ЗАТВЕРДЖУЮ
Проректор з наукової та науково-педагогічної роботи
Національного університету
«Одеська політехніка»

_____ Дмитро ДМИТРИШИН

"04" листопада 2022 р.

ВИСНОВОК

розширеного фахового семінару кафедри кібербезпеки та програмного забезпечення Національного університету «Одеська політехніка» про наукову новизну, теоретичне та практичне значення результатів докторської дисертації Соколова Артема Вікторовича на тему «Методологія розробки ефективної крипто-стеганографічної системи» на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.21 — Системи захисту інформації (протокол засідання №3 від 4 листопада 2022 р)

4.1. Актуальність теми дослідження.

Поточний етап розвитку інформаційних технологій характеризується значним зростанням обсягу мультимедіа контенту, у першу чергу, потокового, що змінює вимоги до сучасних систем захисту інформації, потребує одночасного застосування криптографічної та стеганографічної складової, що обумовило появу поняття крипто-стеганографічної системи або КСС.

Застосування таких КСС часто передбачається на обмежених у ресурсах пристроях, тобто мобільних телефонах, кишенькових комп'ютерах, безпілотних літальних апаратах тощо. Таким чином, поряд з вимогами до забезпечення певних властивостей стеганоповідомлення, нагальною стає вимога до забезпечення можливості роботи КСС на таких ресурсообмежених пристроях. Тим не менш, для рішення задачі забезпечення заданих властивостей стеганоповідомлення із застосуванням відомого на сьогоднішній день у відкритих літературних джерелах теоретичного базису, а також заснованих на ньому методів, передбачається застосування областей перетворення блоків контейнеру (сингулярне розкладання, дискретне косинусне перетворення (ДКП), вейвлет-перетворення та ін.), що призводить до значних обчислювальних витрат на підтримку роботи КСС і часто значно ускладнює, або навіть унеможливлює застосування такої системи захисту. Окрім того, застосування зазначених перетворень призводить до збільшення ймовірності похибок округлення при переході з області в область, що веде до можливого спотворення інформації, що захищається, зниження надійності сприйняття результуючого стеганоповідомлення.

Зазначене призводить до того, що на практиці на ресурсообмежених пристроях, через принципову неможливість застосування повноцінної КСС у зв'язку з її значною обчислювальною складністю, застосовується лише криптографічна складова, що призводить до суттєвого зниження загального рівня захисту.

З іншого боку, необхідність інтеграції стеганографічної та криптографічної складової КСС та забезпечення якнайбільшої імплементації концепцій дифузії та конфузії криптографічними конструкціями, поява практичних методів атаки на криптоалгоритми із застосуванням математичного апарату функцій багатозначної логіки та розвиток методів квантового криптоаналізу потребує розгляду і дослідження всіх можливих уявлень застосовуваних у КСС криптографічних конструкцій, тобто застосування математичного апарату функцій багатозначної логіки, у той час як на сьогодні у відкритих літературних джерелах розглядається лише представлення криптографічних конструкцій за допомогою булевих функцій. Означене призводить до зменшення криптографічної захищеності ДІ у сучасних КСС, дезінтеграції їх криптографічної та стеганографічної складової.

Отже, принципова можливість застосування КСС для забезпечення повноцінного захисту інформації на розповсюджених сьогодні ресурсообмежених пристроях лежить у площині розробки теоретичних основ та конкретних методів вбудовування криптозахищенної додаткової інформації без застосування областей перетворень, тобто у просторовій області контейнеру, що обумовлює актуальність теми дистанційного дослідження.

4.2. Зв'язок роботи з науковими програмами, планами, темами.

Тема дисертації відповідає науковому напряму кафедри кібербезпеки та програмного забезпечення Національного університету «Одеська політехніка».

Тематика роботи та її результати безпосередньо пов'язані зі Стратегією національної безпеки України від 14 вересня 2020 № 392/2020; Стратегією кібербезпеки України від 27 січня 2016 року №96/2016; Законом України Про основні засади забезпечення кібербезпеки України від 24.10.2020 №2163-VIII. Результати досліджень дисертаційної роботи використовувалися під час виконання НДР №0111U009481 «Підвищення ефективності методів цифрової обробки сигналів в радіотехнічних системах», НДР №0116U004923 «Оптимізація методів цифрової обробки інформації в корпоративних мережах та радіотехнічних системах», НДР №710-59 «Методи і технології радіаційного керування параметрами та стійкістю активних елементів електроніки до іонізуючих випромінювань».

4.3. Наукова новизна отриманих результатів.

У дисертації вперше одержані такі нові наукові результати:

1. *Вперше* на основі ЗПАІС встановлено взаємозв'язок між трансформантами двовимірного, одновимірного перетворення Уолша-Адамара та дискретного косинусного перетворення і складовими сингулярного розкладання матриці, що дало можливість отримання формальних достатніх

умов для заданих властивостей стеганоповідомлення, а також теоретичних основ для формування стеганографічних методів з кодовим управлінням.

2. *Вперше* на основі встановленого взаємозв'язку між трансформантами перетворення Уолша-Адамара, ДКП та сингулярним розкладанням матриці сформульовано достатні умови забезпечення надійності сприйняття та нечутливості стеганоповідомлення до збурних дій в області перетворення Уолша-Адамара, що дозволило сформувати основи теоретичного базису створення стеганографічних методів з кодовим управлінням вбудовуванням ДІ в просторовій області, забезпечуючи задані властивості КСС в умовах реального часу з використанням ресурсообмежених платформ.

3. *Вперше* на основі встановленого взаємозв'язку між перетвореннями Уолша-Адамара, ДКП та сингулярним розкладанням матриці сформовано теоретичний базис синтезу ефективних кодових слів та впроваджено і досліджено показники енергії E та селективності κ кодового слова, які дозволили синтезувати багаторівневі кодові слова, що забезпечують ефективність розроблених на їх основі стеганографічних методів з кодовим управлінням вбудовуванням ДІ, яка перевищує ефективність сучасних аналогів.

4. *Вперше* на основі розробленого теоретичного базису створено два стеганографічних методи з кодовим управлінням вбудовуванням ДІ з застосуванням бінарних та багаторівневих кодових слів, ефективність яких перевищує сучасні аналоги, зокрема в умовах потокового контейнера, та, на відміну від існуючих аналогів, забезпечує можливість ефективної роботи КСС в умовах реального часу з використанням ресурсообмежених платформ.

5. *Вперше* на основі концепції кодового управління вбудовуванням ДІ та запропонованих криптографічних примітивів розроблено спосіб формування стеганографічного ключа, який, на відміну від існуючих аналогів, дозволив забезпечити взаємозв'язок та врахувати взаємовплив криптографічної та стеганографічної складової КСС, наслідком чого стало забезпечення можливості її ефективної роботи з потоковим контейнером на ресурсообмежених платформах в режимі реального часу.

6. *Вперше* на основі ЗПАІС та теорії ФБЛ запропоновано науково-обґрунтовану методологію розробки КСС, яка забезпечує високу ефективність КСС, зокрема на ресурсообмежених платформах, на відміну від існуючих сучасних аналогів.

7. *Подальший розвиток* отримала технологія множинного доступу до прихованого каналу зв'язку за рахунок: використання розроблених кодів постійної амплітуди в технології MC-CDMA, двох запропонованих стеганографічних методів з множинним доступом, які базуються на кодах Ріда-Соломона та розроблених кодах просторових розстановок, що дозволило при збереженні переваг кодового управління забезпечити, на відміну від існуючих аналогів, підтримку роботи в системі до кількох тисяч користувачів та одночасну роботу кількох десятків користувачів, підвищити пропускну спроможність групового тракту в порівнянні з аналогами.

8. *Удосконалено* математичний підхід до оцінки якості криптографічних примітивів шляхом використання теорії ФБЛ, в результаті чого побудовано теоретичний базис забезпечення криптографічної якості ФБЛ, який включає

наступні критерії: алгебраїчна нелінійність, дистанційна нелінійність, критерій лавинного ефекту, критерій незалежності виходу від вхідних змінних, що дозволило обґрунтувати вибір ФБЛ для задач формування стеганографічного ключа при використанні стеганографічного методу з кодовим управлінням вбудовуванням ДІ.

9. *Удосконалено* криптографічні примітиви на основі розроблених критеріїв криптографічної якості ФБЛ шляхом синтезу множин S-блоків практично цінних довжин, що володіють максимально можливим рівнем нелінійності як компонентних булевих функцій, так і компонентних ФБЛ, задовольняють критерію розповсюдження помилки найвищих порядків, а також є оптимальними з точки зору критерію незалежності виходу компонентних ФБЛ від їх вхідних змінних, що дало можливість підвищити криптографічну якість конструкцій шифрів КСС.

10. *Удосконалено* БСШ прекодера на основі запропонованих криптографічних примітивів та концепції змінної фрагментації блоків, що дозволило прискорити, в порівнянні з аналогами, формування блоком, який оброблюється, властивостей псевдовипадкової послідовності, знизити обчислювальні затрати на роботу прекодера, підвищити криптографічну стійкість КСС в порівнянні з існуючими аналогами.

4.4. Ступінь обґрунтованості наукових положень та висновків, сформульованих у дисертаційній роботі.

Наукові положення, висновки і методи, отримані за результатами дисертаційного дослідження є обґрунтованими та достовірними.

Засади розробленого теоретичного базису побудови ефективних КСС узгоджуються з фундаментальними положеннями матричного аналізу, теорії інформації та кодування, теорії досконалих алгебраїчних конструкцій, загального підходу до аналізу стану й технології функціонування інформаційних систем.

Ефективність розроблених стеганографічних та криптографічних методів підтверджується проведенням численних експериментів із моделювання їх роботи в умовах різноманітних атак. Дані щодо проведених експериментів є повними та детальними, їх результати — наочними та такими, що узгоджуються з теоретичними очікуваннями.

4.5. Теоретичне та практичне значення результатів роботи.

Наукове значення виконаного дослідження полягає в створенні науково-обґрунтованої методології розробки КСС, яка забезпечує високу ефективність КСС, зокрема на ресурсообмежених платформах, яка не має аналогів в Україні та за її межами. Отримані результати можуть бути застосованими в галузі захисту інформації, кібербезпеки, в галузі інформаційних технологій.

Теоретичні засади та практичні результати, що були отримані в дисертації Соколова Артема Вікторовича впроваджено у навчальний процес Національного університету «Одеська політехніка» та застосовуються у дисципліні «Проблеми кібербезпеки та сучасні підходи до їх вирішення» для

студентів другого (магістерського) рівня вищої освіти спеціальності 125 – Кібербезпека.

Практична цінність роботи базується на тому факті, що отримані наукові результати були доведені до конкретних методів та алгоритмів, які можуть бути використані або вже використовуються у прикладних системах захисту інформації. Розроблені методи характеризуються високою швидкодією та простотою алгоритмічної реалізації, яка витікає з їх роботи у просторовій області та робить їх придатними для роботи з потоковими контейнерами з використанням ресурсообмежених платформ.

Алгоритмічна реалізація стеганографічного методу з кодовим управлінням вбудовуванням ДІ дозволяє забезпечити кількість помилок на рівні 1.6% при вилученні ДІ під дією атаки стиском проти вбудованого повідомлення з коефіцієнтом якості $QF = 10$, що у 8.125 разів менше за подібний показник найкращого відомого аналогу. При цьому значення показника PSNR складає 35.6 дБ, що на 3% перевершує значення найкращого відомого аналогу, який володіє сумірним рівнем стійкості до атак проти вбудованого повідомлення.

Алгоритмічна реалізація розробленого стеганографічного метода з кодовим управлінням вбудовуванням ДІ на основі просторово-частотних матриць дозволяє забезпечити кількість зареєстрованих у системі абонентів, що дорівнює $J = 4800$, а також кількість одночасно працюючих абонентів при нульовому рівні внутрішньосистемних перешкод, що дорівнює $J = 64$. Таким чином розроблений метод дозволяє отримати у 1200 разів більше зареєстрованих абонентів та у 16 разів більше одночасно працюючих абонентів при відсутності внутрішньосистемних перешкод.

Розроблений метод синтезу максимально нелінійних S-блоків як у сенсі компонентних булевих функцій, так і ФБЛ дозволяє синтезувати криптографічні конструкції з 4-нелінійністю $N_{4f} = 10.3431$, що до 21.55% перевищує значення найкращих відомих аналогів. Метод синтезу S-блоків, що відповідають суворому лавинному критерію компонентних 4-функцій та критерію максимального лавинного ефекту компонентних булевих функцій дозволяє покращити лавинні властивості криптографічних конструкцій на 9.375% у порівнянні з найкращими відомими аналогами, тоді як метод синтезу S-блоків з ідеальними матрицями коефіцієнтів кореляції $|R_{ij}| = 0, i, j = 1, 2, ..., k$ дозволяє покращити кореляційні властивості синтезованих криптографічних конструкцій на 12.5%.

На базі сконструйованих у дисертаційній роботі криптографічних примітивів, що засновані на ФБЛ, розроблено спеціалізований шифр для шифрування послідовності переліку станів, а також удосконалений БСШ прекодера, які на відміну від відомих існуючих аналогів, враховують криптографічну якість не тільки компонентних булевих функцій, а і компонентних ФБЛ.

Зменшення кількості необхідних для роботи стеганографічного методу з кодовим управлінням вбудовуванням операцій у $4\mu/3$ порівняно із найкращим аналогом дозволило реалізацію розробленої КСС в умовах обмежених технічних ресурсів, зокрема при роботі із потоковим контейнером в режимі

реального часу. При роботі з ЦВ роздільної здатності 400p/720p/1080p/1140p швидкість роботи КСС становить 1815/825/354/257 fps в режимі вбудовування та 236/106/47/33 fps в режимі вилучення ДІ на найпоширенішій IoT платформі Raspberry Pi 4 під керуванням Raspbian Pi OS. При цьому експериментально встановлено мінімально необхідні значення кількості операцій Single Thread ARM процесорів необхідні для роботи розробленої КСС, які при роботі з ЦВ роздільної здатності 400p/720p/1080p/1140p і частоти 30 fps для операції вбудовування ДІ, складають 7.4/16.6/37.3/52.5/149.2/437.9 MOps/Sec та 53.5/120.3/270.6/380.8/1082.4/4329.6 MOps/Sec для операції вилучення ДІ, що відповідає характеристикам переважної більшості застосовуваних на сучасних ресурсообмежених пристроях процесорів.

4.6. Апробація/використання результатів дисертації.

Матеріали дисертації доповідалися і обговорювалися:

1. На міжнародній науково-практичній конференції «Сучасні електронні та інформаційні технології», м. Одеса, 25-29 травня 2015 р.
2. На 19-му молодіжному форумі «Радіоелектроніка та молодь у XXI столітті», м. Харків, 20-22 квітня 2015.
3. На 17-й міжнародній науково-практичній конференції «Сучасні інформаційні та електронні технології», м. Одеса, 23-27 травня 2016 р.
4. На 20-му ювілейному молодіжному форумі «Радіоелектроніка та молодь у XXI столітті», м. Харків, 19-21 квітня 2016.
5. На 18-й міжнародній науково-практичній конференції «Сучасні інформаційні та електронні технології», м. Одеса, 22-26 травня 2017 р.
6. На V міжнародній науково-технічній конференції «Информационные технологии в образовании, науке и производстве», м. Мінськ, 18-19 листопада 2017 р.
7. На першій міжнародній науково-практичній конференції «Проблеми кібербезпеки інформаційно-телекомунікаційних систем», м. Київ, 5-6 квітня 2018 р.
8. На міжнародній конференції «Theory and Applications of Fuzzy Systems and Soft Computing», м. Київ, січень 2018 року.
9. На другій міжнародній конференції «Computer Modeling and Intelligent Systems», м. Запоріжжя, 2 квітня 2019 року.
10. На сьомій міжнародній науково-практичній інтернет-конференції «Сучасний рух науки», м. Дніпро, 6-7 червня 2019 р.
11. На міжнародній конференції «Cybersecurity Providing in Information and Telecommunication Systems», м. Київ, 7 липня, 2020 р.
12. Міжнародна науково-практична конференція «Наука та суспільне життя України в епоху глобальних викликів людства у цифрову еру», м. Одеса, 21 травня 2021 року.
13. На міжнародній конференції «Knowledge-Basedand Intelligent Information & Engineering Systems: Proceedings of the 25th International Conference», 8-10 вересня 2021, м. Щецин, Польща.
14. На міжнародній конференції «Cybersecurity Providing in Information and Telecommunication Systems», м. Київ, 28 січня 2021 р.

15. На міжнародній конференції «Engineer of XXI Century», м. Більсько-Бяла, Польща, 10 грудня 2021 р.

16. На міжнародній науково-практичній конференції «Intellectual Systems and Information Technologies», м. Одеса, 13-19 вересня 2021 р.

17. На міжнародній конференції «Computer Modeling and Intelligent Systems», м. Запоріжжя, 12 травня 2022 р.

Обґрунтованість основних наукових положень і висновків дисертанта підтверджується доведенням їх до конкретних методів та алгоритмів, які можуть бути використані або вже використовуються у прикладних системах захисту інформації. Отримані результати було впроваджено в діяльність підприємств ТОВ Компанія «Планета-Юг», ТОВ «Телекарт-прилад», ТОВ «Бізнес-центр НТЦ», ТОВ «Продукт – Постачання».

4.7. Оцінка змісту дисертації.

Дисертація складається зі вступу, шести розділів, загальних висновків, списку використаної літератури до кожного розділу, загалом 336 літературних джерел, додатків на 6 сторінках, 57 рисунків і 45 таблиць — всього 377 сторінок. Основний текст дисертації складається з 331 сторінки.

Стиль викладення результатів дисертації є зрозумілим та послідовним, все наведені математичні викладки є коректними та відповідають задачам, які вирішуються. Застосована термінологія відповідає загальноприйнятій в україномовних джерелах.

Структура дисертації, її мова та стиль викладення відповідає вимогам МОН України.

Тема та мета дисертаційної роботи узгоджуються з формулою спеціальності 05.13.21 — Системи захисту інформації «Дослідження теоретичних, науково-технічних і технологічних проблем, пов'язаних із організацією, створенням методів та засобів забезпечення захисту інформації при її зберіганні, обробці й передачі з використанням сучасних математичних методів, інформаційних технологій та технічних засобів».

Наукові результати дисертаційної роботи відповідають основним напрямкам досліджень, які наведено в паспорті спеціальності 05.13.21 — Системи захисту інформації. Аналіз наукової новизни роботи показав, що вона відповідає наступним пунктам:

п. 3. Організація, архітектура, методологія проектування, технологія функціонування систем захисту інформації.

п. 4. Методологія криптографічного аналізу та побудови оцінок криптографічної стійкості шифросистем, методи викриття механізмів криптоперетворень, зокрема дешифрування.

п. 6. Математичні й обчислювальні методи розрахунку надійності криптосистем, прогнозування оцінок криптографічної стійкості, розв'язання завдань криптографічного аналізу та синтезу шифросистем і криптографічних протоколів.

4.8. Дотримання принципів академічної доброчесності.

За результатами науково-технічної експертизи дисертація Соколова Артема Вікторовича визнана оригінальною роботою, яка не містить елементів фальсифікації, компіляції, фабрикації, плагіату та запозичень.

Матеріали кандидатської дисертації Соколова А.В. не використовуються.

4.9. Перелік публікацій за темою дисертації.

За результатами досліджень, які викладені в дисертаційній роботі, опубліковано 63 наукові роботи, з них 22 статті у фахових виданнях України, 29 в міжнародних виданнях, 26 статей у виданнях, що входять до наукометричних баз Scopus та/або Web of Science (з яких 5 статей є перекладами статей у фахових виданнях України), 17 публікацій у збірниках праць міжнародних та регіональних конференцій.

1. Kobozeva A. A., Sokolov A. V. The Sufficient Condition for Ensuring the Reliability of Perception of the Steganographic Message in the Walsh-Hadamard Transform Domain. *Problemele Energeticii Regionale*. 2022. 54 (2). P. 84-100. (**Scopus & Web of Science**)
2. Kobozeva A.A., Sokolov A.V. Efficient Coding of the Embedded Signal in Steganographic Systems with Multiple Access. *Problemele energeticii regionale*. 2021. No. 2 (50). P. 101-113. (**Scopus & Web of Science**)
3. Kobozeva A.A., Sokolov A.V. Robust Steganographic Method with Code-Controlled Information Embedding. *Problemele energeticii regionale*. 2021. No. 4 (52). P. 115-130. (**Scopus & Web of Science**)
4. Sokolov A. V., Zhdanov O. N Synthesis of highly nonlinear S-boxes satisfying higher order propagation criterion. *Journal of Discrete Mathematical Sciences and Cryptography*. 2020. P. 1-15. DOI: 10.1080/09720529.2019.1681675 (**Scopus & Web of Science**)
5. Sokolov A. V., Zhdanov O. N. Correlation immunity of three-valued logic functions. *Journal of Discrete Mathematical Sciences and Cryptography*. 2020. P. 1-17. DOI: 10.1080/09720529.2020.1781882 (**Scopus & Web of Science**)
6. Sokolov A. V., Zhdanov O.N. Regular synthesis method of a complete class of ternary bent-sequences and their nonlinear properties. *Journal of Telecommunication, Electronic and Computer Engineering*. 2016. Vol. 8, No. 9. P. 39-43. (**Scopus**)
7. Zhdanov O. N., Sokolov A. V. Block symmetric cryptographic algorithm based on principles of variable block length and many-valued logic. *Far East Journal of Electronics and Communications*. 2016. Vol. 16, No. 3. P. 573-589. DOI: 10.17654/EC016030573 (**Scopus**)
8. Жданов О. Н., Соколов А. В. О распространении конструкции Ниберг на поля Галуа нечетной характеристики. *Известия высших учебных заведений. Радиоэлектроника*. 2017. Т. 60, №12. С. 696-703. DOI: 10.20535/S0021347017120032 [Перекладений варіант: Zhdanov O. N., Sokolov A. V. Extending Nyberg construction on Galois fields of odd characteristic. *Radioelectronics and Communications Systems*. 2017. Vol. 60, No. 12. P. 538-544. DOI: 10.3103/S0735272717120032 (**Scopus**)]
9. Соколов А. В., Барабанов Н. А. Алгоритм устранения спектральной эквивалентности компонентных булевых функций S-блоков конструкции Ниберг. *Известия высших учебных заведений. Радиоэлектроника*. 2015. Т. 58,

№ 5. С. 41-49. DOI: 10.20535/S0021347015050040 [Перекладений варіант: Sokolov A. V., Barabanov N. A. Algorithm for removing the spectral equivalence of component Boolean functions of Nyberg-design S-boxes. *Radioelectronics and Communications Systems*. 2015. Vol. 58, No. 5. P. 220-227. DOI: 10.3103/S0735272715050040 (**Scopus**)]

10. Мазурков М. И., Соколов А. В., Барабанов Н. А. Метод синтеза бент-последовательностей в базисе Виленкина-Крестенсона. *Известия высших учебных заведений. Радиоэлектроника*. 2016. Т. 59, № 11. С. 47-55. DOI: 10.20535/S0021347016110054 [Перекладений варіант: Mazurkov M. I., Sokolov A. V., Barabanov N. A. Synthesis method for bent sequences in the Vilenkin-Chrestenson basis. *Radioelectronics and Communications Systems*. 2016. Vol. 59, No. 11. P. 510-517. DOI: 10.3103/S0735272716110054 (**Scopus**)]

11. Mazurkov M. I., Sokolov A. V., Tsevukh I. V. Synthesis method for families of constant amplitude correcting codes based on an arbitrary bent-square. *Journal of Telecommunication, Electronic and Computer Engineering*. 2017. Vol. 2, No. 9. P. 99-103. (**Scopus**)

12. Мазурков М. И., Соколов А. В. Алгоритм синтеза экономичных схем S-блоков подстановки на основе клеточных автоматов. *Известия высших учебных заведений. Радиоэлектроника*. 2016. Т. 59, № 5. С. 27-37. DOI: 10.20535/S0021347016050034 [Перекладений варіант: Mazurkov M. I., Sokolov A. V. Algorithm for synthesis of efficient S-boxes based on cellular automata. *Radioelectronics and Communications Systems*. 2016. Vol. 59, No. 5. P. 212-220. DOI: 10.3103/S0735272716050034 (**Scopus**)]

13. Sokolov A. V. Regular synthesis method of the sequences of length N=24 with optimal PAPR of Walsh-Hadamard spectrum. *Far East Journal of Electronics and Communications*. 2016. Vol. 16, No. 2. P. 459-469. DOI: 10.17654/EC016020459 (**Scopus**)

14. Мазурков М. И., Соколов А. В. Конструктивные методы синтеза двоичного корректирующего кода длины 32 для технологии MC-CDMA. *Известия высших учебных заведений. Радиоэлектроника*. 2019. Т. 62, No. 3. С. 123-135. DOI: 10.20535/S0021347019030014 [Перекладений варіант: Mazurkov M. I., Sokolov A. V. Constructive synthesis methods of binary error correcting code of length 32 for MC-CDMA technology. *Radioelectronics and Communications Systems*. 2019. Vol. 62, No. 3. P. 97-108. DOI: 10.3103/S0735272719030014 (**Scopus**)]

15. Sokolov A. V., Tsevukh I.V. Construction Method for Infinite Families of Bent Sequences. *Journal of Telecommunication, Electronic and Computer Engineering*. 2018. Vol. 10, No. 2. P. 51-54. (**Scopus**)

16. Sokolov A. V. Synthesis method of ternary bent-functions of three variables. *Radio Electronics, Computer Science, Control*. 2020. No. 1. P. 82-89. DOI: 10.15588/1607-3274-2020-1-9 (**Web of Science**)

17. Sokolov A. V., Zhdanov O. N. Avalanche Characteristics of Cryptographic Functions of Ternary Logic. *Radio Electronics, Computer Science, Control*. 2019. No.4(51). P.177-185. DOI: 10.15588/1607-3274-2019-4-17 (**Web of Science**)

18. Соколов А. В. Регулярный метод синтеза базовых бент-квадратов произвольного порядка. *Наука и техника*. 2016. Т. 15, №4. С. 345-352. DOI: 10.21122/2227-1031-2016-15-4-345–352 (**Web of Science**).

19. Sokolov A.V. Properties of the full class of quaternary bent-functions of two variables. *Journal of Discrete Mathematical Sciences and Cryptography*. 2021. P. 1-14. **(Scopus & Web of Science)**

20. Sokolov A.V., Radush V.V. A method for synthesis of S-boxes with good avalanche characteristics of component Boolean and quaternary functions. *Journal of Discrete Mathematical Sciences and Cryptography*. 2022. P. 1-12. **(Scopus & Web of Science)**

21. Sokolov A. V., Radush V. V. Avalanche characteristics of Nyberg construction S-boxes represented by the many-valued logic functions. *Informatics and Mathematical Methods in Simulation*. 2019. Vol. 9, No. 3. P. 111-119. DOI: 10.15276/imms.v9.no3.111

22. Соколов А. В., Жданов О. Н., Барабанов Н. А. Генератор псевдослучайных ключевых последовательностей на основе тройственных наборов бент-функций. *Проблемы физики, математики и техники*. 2016. №1(26). С. 85-91.

23. Соколов А. В., Жданов О. Н. Класс совершенных троичных решеток. *Системный анализ и прикладная информатика*. 2018. №2. С. 47-54. DOI: 10.21122/2309-4923-2018-2-47-54

24. Zhdanov O. N., Sokolov A. V. Spectral and Nonlinear Properties of the Sum of Boolean Functions. *Journal of Telecommunication, Electronic and Computer Engineering*. 2019. Vol. 11, No. 2. P. 31-35.

25. Соколов А. В., Жданов О. Н. Нелинейные преобразования конструкции Ниберг над изоморфными представлениями полей Галуа. *«Системный анализ и прикладная информатика»*. 2017. №3. С. 59-67. DOI: 10.21122/2309-4923-2017-3-59-67

26. Жданов О. Н., Соколов А. В. Метод синтеза базовых троичных бент-квадратов на основе оператора триадного сдвига. *Системный анализ и прикладная информатика*. 2017. № 1. С. 77-85. DOI: 10.21122/2309-4923-2017-1-77-85

27. Соколов А .В., Жданов О. Н., Айвазян А. О. Методы синтеза алгебраической нормальной формы функций многозначной логики. *Системный анализ и прикладная информатика*. 2016. №1. С. 69-76.

28. Жданов О. Н., Соколов А. В. Алгоритм построения оптимальных по критерию нулевой корреляции недвоичных блоков замен. *Проблемы физики, математики и техники*. 2015. № 3(24). С. 94-97.

29. Соколов А. В., Цевух И. В. О существовании бинарных С-кодов длины N=32 с заданным значением пик-фактора спектра Уолша–Адамара. *Проблемы физики, математики и техники*. 2017. № 2(31). С. 91-95.

30. Соколов А. В., Красота Н. И. Сильно нелинейные подстановки: метод синтеза S-блоков, обладающих максимальной 4-нелинейностью. *Наукові праці ОНАЗ ім. О.С. Попова*. 2017. № 1. С. 145-154.

31. Sokolov, A.V. Effect of binary orthogonal transform type on the cardinality and structure of constant amplitude codes for the MC-CDMA technology. *Informatics & Mathematical Methods in Simulation*. 2019. Vol. 9. No. 1-2. P. 5-14.

32. Соколов А. В. Метод синтеза полного класса бент-функций шести переменных. *Проблемы физики, математики и техники*. 2016. №4(29). С. 94-102.

33. Соколов А. В., Гаркуша А. А. Бесконечные семейства последовательностей Пэли с оптимальным пик-фактором спектра Уолша-Адамара. *Научные труды ОНАС им. А.С. Попова*. 2016. №2. С. 163-169.

34. Мазурков М. И., Соколов А. В., Барабанов Н. А. О влиянии вида ортогонального преобразования на пик-фактор спектра сигналов в системах с CDMA. *Информатика и математические методы в моделировании*. 2015. Т. 5, №1. С. 28-37.

35. Мазурков М. И., Соколов А. В. Рекуррентные методы синтеза последовательностей с оптимальным пик-фактором спектра Уолша-Адамара. *Информатика и математические методы в моделировании*. 2015. Т. 5, № 4. С. 203-209.

36. Соколов А. В., Барабанов Н. А. Системы ортогональных бифазных сигналов на основе бент-последовательностей. *Научные труды ОНАС им. А.С. Попова*. 2015. №1. С. 127-133.

37. Соколов А. В. Конструктивный метод синтеза последовательностей длины N = 20 с оптимальным спектром Уолша-Адамара. *Научные труды ОНАС им. А.С. Попова*. 2015. №2. С. 118-126.

38. Соколов А. В. Процессорно-ориентированные нелинейные преобразования на основе полных классов изоморфных и автоморфных представлений полей GF(512) и GF(1024). *Системный анализ и прикладная информатика*. 2015. № 4. С. 55-60.

39. Sokolov A. V. Nyberg construction nonlinear transforms based on all isomorphic representations of the Galois field GF(512) [Электронный ресурс]. *Проблеми телекомунікацій*. 2015. № 2 (17). С. 68-75.

40. Sokolov A.V., Isakov D.A. Authenticated encryption mode with blocks skipping. *System analysis and applied information science*. 2021. Vol. 3. P. 59-65.

41. Соколов А.В., Корж А.О. Исследование режимов шифрования с пропуском блоков. *Информатика и математические методы в моделировании*. 2020. Т. 10, №. 1-2. С. 100-108.

42. Судаков А.Ю., Соколов А.В. Розробка системи безпеки клієнт-серверного застосунку на базі операційної системи Android. *Інформатика та математичні методи в моделюванні*. 2020. Т. 10, № 3/4. С. 197-207.

43. Sokolov A.V. Multiple access steganographic method based on code control and frequency arrangements. *Informatics and Mathematical Methods in Simulation*. 2021. Vol. 11, No. 3. P. 147-161.

44. Kobozeva A.A., Sokolov A.V. Theoretical foundations for constructing effective codewords for the code-controlled information embedding steganographic method. *Radiotekhnika*. 2021. 4(207). P. 27–39. https://doi.org/10.30837/rt.2021.4.207.02.

45. Sokolov A.V. The steganographic method with multiple access based on frequency-spatial matrices. *Informatics and Mathematical Methods in Simulation*. 2022. Vol. 12, No. 1/2. P. 5-14.

46. Юровских Д.А., Соколов А.В., Троицкий Б.С. Полуторабайтные нелинейные преобразования конструкции Ниберг. *Информатика и математические методы в моделировании*. 2016. Т. 6, № 2. С. 142-148.

Наукові праці, які засвідчують апробацію матеріалів дисертації:

47. Bakunina E.V., Sokolov A.V. The Pseudorandom Key Sequences Generator Based on IV-Sets of Quaternary Bent-Sequences. *The Fifth International Workshop on Computer Modeling and Intelligent Systems*, Zaporizhzhia, Ukraine, May 12, 2022. P. 144-153. (**Scopus**)

48. Kazakova N. F., Sokolov A. V. Spectral and Nonlinear Properties of the Complete Quaternary Code. *Cybersecurity Providing in Information and Telecommunication Systems* : Proc., 7 July 2020. Kyiv, Ukraine, 2020. P. 76-86. (**Scopus**)

49. Sokolov A. V., Zhdanov O. N. Prospects for the Application of Many-Valued Logic Functions in Cryptography. *Advances in Computer Science for Engineering and Education* : Proceedings, January 2018. Kyiv, Ukraine, 2018. P. 331-339. DOI: 10.1007/978-3-319-91008-6_33 (**Scopus**)

50. Sokolov A. V. Interrelation Between the Class of Bent-Sequences and the Class of Perfect Binary Arrays. Proceedings of the *Second International Workshop on Computer Modeling and Intelligent Systems 2018*. Zaporizhzhia, Ukraine, 2019. P. 339-349. (**Scopus**)

51. Kazakova N.F., Karpinski M., Sokolov A.V., Gancarczyk T. Nonlinearity of Many-Valued Logic Component Functions of Modern Cryptographic Algorithms S-boxes. *Procedia Computer Science*. 2021. Vol. 192. P. 2731-2741. (**Scopus, Web of Science**)

52. Sokolov A., Kazakova N., Kuzmenko L., Mahomedova M. Prerequisites for developing a methodology for estimating and increasing cryptographic strength based on many-valued logic functions. *CEUR Workshop Proceedings*, 2021. 2923. pp. 107–116. (**Scopus**)

53. Соколов А. В., Оверчук Ю. С. О возможности синтеза алгебраической нормальной формы четверичных функций над полем GF(4). *Проблеми кібербезпеки інформаційно-телекомунікаційних систем* : зб. матеріалів першої міжнародної наук.-практ. конф., 5-6 квітня 2018 р. Київ. С. 384–388.

54. Соколов А. В., Жданов О. Н., Барабанов Н. А. Построение троичных бент-последовательностей. *Радиоэлектроника и молодежь в XXI веке* : сб. материалов XIX международного молодежного форума, 20-22 апреля 2015 г. Харьков, 2015. т. 3. С.131-132.

55. Соколов А. В., Корж А. О., Лопуленко О. В. Модифікований алгоритм шифрування зі змінною фрагментацією блоків. *WayScience* : матеріали VII міжнародної наук.-практ. конф., 6-7 червня 2019, Дніпро, 2019. С. 1592-1596.

56. Kazakova N., Sokolov A., Troyanskiy A. Correlation Immunity of Many-Valued Logic Component Functions of Modern Cryptographic Algorithm S-Boxes. *International Scientific and Practical Conference «Intellectual Systems and Information Technologies»*: Conference Proceedings / Odessa State Environmental University. Odessa, September 13-19, 2021. P. 268-275.

57. Соколов А. В., Авєкін В. В., Жук В. Г. Метод синтезу четвіркових бент-квадратів Агієвича. *Современные информационные и электронные технологии* : сб. материалов 18 международной науч.-практ. конф. 22-26 мая 2017 г. Одесса, 2017. С.152–153.

58. Соколов А. В., Ефимов О. И., Годунов А. И. О множестве линейных и нелинейных троичных последовательностей де Брейна длиной N = 9.

Современные информационные и электронные технологии : сб. материалов 18 международной науч.-практ. конф. 22-26 мая 2017 г. Одесса, 2017. С.154–155.

59. Юровских Д. А., Соколов А. В., Шипунова А. О. Полуторабайтные нелинейные преобразования конструкции Ниберг. *Современные информационные и электронные технологии* : сб. материалов 17 международной науч.-практ. конф. 23—27 мая 2016 г. Одесса : ОНПУ, 2016. С. 137–138.

60. Соколов А. В., Гаркуша А. А. Исследование пик-фактора спектра Уолша–Адамара полного кода длины *N*=28. *Современные информационные и электронные технологии* : сб. материалов 17 международной науч.-практ. конф. 23–27 мая 2016 г. Одесса : ОНПУ, 2016. С. 79–80.

61. Соколов А. В., Ткаченко М. В. Модифицированный генератор ключевых последовательностей на основе дуальных пар бент-функций. *Современные информационные и электронные технологии* : сб. материалов 17 международной наук.-практ. конф. 23—27 мая 2016 г. Одесса : ОНПУ, 2016. С. 139–140.

62. Соколов А. В., Юровских Д. А. Полуторабайтные экономичные нелинейные преобразования на основе последовательностей де Брейна. *Радиоэлектроника и молодежь в XXI столетии* : сб. материалов 20 юбилейного молодежного форума, 19-21 апреля 2016 г. Харьков, 2016. т.3. С. 97-98.

63. Соколов А. В., Барабанов Н. А. Системы ортогональных бифазных сигналов на основе бент-последовательностей длины 16. *Современные информационные и электронные технологии* : сб. материалов XVI международной наук.-практ. конф. 25–29 мая 2015 г. Одесса, 2015. С. 139 –140. С. 75-76.

У ході обговорення дисертаційної роботи до неї не було висунуто жодних зауважень щодо самої суті.

5. З урахуванням зазначеного, **на розширеному фаховому семінарі кафедра ухвалила:**

5.1. Докторська дисертаційна робота *Соколова Артема Вікторовича* «Методологія розробки ефективної крипто-стеганографічної системи» є завершеною науковою працею, яка містить раніше незахищені наукові дослідження та отримані автором нові науково-обґрунтовані результати, які у сукупності розв'язують науково-прикладну проблему, що полягає у забезпеченні ефективності роботи крипто-стеганографічної системи, зокрема, в режимі реального часу на ресурсообмежених платформах шляхом розробки науково-обґрунтованої методології, що орієнтована на управління вбудовуванням криптозахищеної додаткової інформації у просторовій області контейнера, що має важливе значення для технічних наук;

5.2. У 63 наукових публікаціях повністю відображені основні результати дисертації, з них 22 статті у фахових виданнях України, 29 в міжнародних виданнях, 26 статей у виданнях, що входять до наукометричних баз Scopus та/або Web of Science (з яких 5 статей є перекладами статей у фахових виданнях України), 17 публікацій у збірниках праць міжнародних та регіональних конференцій.

5.3. Дисертація відповідає паспорту спеціальності *05.13.21 — Системи захисту інформації* (Перелік наукових спеціальностей, затверджений Наказом

Міністерства освіти і науки, молоді та спорту України 14 вересня 2011 року № 1057) та вимогам, які ставляться до робіт на здобуття наукового ступеня доктора наук, п. 7 та 9 Порядку присудження та позбавлення наукового ступеня доктора наук, затвердженого постановою Кабінету Міністрів України від 17 листопада 2021 року № 1197.

5.4. З урахуванням наукової зрілості та професійних якостей *Соколова Артема Вікторовича* дисертаційна робота «Методологія розробки ефективної крипто-стеганографічної системи» рекомендується для подання до розгляду у спеціалізовану вчену раду Д 35.052.18 Національного університету «Львівська політехніка» за спеціальністю 05.13.21 — Системи захисту інформації.

За затвердження висновку проголосували:

за	18	*(вісімнадцять)*
проти	-	*(немає)*
утримались	-	*(немає)*

Головуючий на засіданні
проф. кафедри кібербезпеки
та програмного забезпечення,
д.т.н., професор _____ Сергій ПОЛОЖАЄНКО

Секретар
доцент кафедри кібербезпеки
та програмного забезпечення
к.т.н., доцент _____ Олена ЛЕБЕДЄВА

Рецензенти:

Професор кафедри
комп'ютеризованих систем
та програмних технологій,
д.т.н., доц. _____ Олександр ФОМІН

Завідувач кафедри
електромеханічної інженерії,
д.т.н., професор _____ Дмитро МАЄВСЬКИЙ

Професор кафедри
кафедри кібербезпеки
та програмного забезпечення,
д.т.н., професор _____ Вадим МОКРІЦЬКИЙ

«04» листопада 2022 р.