ВИСНОВОК

про наукову новизну, теоретичне та практичне значення результатів дисертації Бондаренко Микити Олеговича на тему «Моделі та методи інформаційної технології створення криптосистем на основі функцій дійсних змінних», поданої на здобуття ступеня доктора філософії з галузі знань 12 «Інформаційні технології» за спеціальністю 122 «Комп'ютерні науки»

Характеристика особистості здобувача

Бондаренко Микита Олегович у 2018 році закінчив Сумський державний університет за напрямом підготовки «Інформатика», освітній рівень «Бакалавр»; з 2018 по 2019 р. навчався в магістратурі Сумського державного університету за спеціальністю «Комп'ютерні науки та інформаційні технології». З 2020 і по сьогодні є здобувачем наукового ступеню доктора філософії в Сумському державному університеті за спеціальністю 122 «Комп'ютерні науки» на кафедрі комп'ютерних наук.

Тему дисертації у останній редакції затверджено на засіданні Вченої ради СумДУ (протокол № 15 від «29» червня 2023 р.).

За час навчання в аспірантурі Бондаренко М.О. зарекомендував себе сумлінним, відповідальним та високопрофесійним науковцем. Опанував та оволодів сучасними методами наукових досліджень.

Прийняв участь у всеукраїнських та міжнародних науково-практичних конференціях, зокрема Міжнародній науково-практичній конференції «Інформаційна безпека та інформаційні технології»(м. Одеса, 2021 р.), Міжнародній науково-технічній конференції студентів та молодих учених «Інформатика, математика, автоматика» (Суми-Астана, 2022 р.), Міжнародній науково-технічній конференції студентів та молодих учених «Інформатика, математика, автоматика» (Суми-Астана, 2023 р.) та Міжнародній науково-технічній конференції студентів та молодих учених «Інформатика, математика, автоматика» (Суми-Астана, 2024 р.)

Основні результати дисертаційної роботи опубліковано в 10 наукових працях, зокрема 4 статті у наукових фахових виданнях України (у тому числі, одна стаття у виданні, що індексується міжнародною наукометричною базою Scopus), 4 публікації у збірниках матеріалів міжнародних конференцій та 2 патентах на корисну модель. Об'єктом дослідження у дисертаційній роботі Бондаренко М. є процеси криптографічного захисту даних. Предметом досліджень є моделі, методи та алгоритми криптографічних систем на основі функцій дійсної змінної. Метою дослідження є розробка нових моделей та методів криптосистем на

основі функцій дійсної змінної для підвищення стійкості та ефективності шифрування як текстових даних, так і зображень. Наукове завдання складається з наступного:

1. Провести аналіз сучасних криптографічних систем, їх переваг та недоліків. Зокрема, звернути увагу на криптосистеми на основі дійсних чисел.
2. Розробити математичну модель криптосистеми на основі функцій дійсної змінної, яка дозволяє використовувати переваги потужності множини дійсних чисел для підвищення криптостійкості.
3. Створити метод шифрування даних з використанням суми функцій дійсної змінної як симетричних ключів.
4. Розробити метод дешифрування даних, які зашифровані за обчислення невідомих коефіцієнтів ключових функцій.
5. Адаптувати розроблені методи для шифрування та дешифрування зображень, враховуючи специфіку візуальних даних.
6. Розробити алгоритм використання зображення як криптографічного ключа для шифрування інших зображень на основі запропонованих методів.
7. Створити програмну реалізацію розроблених криптосистем
8. Провести експериментальні дослідження їх ефективності.

Актуальність теми

Актуальність даного дослідження зумовлена комплексом факторів, що формують сучасні виклики у сфері інформаційної безпеки та криптографії:

1. Обмеження існуючих криптосистем: більшість сучасних криптографічних систем, таких як AES та RSA, базуються на операціях з цілими числами. Хоча ці системи широко використовуються, вони стикаються з низкою проблем. Зокрема, зі зростанням обчислювальної потужності виникає необхідність постійного збільшення довжини ключів, що призводить до зростання обчислювальних витрат. Крім того, кінцевий набір цілих чисел потенційно обмежує довгострокову стійкість цих систем перед розвитком методів криптоаналізу.
2. Загроза квантових обчислень: розвиток квантових комп'ютерів створює загрозу для багатьох існуючих криптографічних алгоритмів. Зокрема, квантовий алгоритм Шора може ефективно вирішувати проблеми факторизації та дискретного логарифму, на яких базується безпека RSA та ECC. Так, розвиток квантових комп'ютерів становить загрозу для багатьох

криптографічних систем, що підштовхує до принципово інших математичних підходів до шифрування.

3. Потреба в нових підходах: аналіз сучасного стану криптографії показує активні дослідження нових методів на альтернативних засадах, що демонструє потребу в розробці інноваційних способів захисту даних. Однак, більшість з цих нових систем все ще зосереджені на цілих числах і мають свої недоліки.

4. Специфіка захисту зображень: існує окремий напрямок криптографії, спрямований на створення систем для шифрування зображень, що дозволяли б використовувати властивості візуальних даних для покращення стійкості. Це вказує на потребу в спеціалізованих криптографічних рішеннях для різних типів даних.

5. Потенціал систем на основі дійсних чисел: використання криптосистем на основі дійсних чисел представляє перспективний напрямок досліджень. Оскільки потужність множини дійсних чисел вища за потужність множини цілих чисел, це потенційно може забезпечити більший простір ключів та вищу криптографічну стійкість. Однак, дослідження в цьому напрямку є менш розповсюдженими і потребують подальшого розвитку.

6. Інтегральна криптографія: дослідження в області інтегральної криптографії, зокрема використання інтегральних рівнянь Фредгольма, відкривають нові можливості для створення криптосистем з теоретично гарантованою стійкістю. Це вказує на потенціал використання нових математичних підходів у криптографії.

Таким чином, дослідження нових методів криптографічного захисту на основі функцій дійсної змінної та інтегральної непропорційності є актуальним та важливим завданням. Воно має потенціал для створення нових криптографічних примітивів, які могли б подолати обмеження існуючих систем, та запропонувати ефективні рішення для захисту різних типів даних, включаючи зображення. Тема відповідає сучасним тенденціям розвитку криптографії та має потенціал для внеску у підвищення безпеки цифрової інформації в сучасному світі.

Зв'язок роботи з науковими програмами та темами

Дисертаційну роботу виконано на кафедрі комп'ютерних наук Сумського державного університету відповідно до плану науково-дослідних робіт за держбюджетними темами: «Методи, математичні моделі та

інформаційні технології аналізу і синтезу інфокомунікаційних систем» (ДР № 0118U006971, 2018-2023).

Роль автора в цій науково-дослідній роботі полягала в розробці моделей та методів шифрування і дешифрування даних для застосування інфокомунікаційних системах.

Особистий внесок здобувача у виконання дисертаційної роботи

Дисертаційна робота є самостійним завершеним науковим дослідженням. Положення і результати, винесені на захист дисертаційної роботи, отримані здобувачем особисто.

Автором дисертації особисто виконано огляд та аналіз даних літератури за темою наукового дослідження, сформульовані мета роботи, її завдання, створений план. Дисертантом власноруч реалізовані всі етапи дисертаційного дослідження та підготовлені всі розділи роботи з використання сучасних методів наукового дослідження. Дисертантом разом із науковим керівником проведено узагальнення одержаних результатів дослідження, сформульовано основні положення та висновки. Автором самостійно підготовлені матеріали для публікацій та публічних виступів.

Ступінь обґрунтованості та достовірності наукових положень, висновків та рекомендацій, що сформульовані в дисертації

Дисертаційне дослідження Бондаренка Микити Володимировича виконано на високому методичному рівні з використанням комплексу сучасних методів дослідження. Основні наукові положення та висновки, сформульовані в дисертації, логічно випливають з одержаних результатів та є достатньо обґрунтованими. Вони відповідають поставленій меті та завданням дослідження. Дисертаційну роботу виконано на достатньо обґрунтованому рівні. Чітко структуровано основні напрямки дослідження, зокрема питання розробки моделей та методів створення криптосистем на основі функцій дійсної змінної.

Результати експериментальних та теоретичних досліджень доповідались та обговорювались на міжнародних науково-технічних конференціях, а також опубліковані в наукових фахових виданнях. Про достовірність отриманих результатів свідчить їх взаємоузгодженість і позитивні результати комп'ютерного моделювання.

Наукова новизна результатів

В дисертаційній роботі отримано такі наукові результати:

1. Проаналізовано сучасний стан розвитку криптографічних систем і встановлено, що більшість розглянутих методів базуються на використанні множини цілих чисел. Розглянуті та підкреслені недоліки таких систем. Встановлено, що розвиток квантових комп'ютерів становить загрозу для багатьох криптографічних систем, що підштовхує до принципово інших математичних підходів до шифрування. За результатами аналізу аргументовано доцільність переходу від цілих до дійсних значень для побудови криптосистем, обґрунтовано вибір методу на основі використання функцій дійсної змінної в якості криптографічних ключів.

2. Удосконалені моделі та методи створення криптосистем на основі функцій дійсної змінної.

3. Уперше впроваджено метод використання інтегральних функцій непропорційності для дешифрування даних, що дозволяє визначати невідомі коефіцієнтів в сумі функцій дійсної змінної.

4. Уперше розроблено комбіновану криптосистему, що поєднує шифрування за допомогою суми функцій дійсної змінної та шифрування за допомогою інтегральної функції непропорційності.

5. Удосконалено метод шифрування даних шляхом впровадження додаткового елементу перестановки функцій-ключів.

6. Уперше розроблено криптосистему для захисту зображень на основі функцій дійсної змінної шляхом використання функцій інтегральної непропорційності, де інше довільне зображення використовується в якості криптографічного ключа.

7. Експериментально продемонстровано високу криптостійкість розроблених методів шифрування до атак грубої сили, через необхідність підбору значень ключа з високою точністю. Також продемонстровано високу здібність до декореляції значень шифротексту.

Практичне значення отриманих результатів

Розроблені моделі та методи криптографічного захисту на основі функцій дійсної змінної можуть бути використані для подальших досліджень в області альтернативних підходів до шифрування. Запропонована криптосистема для захисту зображень з використанням довільного зображення як ключа може бути застосована для експериментального захисту візуальної інформації в різних сферах. Створене програмне забезпечення для реалізації розроблених криптографічних алгоритмів може бути використане для проведення подальших досліджень та експериментів в області криптографії на основі

функцій дійсної змінної. Результати експериментальних досліджень криптостійкості розроблених методів можуть бути використані для порівняльного аналізу різних підходів до шифрування.

Повнота викладу матеріалів дисертації в опублікованих працях, персональний внесок здобувача

Основні результати дисертаційної роботи опубліковано в 10 наукових працях, зокрема 4 статті у наукових фахових виданнях України (у тому числі, одна стаття у виданні, що індексується міжнародною наукометричною базою Scopus), 4 публікації у збірниках матеріалів міжнародних конференцій та 2 патентах на корисну модель. Сукупність усіх публікацій відображає викладені в дисертації результати дослідження, що відповідає вимогам п. 8, 9 вимог до присудження ступеня доктора філософії «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», затвердженого Постановою Кабінету міністрів України №44 «Про затвердження Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії» від 22 січня 2022 року.

Оцінка мови та стилю дисертації

Матеріали дисертації викладено українською мовою, послідовно за формально-логічною структурою з дотриманням наукового стилю написання.

Відповідність фаху

Дисертаційна робота відповідає спеціальності 122 Комп'ютерні науки.

Відсутність (наявність) порушення академічної доброчесності.

За результатами перевірки дисертаційної роботи Бондаренка Микити Олеговича на тему «Моделі та методи інформаційної технології створення криптосистем на основі функцій дійсних змінних», на наявність ознак академічного плагіату встановлено коректність посилань на першоджерела для текстових та ілюстративних запозичень; навмисних спотворень не виявлено. Звідси можна зробити висновок про відсутність порушень академічної доброчесності.

Наукові праці, в яких опубліковані основні наукові результати дисертації:

[1] V. Avramenko and M. Bondarenko, "Recognition of Reference Signals and Determination of their Weighting Coefficients if an Additive

Interference Presents," *Radio Electronics, Computer Science, Control*, p. 73, Oct. 2023, doi: 10.15588/1607-3274-2023-3-8 (включена до Index Copernicus, BASE, Google Scholar, Ulrich's Periodicals Directory, WoS).

Автором розроблено методи комп'ютерного моделювання системи розпізнавання еталонного сигналу при накладанні завади, проведено аналіз результатів розпізнавання у випадках накладання частот

[2] V. Avramenko and M. Bondarenko, "Encryption of messages by the sum of a real variable functions." *Artificial Intelligence*, vol. 29, pp. 10–19, Jun. 2024, doi: 10.15407/jai2024.02.010. (включена до Google Scholar, ICI Journals Master List, Ulrich's Periodicals Directory, Journal Factor, World Cat, Academia Edu, Internet Archive, Autor AID, ACM Digital Library, Open Academic Journals Index, Info Base Index, The IAEA'S NUCLEUS).

Автором проведена розробка методу шифрування повідомлень сумою функцій дійсної змінною з застосуванням схеми перестановки функцій-ключів, розроблені методи комп'ютерного моделювання, проведений аналіз результатів на предмет декореляції шифротексту.

[3] V. Avramenko and M. Bondarenko, "Encrypting Images Using the Sum of the Functions of a Real Variable," *Transactions of Kremenchuk Mykhailo Ostrohradskyi National University*, vol. 144, no. 1, pp. 140–147, 2024, doi: 10.32782/1995-0519.2024.1.18. (включена до Ulrich's Web Global Serials Directory, Index Copernicus, Polish Scholarly Bibliography, Inspec, Open Academic Journals Index, Google Scholar і Scientific Indexing Services).

Автором розроблений спосіб застосування алгоритму шифрування повідомлень сумою функцій дійсної змінною для захисту візуальних даних, розроблені методи комп'ютерного моделювання.

[4] V. Avramenko and M. Bondarenko, "Image cryptosystem with image key using integral disproportion," *Radioelectronic and Computer Systems*, vol. 2024, pp. 147–159, Apr. 2024, doi: 10.32620/reks.2024.2.12. (включена до Scopus Q3).

Автором розроблені моделі та методи створення криптосистем для захисту зображення використовуючи інше зображення в якості криптографічного ключа, розроблені алгоритми шифрування та дешифрування зображення з використанням інтегральних функцій непропорційності, проаналізовані граничні випадки їх використання, розроблені моделі комп'ютерного моделювання, проведено верифікацію коректності роботи запропонованих методів, проаналізовано результати на предмет стійкості методу до атак грубої сили, проаналізовано здатності запропонованого метода до декореляції шифротексту.

[5] V. Avramenko and M. Bondarenko, "Using the Sum of Real Type Functions to Encrypt Messages," in *CEUR Workshop Proceedings*, 2021. Available: https://ceur-ws.org/Vol-3200/paper2.pdf

Автором проведена розробка методів дешифрування з використанням функцій інтегральної непропорційності першого порядку, розроблені методи комп'ютерного моделювання, проведена верифікація коректності роботи та аналіз результатів.

[6] V. Avramenko and M. Bondarenko, "Combined encryption system using the sum of functions of a real variable," presented at the The International Scientific and Technical Conferences of Students and Young scientists "Informatics. Mathematics. Automation," 2022, p. 71. Available: https://essuir.sumdu.edu.ua/bitstream-download/123456789/87782/1/Conf_IMA_2022.pdf

Автором розроблено моделі та методи поєднання шифрування сумою функцій дійсної змінної та функцією інтегральної непропорційності першого порядку.

[7] V. Avramenko and M. Bondarenko, "Signal recognition and calculation weighting coefficients in the presence of additive interference," presented at the The International Scientific and Technical Conferences of Students and Young scientists "Informatics. Mathematics. Automation," Sumy-Astana, 2023. Available: https://drive.google.com/file/d/1YDGNhbgZY6dfsqwN6P0BcEpcq6CuCKmj/view

Автором розроблено методи комп'ютерного моделювання системи розпізнавання еталонного сигналу при накладанні завади, проведено аналіз розпізнавання у випадках накладання частот

[8] V. Avramenko and M. Bondarenko, "Image encryption with key-image using integral disproportion," presented at the The International Scientific and Technical Conferences of Students and Young scientists "Informatics. Mathematics. Automation," 2024, pp. 38–39. Available: https://drive.google.com/file/d/1jjUd3KWmCmrPnOXTnZZSGbZIbsWWBPzU/view

Автором проведений аналіз існуючих методів шифрування зображень, розроблені моделі та методи створення криптосистем для захисту зображення використовуючи інше зображення в якості криптографічного ключа, розроблені алгоритми шифрування та дешифрування зображення з використанням інтегральних функцій непропорційності, розроблені моделі комп'ютерного моделювання, проведено верифікацію коректності роботи

запропонованої криптосистеми, проаналізовано результати на предмет стійкості до атак грубої сили, проаналізовано здатності запропонованого метода до декореляції шифротексту.

[9] V. Avramenko, M. Bondarenko, and T. Lavryk, "Спосіб шифрування даних за допомогою суми функцій дійсної змінної," 147560, Sep. 05, 2021 Available: https://essuir.sumdu.edu.ua/handle/123456789/85897

Автором проведена розробка моделі шифрування.

[10] V. Avramenko, M. Bondarenko, "Спосіб шифрування графічних зображень," 153107, May 24, 2023 Accessed: Sep. 04, 2024. [Online]. Available: https://essuir.sumdu.edu.ua/handle/123456789/92703

Автором розроблений спосіб застосування алгоритму шифрування повідомлень сумою функцій дійсної змінною для захисту візуальних даних, розроблені методи комп'ютерного моделювання.

Загальний висновок

Дисертаційна робота Бондаренка Микити Олеговича за актуальністю проблеми, методичними підходами, обсягом, ґрунтовністю аналізу та інтерпретацією отриманих даних, повнотою викладу принципових наукових положень, науково-теоретичним та практичним значенням повністю відповідає вимогам п. 6 «Порядку присудження ступеня доктор філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», затвердженого постановою Кабінету Міністрів України від 12 січня 2022 р. № 44, а дисертант, з урахуванням виконання у повному обсязі освітньої складової освітньо-наукової програми та індивідуального плану наукової роботи, заслуговує присудження ступеня доктора філософії з галузі знань 12 «Інформаційні технології» за спеціальністю 122 «Комп'ютерні науки».

Голова апробаційної ради
зі спеціальності 122 «Комп'ютерні науки»,
професор кафедри електроніки
та комп'ютерної техніки
доктор технічних наук, професор Олексій БОРИСЕНКО