Рішення
разової спеціалізованої вченої ради
про присудження ступеня доктора філософії

Здобувач ступеня доктора філософії Бондаренко Микита Олегович, 1997 року народження, громадянин України, освіта вища: закінчив у 2019 році Сумський державний університет за спеціальністю 122 «Комп'ютерні науки», виконав акредитовану освітньо-наукову програму «Інформатика» за спеціальністю 122 «Комп'ютерні науки».

Разова спеціалізована вчена рада, утворена наказом Сумського державного університету, м. Суми від 16 вересня 2024 року № 0858-І, у складі:

Голови разової
спеціалізованої вченої ради - Анатолій Довбиш, доктор технічних наук,
професор, професор кафедри комп'ютерних наук
Сумського державного університету

Рецензентів - В'ячеслав Москаленко, кандидат технічних наук, доцент, доцент кафедри комп'ютерних наук Сумського державного університету

Ольга Бережна, кандидат технічних наук, доцент, доцент кафедри електроніки і комп'ютерної техніки Сумського державного університету

Офіційних опонентів - Володимир Пєвнєв, доктор технічних наук, доцент,
професор кафедри комп'ютерних систем, мереж і кібербезпеки Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут»

Євген Котух, доктор наук з державного управління, професор, професор кафедри безпеки інформації та телекомунікацій Національного технічного університету "Дніпровська політехніка",

на засіданні «14» листопада 2024 року прийняла рішення про присудження ступеня доктора філософії з галузі знань 12 «Інформаційні технології» Микиті Олеговичу на підставі публічного захисту дисертації «Моделі та методи інформаційної технології створення криптосистем на основі функцій дійсних змінних» за спеціальністю 122 «Комп'ютерні науки»

Дисертацію виконано у Сумському державному університеті Міністерства освіти і науки України, міста Суми.

Науковий керівник Віктор Авраменко, доктор технічних наук, доцент, доцент кафедри комп'ютерних наук Сумського державного університету.

Дисертацію подано у вигляді спеціально підготовленого рукопису українською мовою, який містить нові науково обґрунтовані результати проведених здобувачкою досліджень, які виконують конкретне наукове завдання, що має істотне значення для галузі знань 12 «Інформаційні технології». Дисертація оформлена згідно з вимогами, встановленими Міністерством Освіти і Науки України. Максимальний та мінімальний обсяг основного тексту дисертації відповідає освітньо-науковій програмі закладу відповідно до специфіки галузі знань 12 «Інформаційні технології» та спеціальності 122 «Комп'ютерні науки». Вимоги пункту 6 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 від 12 січня 2022 року № 44 (зі змінами) дотримано.

Здобувач має 10 наукових публікації за темою дисертації, з них зокрема 4 статті – що включені до міжнародних наукометричних баз, з яких: 1 стаття **(Scopus, Q3)**, 3 статті у наукових фахових виданнях України, 4 публікацій у збірниках тез доповідей конференцій, 2 патенти на корисну модель відповідно до Вимог пунктів 8, 9 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 від 12 січня 2022 року № 44 (зі змінами) дотримано:

1. Avramenko V., Bondarenko M. Recognition of reference signals and determination of their weighting coefficients if an additive interference presents. Radio Electronics, Computer Science, Control, 2023. P. 73-82. Стаття у науковому фаховому виданні України категорії «А».
2. Avramenko V., Bondarenko M. Encryption of messages by the sum of a real variable functions. Artificial intelligence, 2024. № 29. P. 10–19. Стаття у науковому фаховому виданні України категорії «Б».
3. Avramenko V. Bondarenko M. Encrypting images using the sum of the functions of a real variable. Transactions of Kremenchuk Mykhailo Ostrohradskyi National University, 2024. № 144(1). P. 140–147. Стаття у науковому фаховому виданні України категорії «Б».
4. Avramenko V., Bondarenko M. Image cryptosystem with image key using integral disproportion. Radioelectronic and Computer Systems, 2024. № 2(110). P. 147–159. Стаття у науковому виданні, проіндексованому у базі даних Scopus Q3.

Наукові результати дисертації висвітлені у наукових публікаціях здобувачки. Статті відповідають темі дисертації, обґрунтовують отримані наукові результати відповідно до мети статті, поставленого завдання та висновків, а також опубліковані не більше ніж одна стаття в одному випуску (номері) наукового видання. Усі статті мають активний ідентифікатор DOI (Digital Object Identifier). Використання самоплагіату не виявлено.

У дискусії взяли участь голова, рецензенти, офіційні опоненти та висловили свою думку:

Москаленко В'ячеслав Васильович – рецензент, кандидат технічних наук, доцент, доцент кафедри комп'ютерних наук Сумського державного університету. В дисертаційній роботі автор вирішує актуальну проблему, удосконалює моделі та методи створення криптосистем на основі функцій дійсної змінної. Вперше в роботі запропоновано метод захисту даних з використанням інтегральних функцій непропорційності. Цей метод дозволяє визначати невідомі коефіцієнти в сумі функцій дійсної змінної, що є суттєвим внеском у теорію криптографії. Особливої уваги заслуговує вперше розроблена комбінована криптосистема, яка поєднує шифрування за допомогою суми функцій дійсної змінної та шифрування за допомогою інтегральної функції непропорційності. Нарешті, вперше розроблено криптосистему для захисту зображень на основі функцій інтегральної непропорційності. Особливим аспектом цієї системи є використання довільного зображення в якості криптографічного ключа. Це зображення легше непомітно передати приймальній стороні при використанні симетричних криптосистем. Крім того, зловмиснику буде складніше виявити зображення-ключ серед багатьох зображень, до яких він отримав доступ. Хоча дисертаційне дослідження загалом виконане на достатньо високому рівні, можна вказати декілька зауважень: Так, в роботі не вказані показники швидкодії запропонованих методів – час шифрування та дешифрування. Запропоновані методи мають певні недоліки: У методі шифрування сумою функцій, через вимоги до функцій-ключів, існує необхідність попередньо перевіряти коректність шифрування і дешифрування на всьому алфавіті повідомлення перед узгодженням нового ключа, що підвищує складність процесу. Не

розглянуто випадок, коли передається символ, в якому всі біти нульові – в такому разі, шифротекст відповідного символу теж буде нульовим. Дисертація є самостійним завершеним дослідженням, в якому отримано нові науково обґрунтовані результати, що в сукупності вирішують конкретне наукове завдання, яке має вагоме значення для комп'ютерних наук. Дисертація відповідає вимогам, а її автор, Бондаренко Микита Олегович заслуговує на присудження наукового ступеня доктора філософії.

Бережна Ольга Володимирівна – рецензент, кандидат технічних наук, доцент, доцент кафедри електроніки і комп'ютерної техніки Сумського державного університету. Дисертаційне дослідження Бондаренка М. О. присвячене актуальній темі розробки моделей та методів криптографічних систем на основі функцій дійсної змінної. Актуальність обраної тематики зумовлена комплексом факторів, що формують сучасні виклики у сфері інформаційної безпеки та криптографії. Сучасний стан розвитку інформаційних технологій характеризується стрімким прогресом у галузі обчислювальної техніки, що створює нові загрози для існуючих криптографічних систем. У дисертаційній роботі розв'язано важливу науково-практичну задачу створення моделей та методів криптографічних систем на основі функцій дійсної змінної. Вперше розроблено метод використання інтегральних функцій непропорційності для дешифрування даних, що дозволяє використовувати в криптосистемі дискретні функції-ключі. Також розроблено криптосистему, що поєднує шифрування за допомогою суми функцій дійсної змінної та шифрування за допомогою інтегральної функції непропорційності. 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. При загальній позитивній оцінці дисертаційного дослідження Бондаренка М. О., яке виконане на достатньо високому науковому рівні, варто відзначити деякі зауваження. В роботі не вказано кількісних метрик криптостійкості запропонованих методів. Наприклад, варто було б зазначити, який саме час і ресурси потрібні зловмиснику, щоб зламати цей шифр шляхом атаки грубої сили. Було б доречно додати в дисертаційну роботу таблиці та графіки порівняння характеристик запропонованих методів з іншими криптосистемами. Також, у методі шифрування зображення не шифрується перший піксель, що потенційно може призводити до вразливостей. Дисертація не має ознак порушення академічної доброчесності, вирішує поставлені проблеми та завдання та відповідає вимогам Постанови Кабінету Міністрів України № 44 від 12.01.2022 року «Про затвердження Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії». Автор заслуговує присудження ступеня доктора філософії за спеціальністю 122 «Комп'ютерні науки».

Пєвнєв Володимир Яковлевич – опонент, доктор технічних наук, доцент, професор кафедри комп'ютерних систем, мереж і кібербезпеки Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут». Актуальність роботи зумовлена подальшим розвитком штучного інтелекту та квантових комп'ютерів. Розвиток цих напрямків дозволяє досить швидко вирішувати переборні завдання, до яких можливо віднести і криптологічні. В сфері криптографії з'являються нові направлення, розвиток яких буде визначати шлях цих систем в майбутньому. Вказані особливості предметної області дослідження визначають актуальність теми роботи Бондаренка М. О. В якості новизни можна відмітити те, що поданий підхід, хоча і має певні вади, насправді є пост-квантовим. В даний час протидія новим технологіям криптоаналізу досягається завдяки збільшенню розміру ключа і розміру блоку, що обробляється. Теоретично подібний підхід ґрунтується на неможливості використання методу грубої сили при крипто аналізі. Як тільки буде збудовано відповідний комп'ютер, то криптосистема, заснована на переборі можливих варіантів, буде скомпрометована. При використанні запропонованого підходу, що ми розглядаємо, метод грубої сили просто не працює.

За структурою, мовою та стилем викладення дисертаційна робота відповідає вимогам МОН України. За структурою, мовою та стилем викладення дисертаційна робота відповідає вимогам МОН України. Порушень академічної доброчесності в дисертації та наукових публікаціях, у яких висвітлені основні наукові результати роботи, не виявлено. Наукові результати, які винесено здобувачем на захист, отримано самостійно і висвітлено в опублікованих роботах. Є наступні зауваження.

1. При аналізі криптоалгоритмів не було використано Національного стандарту шифрування ДСТУ 7624:2014 («Калина»).
2. При шифруванні тексту велику роль грають коефіцієнти k, які виробляються випадковим чином. Вимоги до генераторів у роботі не розглядалися. Залежно від використовуваних генераторів ПВЧ змінюватимемося і довжина зашифрованої послідовності, яка може у багато разів перевищувати розмітку елемента, що шифрується (8 біт). Це призводить до порушення однієї з вимог до сучасних криптосистем про не перевищення розміру шифрованої інформації.
3. На мій погляд було надмірним включення до тексту дисертаційної роботи параграфів, які показували роботу запропонованих алгоритмів для відновлення випадкового періодичного сигналу.
4. У роботі немає оцінки ефективності пропонованих алгоритмів для шифрування/розшифрування текстової інформації (розмір інформації, що передається, час шифрування/розшифрування) та їх порівняння з існуючими.
5. У роботі мають місце описки та неточності. Наприклад, стор. 20. «Більшість сучасних криптографічних систем, таких як AES та RSA, базуються на операціях з цілими числами»; стор. 99 «Отриманий шифротекст представляється у вигляді T одновимірних масивів y(j,i) …». У тексті роботи багаторазово використовується коефіцієнт k, з різним смисловим наповненням.
6. Є деякі зауваження до оформлення дисертаційної роботи.

Дисертаційна робота Бондаренка Микити Олеговича є завершеною науково-дослідною роботою, яка містить науково-обгрунтовані результати, має наукову новизну та дає перспективи подальших досліджень. Тематика проведених дослідження за змістом відповідає галузі знань 12 Інформаційні технології та спеціальності 122 Комп'ютерні науки.

Враховуючи актуальність теми, отримані результати та практичну значущість вважаю, що дисертаційна робота Бондаренка Микити Олеговича «Моделі та методи інформаційної технології створення криптосистем на основі функцій дійсних змінних» відповідає вимогам чинного законодавства України, що передбачені в п.6, 7, 8, 9 «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», від 12 січня 2022 р. № 44 зі змінами від 03.05 2024 р. (Постанова КМУ від №507) та вимогам до оформлення дисертації МОН України від 12.01.2017 № 40, сам автор, Бондаренко Микита Олегович, заслуговує присудження йому наукового ступеня доктора філософії зі спеціальності 122 Комп'ютерні науки.

Котух Євген Володимирович – доктор наук з державного управління, професор, професор кафедри безпеки інформації та телекомунікацій Національного технічного університету "Дніпровська політехніка". У дисертаційній роботі розв'язано науково-практичне завдання розробки моделей та методів криптографічних систем на основі функцій дійсної змінної. Тема дослідження обумовлена розвитком технологій квантових обчислень та зростанням ролі методів штучного інтелекту. Тандем цих технологій дозволяють значно прискорити розв'язання задач прямого перебору (brute-force) в практичних реалізаціях алгоритмів, в тому числі алгоритмів криптографічним примітивів. Це зумовлює появу нових напрямів, що визначатимуть розвиток криптоаналізу та зумовлюють актуальність роботи Бондаренко М.О. Автор розв'язав науково-прикладне завдання з розробки методів та алгоритмів криптосистем на основі функцій дійсних змінних, а також впровадив програмного забезпечення, що в продемонструвало застосовність отриманих теоретичних

результатів у практичній роботі. Результатами роботи стали нові наукові результати. До зауважень щодо змісту дисертаційної роботи можна віднести наступні: У роботі відсутні оцінки швидкодії пропонованих алгоритмів для шифрування/розшифрування візуальної інформації. Не наведені чисельні оцінки криптостійкості, які використовуються у випадку шифрування зображень (ентропія, UACI, NPCR, кореляція сусідніх пікселів). Відсутнє порівняння цих показників з наявними системами, особливо в контексті розвитку постквантової криптографії. У методі шифрування зображення шифрується лише візуальна складова зображення без метаданих. Розшифроване зображення є ідентичним до оригінального лише по-піксельно, а не по-байтово, що може породжувати додаткові виклики - наприклад, хеш-сума оригінального та розшифрованого файлів буде різною. Також, байтовий розмір розшифрованого зображення може перевищувати розмір оригінального зображення. У методі шифрування зображення не шифрується перший піксель, що потенційно може призводити до вразливості. У методі шифрування сумою функцій-ключів недостатньо формалізований підхід до створення функцій-ключів. Внаслідок появи помилок округлення даний метод вимагає узгодження числа, наближеного до нуля є при дешифруванні повідомлення. Водночас, дисертаційна робота Бондаренка Микити Олеговича є завершеною науково-дослідною роботою, що містить науково обґрунтовані результати, демонструє наукову новизну та відкриває перспективи для подальших досліджень. Тематика досліджень повністю відповідає галузі знань 12 «Інформаційні технології» та спеціальності 122 «Комп'ютерні науки». З огляду на актуальність теми, отримані результати та їх практичну значущість, вважаю, що дисертація Бондаренка Микити Олеговича на тему «Моделі та методи інформаційної технології створення криптосистем на основі функцій дійсних змінних» відповідає вимогам чинного законодавства України, визначеним у п. 6, 7, 8, 9 «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», від 12 січня 2022 року № 44 зі змінами від 03.05.2024 р. (Постанова КМУ № 507), а також вимогам до оформлення дисертації, затвердженим МОН України від 12.01.2017 № 40. Сам автор, Бондаренко Микита Олегович, заслуговує на присудження наукового ступеня доктора філософії зі спеціальності 122 «Комп'ютерні науки»

Довбиш Анатолій Степанович, голова разової спеціалізованої вченої ради, доктор технічних наук, професор, професор кафедри комп'ютерних наук Сумського державного університету. Колеги, хочу висловити свою підтримку здобувачу та відзначити високий рівень дисертаційного дослідження Бондаренка Микити Олеговича, яке присвячене актуальній проблематиці розробки криптографічних систем на основі функцій дійсної змінної. Тематика дисертації актуалізується щоденно, особливо в контексті стрімкого розвитку квантових обчислень та методів штучного інтелекту.

Варто підкреслити, що дана дисертаційна робота є, безумовно, цікавою і вирішує вагоме питання пошуку нових науково-методичних підходів у сфері криптографічного захисту даних. Особливо треба відзначити, що дисертант не просто розвиває існуючі підходи, а пропонує нові рішення, зокрема: вперше запропоновано метод захисту даних з використанням інтегральних функцій непропорційності, що відкриває новий напрямок у криптографії; розроблено оригінальну комбіновану криптосистему, яка органічно поєднує різні підходи до шифрування; створено криптосистему для захисту зображень, де криптографічним ключем виступає інше довільне зображення. Дисертація створює широке поле для подальших досліджень - можна розробляти нові модифікації запропонованих методів, досліджувати їх властивості, розширювати сфери застосування. Вважаю, що дисертація Бондаренка Микити Олеговича є завершеною науково-дослідною роботою зі спеціальності 122 «Комп'ютерні науки», а сам автор заслуговує присудження йому наукового ступеня доктора філософії.

Результати відкритого голосування:

«За» 5 членів ради,

«Проти» 0 членів ради.

На підставі результатів відкритого голосування разова спеціалізована вчена рада присуджує Микиті Бондаренку ступінь доктора філософії з галузі знань 12 «Інформаційні технології» за спеціальністю 122 «Комп'ютерні науки»

Відеозапис трансляції захисту дисертації додається.

Голова разової спеціалізованої вченої ради _____ Анатолій Довбиш
(підпис)

М.П.