.

1 tab. 5 fig. Ref: 12 items.

УДК 004.056.5

Створення систем захисту інформації на базі open portable trusted execution environment (OP-TEE), KVM/QEMU та intel trust domain extensions / П.В. Шулік, Д.С. Балагура, В.В. Просолов, Д.О. В'юхін // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2025. Вип. 223. С. 51–56.

Метою статті є розгляд одного із підходів інтеграції OP-TEE фреймворка з Intel-X86 платформами із використанням технології intel trust domain extensions. Предметом дослідження є програмні засоби інтеграції OP-TEE фреймворка з Intel-x86 VT-d/VT-x з використанням Intel TDX.

Запропоноване в роботі рішення базується на ізоляції OP-TEE в окремій TD. Рішення базується тільки на використанні в якості хостової операційної OS Linux або Android, тому у якості системи віртуалізації використовується Kernel-based Virtual Machine (KVM).

Для стандартної реалізації OP-TEE з відкритим кодом існує реалізація QEMU для платформ ARM TrustZone, яка легко інтегрується і запускається в середовищі KVM. Таким чином, можливо запустити OP-TEE/QEMU/KVM як TD.

Стаття буде корисною фахівцям у галузі інформаційної безпеки, які займаються питаннями захисту даних в операційних системах комп'ютерних систем.

Ключові слова: OP-TEE; Intel x86; trust domain extensions; KVM; QEMU.

Табл. 1. Іл. 5. Бібліогр.: 12 назв.

UDC 004.056.5:629.7.052; 519.725:629.7.052

Overview of approaches to building secure, interference-resistant streaming video transmission systems for UAVs / S.Ya. Hilgurt, L.V. Kovalchuk, A.M. Davydenko // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2025. № 223. P. 57 – 65.

The article provides a systematic review of modern approaches that can be used to build a secure, interference-resistant system for transmitting streaming video from unmanned aerial vehicles (UAVs), in particular FPV kamikaze drones, which have become widespread in the military sphere. The problem of simultaneously ensuring cryptographic protection and interference resistance of the communication channel under the active influence of electronic warfare means is analyzed. Known solutions are considered, taking into account the requirements for such systems and the limitations imposed on them – ensuring minimal delay, limitations on computing resources and the sufficiency of ensuring temporary cryptoresistance, as well as the ability to function in interference conditions. The results of the study indicate the absence of an existing universal solution that would satisfy all requirements. The conclusion is made about the need to create new combined approaches to video stream encryption taking into account temporary stability, adaptability to channel conditions and the possibility of hardware implementation on FPGAs or systems on a chip.

Key words: UAV; video stream; encryption; interference-resistant; low-resource algorithms; FPGA; SoC.

Ref: 39 items.

УДК 004.056.5:629.7.052; 519.725:629.7.052

Огляд підходів до побудови захищених завадостійких систем передачі потокового відео з БпЛА / С.Я. Гільгурт, Л.В. Ковальчук, А.М. Давиденко // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2025. Вип. 223. С. 57 – 65.

Проведено системний огляд сучасних підходів, які можуть бути застосовані для побудови захищеної завадостійкої системи передачі потокового відео з безпілотних літальних апаратів (БпЛА), зокрема FPV-дронів-камікадзе, що набули широкого поширення у військовій сфері. Проаналізовано проблему одночасного забезпечення криптографічного захисту та завадостійкості каналу зв'язку в умовах активного впливу засобів радіоелектронної боротьби. Розглянуто відомі рішення з урахуванням вимог до таких систем та обмежень, що на них накладаються – забезпечення мінімальної затримки, обмеження на обчислювальні ресурси та достатності забезпечення тимчасової криптостійкості, а також здатності функціонування в умовах завад. Результати дослідження свідчать про відсутність наявного універсального рішення, яке б задовольняло всім вимогам. Зроблено висновки про необхідність створення нових комбінованих підходів до шифрування відеопотоку з урахуванням тимчасової стійкості, адаптивності до умов каналу та можливості апаратної реалізації на ПЛІС або системах на кристалі.

Ключові слова: БпЛА; відеопотік; шифрування; завадостійкість; малоресурсні алгоритми; ПЛІС; SoC.

Бібліогр.: 39 назв.

UDC 004.056.53

Evaluation of the effectiveness of AI-based attacks on fingerprint biometric authentication systems / I.V. Oleshko, V.I. Lutsenko, O.Y. Petrenko, O.A. Melnykova // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2025. № 223. P. 66 – 74.

The paper considers the urgent problem of information security in the context of the rapid development of artificial intelligence technologies and their use to bypass fingerprint biometric authentication systems. Comparative analysis of modern attack methods was conducted, particularly synthetic generation technologies such as SpoofGAN and FingerFaker, as well as algorithms for reconstructing fingerprints from minutiae templates, such as the methods of Feng and Jain and also Buzaglo and Keller. The vulnerability of fingerprint authentication systems to cyber threats utilizing Generative Adversarial Networks was analyzed. It is noted that the greatest threat to personalized security is posed by reconstruction methods, which allow attackers to recover the unique papillary pattern of a specific individual from a compromised template.

Reconstruction attack method based on the Buzaglo and Keller approach was implemented. The architecture of the implemented method was described, which includes an algorithm for minutiae map formation, a ResNet50-based encoder for creating a latent vector, and a StyleGAN2 generator. Hardware and software requirements for deploying such an attack using CUDA and Python was described. The process of converting a discrete set of minutiae into a

structured spatial representation and the subsequent generation of a realistic fingerprint image was described. A study was conducted using the standardized BOZORTH3 comparison algorithm to quantitatively assess the effectiveness of the proposed attack. Experimental results demonstrated the vulnerability of biometric systems to reconstruction-based attacks. It was established that even with strict security system settings with a False Acceptance Rate of 0.01%, the reconstructed fingerprints achieved a recognition accuracy of 96.68%.

A comparative analysis of the effectiveness of the implemented method against other AI-based attacks was performed. It was determined that while synthetic generation methods demonstrate high overall accuracy, the reconstruction method is critically dangerous specifically for targeted attacks on specific accounts.

Key words: biometrics; authentication; fingerprint; attack; reconstruction; neural network.

3 tab. 6 fig. Ref: 13 items.

УДК 004.056.53

Оцінка ефективності атак з використанням штучного інтелекту на системи біометричної автентифікації за відбитками пальців / І.В. Олешко, В.І. Луценко, О.Є. Петренко, О.А. Мельникова // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2025. Вип. 223. С. 66 – 74.

Розглядається актуальна проблема інформаційної безпеки в контексті стрімкого розвитку технологій штучного інтелекту та їх використання для обходу систем біометричної аутентифікації за відбитками пальців. Проведено порівняльний аналіз сучасних методів атак, зокрема технологій синтетичної генерації SpoofGAN та FingerFaker, а також алгоритмів реконструкції відбитків із шаблонів дрібниць, заснованих на методах Фенга і Джейна та Бузагло і Келлера. Проаналізовано вразливість систем автентифікації за відбитками пальців до кіберзагроз, що використовують генеративні змагальні мережі. Зазначено, що найбільшу загрозу для персоналізованої безпеки становлять саме методи реконструкції, які дозволяють зловмисникам відновлювати унікальний папілярний візерунок конкретної особи з компрометованого шаблону.

Реалізовано метод атаки реконструкцією, що базується на підході Бузагло і Келлера. Для цього було використано алгоритм формування карти дрібниць, енкодер на основі ResNet50 для створення латентного вектора та генератор StyleGAN2. Описано апаратні та програмні вимоги для розгортання такої атаки з використанням CUDA та Python. Показано процес перетворення дискретного набору мінуцій у структуроване просторове представлення та подальшу генерацію реалістичного зображення відбитка пальця. Проведено дослідження з використанням стандартизованого алгоритму порівняння BOZORTH3 для кількісної оцінки ефективності реалізованої атаки. Результати експерименту продемонстрували вразливість біометричних систем до атак за допомогою реконструкції. Встановлено, що навіть при жорстких налаштуваннях системи безпеки з коефіцієнтом хибного прийняття 0.01 % реконструйовані відбитки досягли точності розпізнавання на рівні 96.68 %.

Виконано порівняльний аналіз ефективності реалізованого методу з іншими атаками на основі штучного інтелекту. Визначено, що хоча методи синтетичної генерації демонструють високу загальну точність, метод реконструкції є критично небезпечним саме для цільових атак на конкретні облікові записи.

Ключові слова: біометрія; автентифікація; відбиток; атака; реконструкція; нейромережа.

Табл. 3. Іл. 6. Бібліогр.: 13 назв.

UDC 004.056.5

Using deep learning methods for visualization and detection of malware / O.I. Fediushyn, P.V. Shulik, V.V. Prosolov, D.O. Viukhin, O.V. Chechui // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2025. № 223. P. 75 – 84.

The purpose of the article is to conduct a comparative analysis of the effectiveness of common convolutional neural network architectures for the task of classifying malware, which was previously converted into graphic images. The approach is based on converting executable PE-files into grayscale images. The transfer learning method is applied to classify these images. The paper provides an experimental comparison of seven architectures (XceptionNet, DenseNet169, EfficientNetB0, MobileNetV2, InceptionV3, ResNet50V2, and VGG16) based on Accuracy, Precision, Recall, and F1-score metrics to determine the most effective and computationally balanced model for threat analysis.

The article will be useful to specialists in the field of cybersecurity and machine learning who are involved in the development of intelligent systems for detecting "zero-day" and polymorphic threats.

Key words: deep learning; convolutional neural network; malware; visualization; PE-file; transfer learning; cybersecurity.

2 tab. 6 fig. Ref: 12 items.

УДК 004.056.5

Використання методів глибокого навчання для візуалізації та виявлення шкідливого програмного забезпечення / О.І. Федюшин, П.В. Шулік, В.В. Просолов, Д.О. В'юхін, О.В. Чечуй // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2025. Вип. 223. С. 75 – 84.

Метою статті є проведення порівняльного аналізу ефективності поширених архітектур згорткових нейронних мереж для задачі класифікації шкідливого програмного забезпечення, яке було попередньо перетворено у графічні зображення. Підхід базується на перетворенні виконуваних PE-файлів у зображення у відтінках сірого. Для класифікації цих зображень застосовується метод трансферного навчання. У роботі проводиться експериментальне порівняння семи архітектур (XceptionNet, DenseNet169, EfficientNetB0, MobileNetV2, InceptionV3, ResNet50V2 та VGG16) на основі метрик Accuracy, Precision, Recall, F1-score для визначення найбільш ефективною та обчислювально збалансованою моделі при аналізі загроз.

Стаття буде корисною фахівцям у галузі кібербезпеки та машинного навчання, які займаються розробкою інтелектуальних систем виявлення "zero-day" та поліморфних загроз.

Ключові слова: глибоке навчання; згорткова нейронна мережа; шкідливе програмне забезпечення; візуалізація; PE-файл; трансферне навчання; кібербезпека.

Табл. 2. Іл. 6. Бібліогр.: 12 назв.

UDC 004.056

Analysis of resistance of the FULEECA, WAVE, BISCUIT, and RYDE post-quantum digital signature algorithms / A.A. Telnova, T.O. Hrinenko, O.P. Nariezhnii // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2025. № 223. P. 85 – 99.

Post-quantum digital signature algorithms are being developed as an alternative to classical schemes, capable of ensuring cryptographic security even in the presence of quantum computing power.

The results of the analysis and research of the FULEECA, WAVE, BISCUIT, and RYDE post-quantum digital signature algorithms, which are based on different cryptographic approaches to ensuring resistance in quantum computing environments — from code and rank schemes to multilateral quadratic constructions — providing multi-level resistance to a wide range of attacks, are presented.

The analysis showed that all the algorithms considered have high potential for use in post-quantum systems, meeting key requirements for security, performance, and efficiency. At the same time, each algorithm has its own requirements for resources, key and signature sizes, implementation features, and cryptographic resistance to classical and quantum attacks.

The results provide a basis for further comparative analysis, as well as for formulating recommendations for the application of each of the algorithms depending on the specifics of the information system, the level of threats, and the limitations of the implementation environment.

Key words: BISCUIT; FULEECA; post-quantum digital signature algorithm; quantum computer; quantum cryptography; RYDE; WAVE.

2 fig. Ref: 22 items.

УДК 004.056

Аналіз стійкості алгоритмів постквантового цифрового підпису FULEECA, WAVE, BISCUIT ТА RYDE / А.А. Тельнова, Т.О. Грінєнко, О.П. Нарєжний // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2025. Вип. 223. С. 85 – 99.

Алгоритми постквантового цифрового підпису розробляються як альтернатива класичним схемам, що здатна забезпечити криптографічну безпеку навіть за умови наявності квантових обчислювальних потужностей.

Надано результати аналізу та дослідження постквантових алгоритмів цифрового підпису FULEECA, WAVE, BISCUIT ТА RYDE, які представляють різні криптографічні підходи до забезпечення стійкості в умовах квантових обчислень – від кодових та рангових схем до багатосторонніх квадратичних конструкцій, що забезпечує різнорівневу стійкість до широкого спектру атак.

Проведений аналіз продемонстрував, що всі розглянуті алгоритми мають високий потенціал для використання у постквантових системах, задовольняючи ключові вимоги до безпеки, продуктивності та ефективності. Разом з тим, кожен з алгоритмів має свої вимоги до ресурсів, розмір ключів і підписів, особливості реалізації, а також криптостійкості до класичних і квантових атак.

Отримані результати створюють основу для подальшого порівняльного аналізу, а також для формування рекомендацій щодо застосування кожного з алгоритмів у залежності від специфіки інформаційної системи, рівня загроз та обмежень середовища реалізації.

Ключові слова: квантова криптографія; квантовий комп'ютер; постквантовий алгоритм цифрового підпису; FULEECA; WAVE; BISCUIT; RYDE.

Іл. 2. Бібліогр.: 22 назв.

UDC 004.056.55:004.8:004.75

ML-WAF information technology for classification and blocking of injection attacks in a containerized Web environment / T.I. Korobeinikova, N.V. Kravchuk // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2025. № 223. P. 100 – 110.

This paper presents an adaptive ML-based Web Application Firewall (ML-WAF) designed for the classification and blocking of injection attacks in containerized web environments. The relevance of this work is driven by the widespread adoption of micro-services, container orchestration, and Kubernetes, which significantly reshapes the requirements for securing HTTP(S) traffic. Traditional signature-based WAF solutions exhibit limited effectiveness against SQL Injection, Cross-Site Scripting, and Command Injection due to their variability, contextual dependence, and susceptibility to evasion techniques. The aim of the study is to develop and experimentally evaluate a ML-oriented web-filtering technology that provides high-accuracy detection of malicious HTTP(S) requests, low processing latency, and continuous model self-updating within an MLOps pipeline. To achieve this goal, the paper introduces conceptual, structural, functional, and information-logical models of the ML-WAF, along with UML representations (Use Case, Activity, Class, Sequence) that formalize the architecture, behaviour, and interactions between system components. The proposed technology incorporates a multi-stage processing pipeline, including TF/IDF vectorization with enriched features, a KNN classifier, a risk-based decision engine (ALLOW/SANDBOX/BLOCK), monitoring and logging subsystems, and automated model retraining. A hybrid method of integrating the ML component into a WAF in Kubernetes is pro-

posed, combining an Ingress Controller, a dedicated ML-service, and a Horizontal Pod Autoscaler. This approach ensures high scalability and stable performance under varying workloads. The practical evaluation was conducted in a Kubernetes-based containerized environment using realistic SQLi and XSS datasets and load testing with Apache JMeter. Experimental results demonstrate that the ML-WAF achieves a Precision of 0.95, Recall of 0.93, and an F_1 -score of 0.94, with an average processing latency of 3.9 ms and a throughput of approximately 700 requests per second. The system reduced false positives to 2.3%, compared to 6.8% for ModSecurity, while scaling the ML-WAF to six Pods increased throughput by 27% without degrading classification quality. The presented results confirm that the proposed ML-WAF technology forms a robust foundation for next-generation AI-driven security gateways in cloud-native and containerized infrastructures.

Key words: cybersecurity; ML-WAF; injection attacks; SQLi; XSS; containerized web environment; Kubernetes; KNN; TF/IDF; MLOps.

2 tab. 6 fig. Ref: 14 items.

УДК 004.056.55:004.8:004.75

Інформаційна технологія ML-WAF для класифікації та блокування ін'єкційних атак у контейнеризованому веб-середовищі / Т.І. Коробейнікова, Н.В. Кравчук // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2025. Вип. 223. С. 100–110.

Запропоновано адаптивну інформаційну технологію ML-WAF для класифікації та блокування ін'єкційних атак у контейнеризованому веб-середовищі. Актуальність роботи зумовлена широким поширенням мікросервісної архітектури, контейнеризації та Kubernetes, що змінює вимоги до кіберзахисту HTTP(S)-трафіку та знижує ефективність традиційних сигнатурних WAF-рішень у протидії SQL Injection, Cross-Site Scripting та Command Injection. Метою дослідження є розроблення та експериментальна оцінка ML-орієнтованої технології веб-фільтрації, яка забезпечує високоточне виявлення шкідливих HTTP(S)-запитів, низьку затримку обробки та підтримку самооновлення моделі в MLOps-конвеєрі. Для досягнення цієї мети побудовано концептуальну, структурну, функціональну та інформаційно-логічну моделі ML-WAF, а також UML-подання (Use Case, Activity, Class, Sequence), що формалізують архітектуру, поведінку та взаємодію компонентів. Технологія включає конвеєр обробки запитів із TF/IDF-векторизацією та ознаковим збагаченням, KNN-класифікатором, модулем прийняття рішень на основі ризику (ALLOW/SANDBOX/BLOCK), підсистемами моніторингу, логування та безперервного перенавчання моделі. Запропоновано гібридний метод інтеграції ML-компоненти у WAF у середовищі Kubernetes із використанням Ingress Controller, окремого ML-сервісу та Horizontal Pod Autoscaler, що забезпечує автоматичне масштабування без зниження якості класифікації. Практичну оцінку виконано в контейнеризованій інфраструктурі Kubernetes з використанням реалістичного набору SQLi та XSS-запитів і навантажувального тестування Apache JMeter. Експериментальні результати показали, що ML-WAF досягає точності (Precision) 0,95, повноти (Recall) 0,93 та F_1 -score 0,94 при середній затримці 3,9 мс і пропускній здатності близько 700 запитів/с. Частка хибно позитивних спрацьовувань знижена до 2,3 % проти 6,8 % у ModSecurity, а масштабування до шести Pod забезпечило зростання пропускної здатності на 27 % без втрати якості. Отримані результати підтверджують, що запропонована технологія ML-WAF є перспективною основою для побудови проактивних AI-керованих шлюзів безпеки в хмарних і контейнеризованих інфраструктурах.

Ключові слова: кібербезпека; ML-WAF; ін'єкційні атаки; SQLi; XSS; контейнеризоване веб-середовище; Kubernetes; KNN; TF/IDF; MLOps.

Табл. 2. Іл. 6. Бібліогр.: 14 назв.

UDC 004.056:174

Ethical principles and normative regulation of professional activity in cybersecurity: international standards, Ukrainian context, and practical guidelines / M.O. Yevdokymenko, V.Kh. Chakryan, V.V. Yevdokymenko // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2025. № 223. P. 111 – 120.

This paper explores the ethical foundations and legal regulation of professional activity in cybersecurity amid digital transformation. The authors emphasize the growing importance of digital trust and moral responsibility in the daily work of cybersecurity professionals. A comparative analysis of European, American, and Ukrainian frameworks (including GDPR, ACM and (ISC)² Codes of Ethics, ENISA recommendations, and Ukrainian legislation) identifies key normative anchors and ethical principles. The study highlights complex dilemmas such as the boundary between privacy and surveillance, ethical vulnerability disclosure, and the role of cybersecurity experts during cyber conflicts. Attention is given to the need for professional certification standards to include ethical components, as well as the integration of ethics into organizational policies, audit procedures, and education. The paper proposes practical guidelines for ethical auditing, internal policy-making, and protection of responsible researchers. Recommendations are also made for harmonizing Ukrainian regulations with international ethical standards and for developing a national code of ethics. This research contributes to the development of a professional cybersecurity culture based on responsibility, transparency, and digital rights. The results are applicable in academic curricula, policy design, and industry governance.

Key words: ethics; cybersecurity; trust; privacy; responsibility; legislation; standard; regulation; transparency; integrity.

1 fig. Ref: 22 items.

Етичні засади та нормативне регулювання професійної діяльності в сфері кібербезпеки: міжнародні стандарти, український контекст і практичні орієнтири / М.О. Євдокименко, В.Х. Чакрян, В.В. Євдокименко // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2025. Вип. 223. С. 111 – 120.

Розглядаються етичні основи та нормативне регулювання професійної діяльності у сфері кібербезпеки в умовах цифрової трансформації. Акцент зроблено на важливості цифрової довіри, моральної відповідальності та дотримання етичних норм у повсякденній роботі фахівців з кібербезпеки. На основі порівняльного аналізу стандартів ЄС, США та України (зокрема, GDPR, кодекси етики ACM і (ISC)², рекомендації ENISA, українське законодавство) окреслено ключові нормативні принципи. Розкрито складні етичні дилеми: межа між конфіденційністю і контролем, відповідальне розкриття вразливостей, поведінка фахівців у ситуаціях кібервійни. Обґрунтовано необхідність включення етичного компонента до професійної сертифікації, освітніх програм та внутрішніх політик організацій. Запропоновано практичні рекомендації щодо етичного тестування, формування політик, захисту дослідників та впровадження моделі “етики за замовчуванням”. Порушено питання гармонізації українських регуляторних підходів із міжнародними стандартами та доцільності створення національного етичного кодексу. Результати можуть бути використані в освітньому процесі, для формування політик безпеки та вдосконалення професійної культури у сфері цифрових технологій.

Ключові слова: етика; кібербезпека; довіра; приватність; відповідальність; закон; стандарт; регулювання; відкритість; доброчесність.

Лл. 1. Бібліогр.: 22 назв.

UDC 004.056.55:621.391

Unified cryptographic coprocessor architecture for post-quantum cryptography in 6G network equipment / Y.V. Kotukh // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2025. № 223. P. 121 – 125.

The advent of quantum computing poses significant threats to current cryptographic infrastructure protecting 5G and emerging 6G networks. In August 2024, the National Institute of Standards and Technology (NIST) published the first post-quantum cryptography (PQC) standards: ML-KEM (FIPS 203) for key encapsulation and ML-DSA (FIPS 204) for digital signatures. Real-world security protocols such as TLS 1.3 and IPsec require both operations simultaneously, necessitating efficient unified hardware implementations. This paper presents a novel unified cryptographic coprocessor architecture (UniPQC) supporting both ML-KEM and ML-DSA algorithms for deployment in 6G network equipment. The proposed architecture leverages the shared mathematical foundation of both algorithms, specifically the Number Theoretic Transform (NTT), to achieve significant resource optimization. We implement a configurable NTT engine with shared butterfly units capable of processing both 256-coefficient polynomials for ML-KEM and ML-DSA with different moduli ($q=3329$ and $q=8380417$). The architecture includes: Unified Polynomial Arithmetic Module (UniPAM), Hash and Sampling Unit (HSU) with Keccak-f[1600] core, Memory Management Unit (MMU) with conflict-free addressing, and Control Configuration Logic (CCL). The architecture is implemented on Xilinx Zynq UltraScale+ FPGA, achieving 285 MHz operating frequency with 4,512 LUTs, 3,245 FFs, 24 DSPs, and 8 BRAMs. Performance evaluation demonstrates that the unified design reduces area-time product by 34% compared to separate implementations while meeting the latency requirements for 6G Ultra-Reliable Low-Latency Communication (URLLC) applications. Complete TLS 1.3 handshake is achieved in under 300 μ s, with power consumption of 245 mW for ML-KEM and 312 mW for ML-DSA operations.

Key words: post-quantum cryptography; ML-KEM; ML-DSA; NTT; FPGA; 6G networks; hardware acceleration; unified architecture; URLLC; lattice-based cryptography.

Tab. 2. Ref: 33 items.

УДК 004.056.55:621.391

Щодо уніфікованої архітектури криптографічного копроцесора для постквантової криптографії в обладнанні мереж 6G / Є.В. Котух // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2025. Вип. 223. С. 121 – 125.

Стрімкий розвиток квантових обчислень створює значні загрози для криптографічної інфраструктури, що захищає мережі 5G та перспективні мережі 6G. У серпні 2024 р. Національний інститут стандартів і технологій США (NIST) опублікував перші стандарти постквантової криптографії (PQC): ML-KEM (FIPS 203) для інкапсуляції ключів та ML-DSA (FIPS 204) для цифрових підписів. Реальні протоколи безпеки, такі як TLS 1.3 та IPsec, потребують одночасного виконання обох операцій, що вимагає ефективних уніфікованих апаратних реалізацій. У статті представлено нову уніфіковану архітектуру криптографічного копроцесора (UniPQC), що підтримує обидва алгоритми ML-KEM та ML-DSA для розгортання в обладнанні мереж 6G. Запропонована архітектура використовує спільну математичну основу обох алгоритмів, зокрема теоретико-числове перетворення (NTT), для досягнення значної оптимізації ресурсів. Реалізовано конфігурований NTT-двигун зі спільними блоками-метеликами, здатний обробляти 256-коефіцієнтні поліноми для ML-KEM та ML-DSA з різними модулями ($q=3329$ та $q=8380417$). Архітектура включає: уніфікований модуль

поліноміальної арифметики (UniPAM), блок хешування та семплювання (HSU) з ядром Кессак-ff[1600], блок керування пам'яттю (MMU) з безконфліктною адресацією та логіку керування конфігурацією (CCL). Архітектуру реалізовано на FPGA Xilinx Zynq UltraScale+ із досягненням робочої частоти 285 МГц при використанні 4512 LUT, 3245 FF, 24 DSP та 8 BRAM. Оцінка продуктивності демонструє, що уніфікований дизайн зменшує добуток площі на час на 34 % порівняно з окремими реалізаціями, водночас задовольняючи вимоги латентності для застосувань 6G URLLC (надійний зв'язок з наднизькою затримкою). Повне рукописання TLS 1.3 виконується менш ніж за 300 мкс, споживана потужність становить 245 мВт для операцій ML-KEM та 312 мВт для ML-DSA.

Ключові слова: постквантова криптографія; ML-KEM; ML-DSA; NTT; FPGA; мережі 6G; апаратне прискорення; уніфікована архітектура; URLLC, решіткова криптографія.

Табл. 2. Бібліогр.: 33 назв.

RADIO ELECTRONIC AND INFORMATION SYSTEMS РАДІОЕЛЕКТРОННІ ТА ІНФОРМАЦІЙНІ СИСТЕМИ

UDC 621.391.8:004.89:004.056.5

Hierarchical clustering using a Kohonen neural network for secured wireless sensor networks /

L.I. Melnikova, O.V. Linnyk, S.V. Shtangei // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2025. № 223. P. 126 – 132.

In today's world, wireless sensor networks (WSNs) have found widespread application in environmental monitoring systems, smart cities, healthcare, and military technologies. However, despite their flexibility and scalability, WSNs remain vulnerable to a wide range of cyber threats, namely, from data interception to routing attacks and node spoofing. This study explores an approach to information protection in WSNs based on node clustering using the Kohonen neural network.

Modeling of clustering in wireless sensor networks using the Kohonen neural network has demonstrated significant effectiveness in solving the problem of adaptive network structure management. The generated topological maps show the network's ability to self-organize, form stable clusters, and integrate new sensors without disrupting classification logic. The Kohonen network successfully distributes sensors based on behavioral features, creating stable and adaptive clusters. The introduction of a new sensor and its automatic assignment to a cluster confirms the model capacity for dynamic response. Cluster formation that considers residual energy and spatial centralization contributes to energy conservation and extends the network lifecycle.

The proposed clustering approach based on the Kohonen neural network enables an efficient, flexible, and adaptive WSN structure, especially under dynamic operating conditions. Automatic determination of cluster membership for new sensors facilitates rapid response to topology changes without the need for centralized processing. The self-organizing nature of the Kohonen network makes it a promising tool for early detection of cyber threats through node behavior classification. Simulation results demonstrate the advantages of neural approaches in tasks related to information protection, network adaptation, and energy consumption optimization.

Key words: wireless sensor networks; Kohonen neural networks; clustering; data security; dynamic topology; energy efficiency; machine learning.

1 tab. 7 fig. Ref: 17 items.

УДК 621.391.8:004.89:004.056.5

Ієрархічна кластеризація для безпечної комунікації в сенсорних мережах з нейромережею Кохонена

/ Л.І. Мельнікова, О.В. Лінник, С.В. Штангей // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2025. Вип. 223. С. 126 – 132.

У сучасному світі безпроводові сенсорні мережі (БСМ) набули широкого застосування в системах моніторингу навколишнього середовища, розумних містах, охороні здоров'я та військових технологіях. Проте попри їхню гнучкість і масштабованість, БСМ залишаються вразливими до широкого спектру кіберзагроз – від перехоплення даних до атак на маршрутизацію та підробку вузлів. Розглядається підхід до захисту інформації в БСМ, що базується на кластеризації вузлів за допомогою мережі Кохонена.

Проведене моделювання кластеризації в безпроводових сенсорних мережах (БСМ) з використанням нейронної мережі Кохонена показало значну ефективність у розв'язанні задачі адаптивного управління структурою мережі. Згенеровані топологічні карти демонструють здатність мережі до самоорганізації, створення стабільних кластерів та інтеграції нових сенсорів без порушення логіки класифікації. Мережа Кохонена успішно розподіляє сенсори за поведінковими ознаками, створюючи стабільні та адаптивні кластери. Введення нового сенсора й автоматичне визначення його належності до кластеру підтверджує здатність моделі до динамічного реагування. Формування кластерів з урахуванням залишкової енергії та просторової централізації сприяє енергозбереженню та подовженню життєвого циклу мережі.

Запропонований підхід кластеризації на базі нейронної мережі Кохонена дозволяє забезпечити ефективну, гнучку та адаптивну структуру БСМ, особливо у динамічних умовах роботи мережі. Автоматичне визначення кластерної належності нових сенсорів сприяє оперативному реагуванню на зміни топології без потреби у централізованій обробці. Самоорганізаційна природа мережі Кохонена робить її перспективним інструментом для раннього виявлення кіберзагроз через класифікацію поведінки вузлів. Результати моделювання демонстру-

ють перевагу нейронних підходів у задачах захисту інформації, адаптації мережі та оптимізації енергоспоживання.

Ключові слова: безпроводові сенсорні мережі; нейронні мережі Кохонена; кластеризація; безпека даних; динамічна топологія; енергоефективність; машинне навчання.

Табл. 1. Іл. 7. Бібліогр.: 17 назв.

UDC 621.396:002.53

Detection of new radio emissions in automated radio monitoring / V.M. Bezruk, Y.M. Holoborodko, V.I. Zabolotny // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2025. № 223. P. 133 – 137.

The purpose of this work is to develop and investigate methods for detecting new radio emissions against a background of stationary interference under conditions of a priori uncertainty.

The methods used include the approach based on a probabilistic model of orthogonal expansions of observations. Decision rules were developed by comparing the Mahalanobis distance and Euclidean distances between current and reference signal energy spectra. Experimental studies were conducted on samples of real data from the shortwave range.

The main results and significance proposed and justified here include a family of detection algorithms, adapted to conditions of a priori uncertainty (particularly for Gaussian distributions). Experimental results confirmed the high effectiveness of the proposed algorithms. The developed algorithms are suitable for application in automated radio monitoring systems for the timely detection of new radiation sources.

Key words: radio control; stationary interference; detection of unknown signals; probabilistic properties of signals.

1 tab. 2 fig. Ref: 5 items.

УДК 621.396:002.53

Виявлення нових радіовипромінювань при автоматизованому радіоконтролі / В.М. Безрук, Ю.М. Голобородько, В.І. Заболотний // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2025. Вип. 223. С. 133 – 137.

Мета роботи: розробка та дослідження методів виявлення нових радіовипромінювань на тлі стаціонарних завад в умовах апіорної невизначеності.

Методи: використано підхід, заснований на ймовірнісній моделі ортогональних розкладів спостережень. Розроблено вирішальні правила, що ґрунтуються на порівнянні відстані Махаланобіса та евклідових відстаней між поточними та еталонними енергетичними спектрами сигналів. Експериментальні дослідження проведено на вибірках реальних сигналів та завад у короткохвильовому діапазоні.

Основні результати та значення: запропоновано та обґрунтовано сімейство алгоритмів виявлення, адаптованих до умов апіорної невизначеності (зокрема, для гаусівських розподілів). Отримано результати експериментальних досліджень, що підтвердили високу ефективність алгоритмів. Розроблені алгоритми можуть бути застосовані в системах автоматизованого радіоконтролю для оперативного виявлення нових джерел випромінювання.

Ключові слова: радіоконтроль; стаціонарні завади; виявлення невідомих сигналів; ймовірнісні властивості сигналів.

Табл. 1. Іл. 2. Бібліогр.: 5 назв.

UDC 004.942:623.465

Critical analysis of known missile guidance methods / I.O. Romanenko, A.L. Yalovets // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2025. № 223. P. 138 – 143.

Modern missile guidance methods play a key role in ensuring the effectiveness and reliability of air and missile defense systems. The choice of an appropriate guidance method directly affects target interception accuracy, flight time, and hardware implementation requirements of control systems. Until recently, most guidance methods were developed for limited engagement conditions, making their critical analysis particularly relevant from the standpoint of modern requirements.

The purpose of this study is to analyze and systematize well-known missile guidance methods to identify their advantages, limitations, and areas of effective application. Studying this issue makes it possible to obtain a deeper understanding of the current state of missile guidance theory and to substantiate the necessity of further research in this field. Thus, the article aims to perform a comparative analysis of classical guidance methods and to formulate requirements for a prospective guidance method capable of improving the performance of air and missile defense systems.

The paper considers pursuit guidance, constant lead angle guidance, proportional navigation, and parallel navigation methods. Their kinematic trajectories, application conditions, and compliance with the main requirements for modern guidance algorithms are analyzed. It is shown that none of the considered methods simultaneously satisfies all the stated requirements. Based on the performed analysis, the relevance of developing a new guidance method is substantiated. This method should be based on the further development of parallel navigation and incorporate an agent-oriented approach in three-dimensional space.

Key words: missile guidance method; missile; target; kinematic trajectory; proportional navigation; parallel navigation; agent-oriented approach; guidance system.

4 fig. Ref: 9 items.

УДК 004.942:623.465

Критичний аналіз відомих методів наведення ракет / І.О. Романенко, А.Л. Яловець // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2025. Вип. 223. С. 138 – 143.

Сучасні методи наведення ракет відіграють ключову роль у забезпеченні ефективності та надійності функціонування систем протиповітряної та протиракетної оборони. Вибір доцільного методу наведення безпосередньо впливає на точність ураження цілей, часові характеристики перехоплення та вимоги до апаратної реалізації систем управління. Донедавна більшість методів наведення розроблялись для обмежених умов застосування, що зумовлює необхідність їх критичного аналізу з позицій сучасних вимог.

Метою даної роботи є аналіз і систематизація відомих методів наведення ракет з метою визначення їхніх переваг, недоліків та меж ефективного застосування. Дослідження цього питання дозволяє глибше зрозуміти сучасний стан розвитку теорії наведення та обґрунтувати необхідність подальших наукових досліджень у цьому напрямі. Таким чином, у статті поставлено завдання виконати порівняльний аналіз класичних методів наведення та визначити вимоги до перспективного методу, здатного забезпечити підвищення ефективності систем ППО/ПРО.

Розглянуто методи погоні, постійного випередження, пропорційного та паралельного зближення. Проаналізовано кінематичні траєкторії, умови застосування та відповідність кожного з методів основним вимогам до сучасних алгоритмів наведення. Показано, що жодний із розглянутих методів не задовольняє всім вимогам одночасно. На основі аналізу обґрунтовано актуальність розроблення нового методу наведення, який має ґрунтуватися на розвитку методу паралельного зближення з використанням агентно-орієнтованого підходу у тривимірному просторі.

Ключові слова: метод наведення; ракета; ціль; кінематична траєкторія; пропорційне зближення; паралельне зближення; агентно-орієнтований підхід; система наведення.

Лл. 4. Бібліогр.: 9 назв.

BIOMEDICAL ENGINEERING БІОМЕДИЧНА ІНЖЕНЕРІЯ

UDC 004.93.1; 004.85; 681.7.06

Evaluation of the effectiveness of distance determination using the ARCore framework in low-light conditions / A. A. Sokolov, O. G. Avrunin, Ya.V.Nosova, T.V. Nosova // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2025. № 223. P. 144 – 150.

This paper presents results of the experimental evaluation of distance measurement accuracy using the ARCore under low-light conditions. The study employed a POCO X5 Pro smartphone with a test application, an Ekotenzor-03 photometer, and an INKERSI KE50 laser rangefinder as a reference. It was found that at illumination levels below 30–40 lx, errors increase significantly, especially at distances over 2 m, leading to failures in depth map generation. Applying averaging and median filtering across multiple measurements partially improved stability but did not eliminate the dependence on illumination. The results complement previous studies conducted under daylight conditions and outline practical limitations of the ARCore for navigation systems for visually impaired users.

Key words: ARCore; augmented reality; navigation; low illumination; distance measurement.

1 tab. 5 fig. Ref: 15 items.

УДК 004.93.1; 004.85; 681.7.06

Оцінка ефективності визначення відстані засобами фреймворку ARCore в умовах низького освітлення / А.А. Соколов, О.Г. Аврунін, Я.В. Носова, Т.В. Носова // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2025. Вип. 223. С. 144 – 150.

Подано результати експериментальної оцінки точності визначення відстані засобами ARCore в умовах низької освітленості. Для дослідження використано смартфон POCO X5 Pro з тестовим застосунком, фотометр Екотензор-03 та лазерний далекомір INKERSI KE50 як еталон. Встановлено, що при рівні освітленості нижче 30–40 лк похибка суттєво зростає, особливо на відстанях понад 2 м, що призводить до зриву побудови карти глибини. Використання усереднення та медіанного значення з кількох вимірів частково підвищує стабільність, проте не усуває залежності від освітленості. Результати доповнюють попередні дослідження, виконані за умов денного світла, та визначають практичні обмеження застосування ARCore у навігаційних системах для осіб із порушенням зору.

Ключові слова: ARCore; доповнена реальність; навігація; низька освітленість; вимірювання відстані.

Табл. 1. Лл. 5. Бібліогр.: 15 назв.

UDC 616-073.7

Simulation of a slice phantom of human vertebra trabecular tissue for the study of its CT reconstruction / S.O. Filimonov, L.O. Averianova // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2025. № 223. P. 151 – 156.

The relevance of the study is due to the need to assess the influence of CT reconstruction settings on the accuracy of calculating the parameters of the trabecular bone of the vertebrae. The aim of this study is to develop a digital phantom that accurately reflects the microarchitecture of trabecular bone tissue and can be used to model the results in real scanning conditions, with subsequent comparative analysis of morphometric parameters of cancellous bone obtained using CT. The phantom model of the trabecular bone section was developed based on histological characteristics obtained from micro-CT images. The complete workflow for the synthesis of a digital phantom of bone structures is based on micro-CT with subsequent complex data processing, including sinogram generation and image reconstruction. The projection sinogram was generated using the Radon transform with a predefined angular step, and then subjected to CT image reconstruction. The procedure for constructing and studying a digital CT phantom consisted of several key steps:

phantom generation, simulation of its CT image under conditions close to those of real clinical scans, and subsequent quantitative assessment of discrepancies between phantom image parameters and the reconstructed image. The results demonstrate the possibility of modeling trabecular bone architecture using a digital phantom, which provides a reproducible basis for quantitative assessment of bone microstructure. All stages of calculations and modeling were performed in the MATLAB environment (R2023b, MathWorks version) using the Image Processing Toolbox for image processing, as well as specially developed scripts for morphometric analysis adapted to the specific characteristics of trabecular architecture.

Key words: bone trabecular structure; synthetic CT phantom; Radon transform; inverse reconstruction; noise.

1 tab. 6 fig. Ref: 15 items.

УДК 616-073.7

Моделювання фантома зрізу трабекулярної тканини хребця людини для дослідження його КТ-реконструкції / С.О. Філімонов, Л.О. Авер'янова // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2025. Вип. 223. С. 151 – 156.

Актуальність дослідження зумовлена необхідністю оцінки впливу налаштувань КТ-реконструкції на точність розрахунку параметрів трабекулярної кістки хребців. Метою дослідження є розробка цифрового фантома, який точно відображає мікроархітектуру трабекулярної кісткової тканини та може бути використаний для моделювання результатів у реальних умовах сканування з подальшим порівняльним аналізом морфометричних параметрів губчастої кістки, отриманих за допомогою КТ. Модель фантома зрізу трабекулярної кістки розроблена на основі гістологічних характеристик, отриманих з мікро-КТ зображень. Повний процес синтезу цифрового фантома кісткових структур базувався на мікро-КТ з подальшою комплексною обробкою даних, включаючи генерацію синограми та реконструкцію зображення. Проекційна синограма була згенерована за допомогою перетворення Радона з попередньо визначеним кутовим кроком, а потім піддана КТ-реконструкції зображення. Процедура побудови та дослідження цифрового КТ-фантома складалася з кількох ключових етапів: генерація фантома, моделювання його КТ-зображення в умовах, що наближаються до умов реальних клінічних сканувань, та подальша кількісна оцінка розбіжностей між параметрами фантомного та реконструйованого зображень. Результати демонструють можливість моделювання архітектури трабекулярної кістки за допомогою цифрового фантома, що забезпечує відтворення основи для кількісної оцінки мікроструктури кістки. Усі етапи обчислень та моделювання були виконані в середовищі MATLAB (версія R2023b, MathWorks) з використанням Image Processing Toolbox для обробки зображень, а також спеціально розроблених скриптів для морфометричного аналізу, адаптованих до специфічних характеристик трабекулярної архітектури.

Ключові слова: кісткова трабекулярна структура; синтетичний КТ-фантом; Радон-перетворення; обернена реконструкція; шум.

Табл. 1. Іл. 6. Бібліогр.: 15 назв.

PHYSICS OF DEVICES, ELEMENTS AND SYSTEMS ФІЗИКА ПРИЛАДІВ, ЕЛЕМЕНТІВ І СИСТЕМ

UDC 621.3729(75)

Optimization of fluctuating power of diesel generators used in avionics systems / O.D. Menyailo, O.V. Grigorieva, V.G. Makhonin // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2025. № 223. P. 157 – 162.

The article is devoted to the consideration of methods for optimizing the fluctuation power of low-frequency frequency generators. The power supply to the forming mechanism is determined by the amplitude of the frequency-modulated components of fluctuation noise, their analytical analysis was carried out and the results of experimental observations were compiled. A clear geometric interpretation of the mechanism for minimizing the fluctuation parameters of the diode generator is given.

Among the significant number of methods for tracking the fluctuation parameters of diode generators in the robot, the victor is the method of separating their noise into amplitude-modulated and frequency-modulated components. Based on a thorough analysis of other optimization methods, the optimal operating modes of the generator on avalanche flow diodes were determined from the point of view of its fluctuation authorities.

The results of the investigations make it possible to optimize or regulate the level of their noise fluctuations during the design process of low-frequency generators.

Key words: diode low-frequency generators; fluctuation noise; amplitude-modulated components; frequency-modulated components; optimization methods.

4 fig. Ref: 8 items.

УДК 621.3729(75)

Оптимізація флуктуаційних властивостей діодних генераторів вбудованих систем авіоніки / О.Д. Меняйло, О.В. Григор'єва, В.Г. Махонін // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2025. Вип. 223. С. 157 – 162.

Присвячено розгляду методів оптимізації флуктуаційних властивостей діодних генераторів НВЧ. Розглянуто питання механізму формування амплітудно- та частотно-модульованих компонентів флуктуаційного шуму, проведено їх аналітичний аналіз та наведено результати експериментальних досліджень. Надано наглядну геометричну інтерпретацію механізму мінімізації флуктуаційних параметрів діодного генератора

Серед значної кількості методів досліджень флуктуаційних параметрів діодних генераторів в роботі використано метод розділення їх шумів на амплітудно-модульовані та частотно-модульовані компоненти. На основі

порівняльного аналізу оптимізаційних методів визначено оптимальні режими роботи генератора на лавино-протічних діодах з точки зору його флуктуаційних властивостей.

Результати досліджень дають можливість в процесі проектування діодних генераторів НВЧ оптимізувати, або регулювати рівень їх шумових флуктуацій.

Ключові слова: діодні генератори НВЧ; флуктуаційний шум; амплітудно-модульовані компоненти; частотно-модульовані компоненти; оптимізаційні методи.

Лл. 4. Бібліогр.: 8 назв.

UDC 621.385

Spectral Simulation of Mode Competition in a Magnetron with an Essential Influence of Space Charge /

I.M. Bondarenko, O.S. Hnatenko, A.V. Gritsunov, O.G. Pashchenko, H.M. Bendeberia, M.A. Kopot, S.V. Hryshkov // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2025. № 223. P. 163 – 171.

The article investigates the excitation and competition of different types of oscillations (modes) in a resonant system of a typical 2450 MHz magnetron of medium power (1 kW), which are usually used in microwave ovens for household and corporate purposes. A feature of such magnetrons is the significant influence of space charge forces on the process of spoke formation during the mutual transformation of modes while the “hopping” of modes. Inevitably, in such cases, the expansion of the spectrum of the output signal can, under several conditions (primarily, inadequate quality of the high-frequency shielding system), significantly worsen the electromagnetic environment around the microwave device, which can lead to disruption of the operation of Wi-Fi communication systems in adjacent frequency ranges.

The research is carried out by the method “Particle in Cell” using the Magnol Problem of the TULIPgm application package. A two-dimensional approximation and a second-level spectral model (the method of complex amplitudes) are used. The spectra of the output signal and the induced current of the probe, which is in the middle of the interaction space, are analyzed. During the research, it was possible to simulate the transition process between the working ($N/2$) mode of oscillations and the high-voltage neighboring ($N/2-1$) mode. Further transition to the ($N/2-2$) mode does not occur, instead the destruction of the spoke grouping takes place. During the transition process, a significant (although relatively short-term) broadening of the spectra is observed. The spectrum of the output signal when operating on the $N/2-1$ mode is analyzed in detail, in particular, the preservation of the component with the frequency of the operating ($N/2$) mode of relatively large amplitude is established. The essential effect of the space charge in relatively low-power magnetrons leads to significant nonlinearity of the electron cloud, which sharply increases the amplitudes of the intermodulation components during the transition processes and creates the phenomenon of anode voltage hysteresis when switching from one mode of oscillation to another and vice versa. Based on the research performed, design solutions can be proposed for further optimization of the operating modes of the most common magnetron generators.

Key words: computer simulation; magnetron; mode of oscillation; space charge; signal spectrum; transient process.

1 tab. 9 fig. Ref: 20 items.

УДК 621.385

Спектральне моделювання конкуренції видів коливань в магнетроні з суттєвим впливом просторового заряду / І.М. Бондаренко, О.С. Гнатенко, О.В. Гришунів, О.Г. Пащенко, Г.М. Бендеберія, М.А. Копоть, С.В. Гришков // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2025. Вип. 223. С. 163 – 171.

Досліджується збудження і конкуренція різних видів коливань (мод) резонансної системи типового 2450 МГц магнетрону середньої потужності (1 кВт), які зазвичай застосовуються в мікрохвильових печах побутового та корпоративного призначення. Особливістю таких магнетронів є суттєвий вплив сил просторового заряду на процес формування спиць при взаємному перетворенні мод під час «перескоку» видів. Неминуче в подібних випадках розширення спектру вихідного сигналу може за ряду умов (в першу чергу, неналежної якості системи високочастотного екранування) значно погіршити електромагнітну обстановку навколо НВЧ пристрою, чим призвести, зокрема, до порушення роботи систем Wi-Fi зв'язку в прилеглих діапазонах частот.

Дослідження виконуються методом “Particle in Cell” з використанням Задачі Magnol пакета прикладних програм TULIPgm. Використовується двовимірне наближення і спектральна модель другого рівня (метод комплексних амплітуд). Аналізуються спектри вихідного сигналу, а також наведеного струму зонду, який розташовано посередині простору взаємодії. В процесі досліджень вдалося змодельовати перехідний процес між робочим ($N/2$) видом коливань і високовольним сусіднім ($N/2-1$) видом. Подальший перехід до ($N/2-2$) моди не відбувається, натомість має місце руйнування угруповання спиць. Протягом перехідного процесу спостерігається суттєве (хоча й відносно короткочасне) розширення спектрів. Детально проаналізовано спектр вихідного сигналу при роботі на $N/2-1$ виді, зокрема, встановлено збереження компоненти з частотою робочого ($N/2$) виду відносно великої амплітуди. Суттєвий вплив об'ємного заряду у відносно малопотужних магнетронах призводить до суттєвої нелінійності електронної хмари, яка різко підвищує амплітуди інтермодуляційних компонент протягом перехідних процесів і створює явище гістерезису анодної напруги при переході від одного виду коливань до іншого та навпаки. На основі виконаних досліджень можуть бути запропоновані конструкторські рішення стосовно подальшої оптимізації експлуатаційних режимів найбільш розповсюджених магнетронних генераторів.

Ключові слова: комп'ютерне моделювання; магнетрон; вид коливань; просторовий заряд; спектр сигналу; перехідний процес.

Табл. 1. Лл. 9. Бібліогр.: 20 назв.

Composition, structure and microhardness of multicomponent tungsten carbide based coatings formed using the inverse magnetron sputtering system / D.V. Sliusar, O.M. Chugai, I.V. Kolodiy, S.V. Oliynyk, O.O. Poluboiarov, Y.A. Voloshyn, S.M. Kulish // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2025. № 223. P. 172 – 177.

The subject of research is the processes of forming multicomponent coatings based on tungsten carbide (WC) by sputtering of elements by the ion-plasma method. The aim is to study the influence of metals from the composition of its structural parts on the structure and microhardness of WC coatings formed using an ion-plasma spray system. The task is to study the effect of metals from the composition of the structural parts of the magnetron sputtering system on the period of the crystal lattice, the size of the coherent scattering region X-rays and the microhardness of WC coatings. The methods used in the research: X-ray diffraction analysis, scanning electron microscopy and microhardness. The results obtained: coatings based on WC coatings with a thickness of 3-6 microns. The coatings also contain the following elements: Fe, Mo, Cr, Ni, Ti, and O. Content of W in the samples varies widely. Moreover, with a decrease of this element, the iron content increases. At the same time, the chromium content varies slightly from sample to sample. Nickel and titanium are found only in some samples. It was found that the structure of the coatings belongs to the B1 type, the spatial group is №225. In all samples the lattice parameter of tungsten carbide significantly exceeds the value known from the literature ($a = 4,215\text{\AA}$). An important feature of the studied coating samples is the presence of a (200) texture in most of them. With an increase in the area of coherent scattering of X-rays, a tendency towards a decrease in the crystal lattice period and microhardness of the coatings is observed. Conclusions. The scientific novelty of the obtained results lies in the fact that for the first time the influence of metals from the composition of the structural parts of the inverted magnetron sputtering system on the crystal lattice period, the size of the coherent X-ray scattering region, and the microhardness of WC coatings has been established. At the same time, for the entire set of samples coatings, these parameters correlate with each other. The data obtained indicate the prospects for controlling a wide range of physical and technical properties of multicomponent coatings based on tungsten carbide during their formation using inverse magnetron sputtering systems with sectioned cathode units.

Key words: tungsten carbide; multicomponent coatings; magnetron sputtering systems; microhardness; crystal lattice period; coherent X-ray scattering region; texture.

1 tab. 2 fig. Ref: 17 items.

УДК 539.21: 621.79

Склад, структура та мікротвердість багатокомпонентних покриттів на основі карбіду вольфраму, сформованих методом інверсного магнетронного розпилення / Д.В. Слюсар, О.М. Чугай, І.В. Колодій, С.В. Олійник, О.О. Полубояров, Ю.А. Волошин, С.М. Куліш // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2025. Вип. 223. С. 172 – 177.

Предметом дослідження є процеси формування багатокомпонентних покриттів на основі карбіду вольфраму (WC) шляхом розпорошення елементів іонно-плазмовим методом. Метою є дослідження впливу на структуру та мікротвердість покриттів WC, що сформовані за допомогою іонно-плазмової розпорошувальної системи, металів зі складу її конструкційних деталей. Завдання дослідити вплив металів зі складу конструкційних деталей магнетронної розпорошувальної системи на період кристалічної решітки, розмір області когерентного розсіювання рентгенівських променів та мікротвердість покриттів WC. При проведенні досліджень використовувались методи: рентгеноструктурного аналізу, растрової електронної мікроскопії та мікротвердості. Одержано наступні результати. На підкладках зі сталі 14X17 сформовані покриття на основі WC товщиною 3-6 мкм. В складі покриттів є також елементи: Fe, Mo, Cr, Ni, Ti та O. Вміст W в зразках змінюється в широких межах. Причому зі зменшенням вмісту цього елемента зростає вміст заліза. У той же час вміст хрому несуттєво змінюється від зразка до зразка. Нікель і титан виявлено лише в деяких зразках. Встановлено, що структура покриттів відноситься до типу B1, просторова група №225. В усіх зразках параметр решітки карбіду вольфраму значно перевищує відоме з літературних джерел значення ($a = 4,215\text{\AA}$). Важливою особливістю досліджених зразків покриттів є наявність в більшості з них текстури (200). Зі збільшенням області когерентного розсіювання рентгенівських променів спостерігається тенденція до зменшення періоду кристалічної решітки та мікротвердості покриттів. Висновки. Наукова новизна одержаних результатів полягає в тому, що вперше встановлено вплив металів зі складу конструкційних деталей інверсної магнетронної розпорошувальної системи на період кристалічної решітки, розмір області когерентного розсіювання рентгенівських променів та мікротвердість покриттів WC. При цьому для всієї сукупності зразків покриттів зазначені параметри корелюють один з одним. Одержані дані свідчать про перспективність управління широким спектром фізико-технічних властивостей багатокомпонентних покриттів на основі карбіду вольфраму при їхньому формуванні за допомогою інверсних магнетронних розпорошувальних систем з секціонованими катодними вузлами.

Ключові слова: карбід вольфраму; багатокомпонентні покриття; магнетронні розпорошувальні системи; мікротвердість; період кристалічної решітки; область когерентного розсіювання рентгенівських променів; текстура.

Табл. 1. Іл. 2. Бібліогр.: 17 назв.

Modern BLDC motor control methods play a key role in ensuring the efficiency and reliability of their operation. Until recently, controlling these motors was a complex task, requiring high costs for specialized equipment and software. However, thanks to the constant development of technology, today's control methods have become more accessible and effective. The purpose of this study is to review English-language scientific sources devoted to BLDC motor control methods. Studying this issue will allow to obtain a deeper understanding of current trends and achievements in this area, which plays an important role in the further development of electrical systems and devices. Thus, this article sets itself the task of systematizing and analysing the scientific literature on BLDC motor control in order to highlight the current state of research in this area and identify prospects for further development. This article discusses the main aspects control systems for brushless DC motors (BLDC), which play an important role in modern technologies. The relevance of the study lies in the need to develop effective and reliable control systems to ensure optimal performance and functionality of devices using BLDC motors.

Key words: BLDC motor; control method; back EMF; torque; control system; controller; PID controller; vector control; direct torque control.

28 fig. Ref: 22 items.

УДК 621.313:681.5

Аналіз систем керування двигунами BLDC / П.В. Трофімов // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2025. Вип. 223. С. 178 – 193.

Сучасні методи керування BLDC-двигунами відіграють ключову роль у забезпеченні ефективності та надійності їхньої роботи. Донедавна керування цими двигунами було складним завданням, що вимагало високих витрат на спеціалізоване обладнання та програмне забезпечення. Однак завдяки постійному розвитку технологій, сучасні методи керування стали більш доступними та ефективними. Метою дослідження є огляд англomовних наукових джерел, присвячених методам керування BLDC-двигунами. Вивчення цього питання дозволить глибше зрозуміти сучасні тенденції та досягнення в цій галузі, що відіграє важливу роль у подальшому розвитку електричних систем та пристроїв. Таким чином, стаття ставить перед собою завдання систематизувати та проаналізувати наукову літературу з керування BLDC-двигунами, щоб висвітлити сучасний стан досліджень у цій галузі та визначити перспективи подальшого розвитку. Розглядаються основні аспекти систем керування безщітковими двигунами постійного струму (BLDC), які відіграють важливу роль у сучасних технологіях. Актуальність дослідження полягає в необхідності розробки ефективних та надійних систем керування для забезпечення оптимальної продуктивності та функціональності пристроїв, що використовують BLDC-двигуни.

Ключові слова: BLDC мотор; метод керування; зворотна ЕРС; крутний момент; система керування; контролер; ПІД-регулятор; векторне керування; пряме керування моментом.

Іл. 28. Бібліогр.: 22 назв.

COLLECTION OF SCIENTIFIC PAPERS

RADIOTEKHNIKA

Issue 223

In English and Ukrainian

ЗБІРНИК НАУКОВИХ ПРАЦЬ

РАДІОТЕХНІКА

Випуск 223

Англійською та українською мовами

Коректор Л.І. Сащенко

Підп. до друку 29.12.2025. Формат 60х90/8. Папір офсет. Гарнітура Таймс. Друк. ризограф.
Ум. друк. арк. 13,3. Обл.-вид. арк. 11,8 Тираж 300 прим. Зам. № 189. Ціна договір.

Харківський національний університет радіоелектроніки (ХНУРЕ)
Просп. Науки, 14, Харків, 61166.

Оригінал-макет підготовлено і збірник надруковано у ПФ „Колегіум”,
Свідоцтво про внесення суб’єкта видавничої діяльності до Державного реєстру видавців.
Сер. ДК №1722 від 23.03.2004.