ВІДГУК
ОФІЦІЙНОГО ОПОНЕНТА
Казакової Надії Феліксівни,
доктора технічних наук, професора,
завідувачки кафедри інформаційних технологій
Одеського національного університету імені І.І. Мечникова
на дисертаційну роботу
Хамітова Віталія Миколайовича
на тему «Моделі та методи підвищення конфіденційності та цілісності обміну зображеннями для групи довірених користувачів», що представлена на здобуття наукового ступеня доктора філософії за спеціальністю 122 – Комп'ютерні науки галузь знань 12 – Інформаційні технології

1. Актуальність теми дисертації

У професійному сегменті світового медіатрафіку значне місце займають зображення високої роздільної здатності, що характерно для таких областей, як супутниковий моніторинг, телемедицина та криміналістична експертиза. Дані, що передаються по відкритих каналах зв'язку, вимагають надійного захисту від несанкціонованого доступу і високої швидкості передачі в режимі реального часу. Однак на практиці досягнення високої швидкості при надійному шифруванні стикається із серйозними обмеженнями. Незважаючи на численні дослідження в галузі захисних перетворень, використання сучасних методів обмежене їхньою високою ресурсоємністю та залежністю від програмно-апаратної платформи. Це створює суперечність між високою затребуваністю методів захисту (зокрема, на основі хаотичних відображень) та жорсткими вимогами до їхньої швидкодії. Вирішення даної суперечності і обумовлює актуальність теми дослідження.

2. Структура та обсяг дисертації

Дисертація складається з вступу, чотирьох розділів, висновків, списку використаних джерел і додатків. Повний обсяг дисертації складає 200 сторінок. Робота містить 53 рисунки, 6 таблиць та 7 додатків. список використаних джерел зі 102 найменувань.

У **вступі** наведено загальну характеристику дисертаційної роботи, обґрунтовано актуальність досліджуваної проблеми, сформульовано мету,

об’єкт і предмет дослідження, визначено основні завдання, методи дослідження, наукову новизну та практичне значення отриманих результатів. Також у вступі подано відомості про апробацію результатів дослідження та їх впровадження.

У **першому розділі** дисертації здійснено систематичний аналіз сучасних підходів до рішення актуальної науково-практичної задачі підвищення конфіденційності та цілісності обміну цифровими зображеннями для групи довірених користувачів. Досліджено існуючі рішення, їх основні характеристики та тенденції розвитку. За результатами аналізу обґрунтовано необхідність розроблення нових моделей і методів обміну зображеннями, які були б більш надійними, захищеними і швидкодіючими. Сформульовано мету і завдання дослідження.

У **другому розділі** запропоновано новий підхід для генерації довгих псевдохаотичних послідовностей. Розроблено метод шифрування зображень на основі хаотичного відображення Tent з управлінням, перевагою якого є коротка довжина ключа, що передається, та незалежність алгоритму від застосовуваної апаратно-програмної платформи.

Для комплексного оцінювання якості шифрування та обґрунтованого вибору потокових та блочних шифрів запропоновано інтегральний критерій якості шифрування.

У **третьому розділі** отримані формули представлення згорнутих чисел k-перетину послідовності Фібоначчі та визначені властивості цієї послідовності, знайдені нові зв'язки між елементами послідовності та знайдені формули типу Біне для згорнутих чисел. У розділі проведено дослідження послідовності згорнутих чисел k-перетину послідовності Фібоначчі як генератора псевдовипадкових чисел та показано, що послідовність може бути використаною для створення високоякісних паролів довірених користувачів. Слід відмітити, що отримані послідовності є оригінальними і представлені в енциклопедії OEIS.

У **четвертому розділі** розроблено метод обміну конфіденційними зображеннями групи довірених користувачів із застосуванням псевдовипадкових послідовностей на основі модифікованого хаотичного відображення Тент.

Розроблено протокол формування групи довірених користувачів, яким дозволено доступ до зображень. Збереження зображень забезпечується шістьма рівнями захисту. Протокол ґрунтується на застосуванні операцій на еліптичних кривих Монтґомері.

Запропоновано методику дослідження ефективності протоколів групового узгодження ключів.

Наведено результати апробації розробленої програмної системи, підтверджено її практичне значення та ефективність.

У загальних **висновках** узагальнено основні наукові та практичні результати дисертаційного дослідження, сформульовано підсумкові висновки та визначено напрями подальших досліджень.

У додатках наведено матеріали, що доповнюють основний зміст роботи, зокрема акти впровадження результатів дисертаційного дослідження, довідки про використання результатів у навчальному процесі, фрагменти програмного коду, перелік наукових публікацій здобувача та відомості про апробацію результатів дисертаційної роботи.

3. Ступінь обґрунтованості наукових положень, висновків і рекомендацій

Наукові положення, висновки та рекомендації, сформульовані у дисертаційній роботі, є обґрунтованими, оскільки ґрунтуються на аналізі сучасних і рейтингових наукових джерел у галузях дискретної математики, криптоаналізу, цифрової обробки зображень, математичної статистики та оптимізаційних методів. Використані теоретичні підходи відповідають сучасному стану розвитку комп’ютерних наук і широко застосовуються у наукових та прикладних дослідженнях.

Достовірність отриманих наукових результатів підтверджується результатами комплексних експериментальних досліджень, проведених на реальних і синтетично сформованих зображеннях з використанням метрик оцінювання якості моделей. Узгодженість теоретичних положень із результатами експериментів свідчить про коректність запропонованих підходів та їх придатність для розв’язання практичних задач обміну зображеннями для груп довірених користувачів,

Обґрунтованість наукових положень, висновків і рекомендацій також забезпечується коректним застосуванням математичного апарату, використанням сучасних методів комп’ютерного моделювання та аналізу даних, а також результатами практичної апробації розроблених методів і моделей. Практичні результати дослідження підтверджені актами впровадження, які наведені у додатках до дисертаційної роботи.

4. Практична значимість розроблених моделей та методів

Практична значимість дослідження підтверджується використанням результатів при організації обміну зображеннями для груп довірених користувачів. Розроблені моделі та методи реалізовані у вигляді програмних компонентів, що забезпечують захисне шифрування, передачу та дешифрування зображень. Це дозволяє застосовувати розроблені рішення у практичних сценаріях обміну зображеннями, а також інтегрувати їх у існуючі інструментальні засоби безпеки.

Розроблена в дисертаційній роботі модель побудови псевдовипадкових послідовностей дозволяє отримати сімейство узагальнених послідовностей Фібоначчі, які можуть бути використані для підвищення рівня забезпечення цілісності інформації для широкого кола завдань криптографічного захисту інформації. Отримані послідовності є оригінальними.

Використання розроблених підходів сприяє підвищенню швидкодії шифрування та розшифрування при збереженні стійкості цифрових зображень групи довірених користувачів.

Розроблені в роботі наукові положення та практичні результати отримали впровадження у діяльності державного підприємства «Український науково-дослідний інститут медицини транспорту Міністерства охорони здоров'я України», у діяльності Військово-медичного клінічного центру Південного регіону та знайшли відображення у навчальному (Додаток Д) та у науково-дослідницькому процесі Національного університету «Одеська політехніка». Це підтверджує їх практичну придатність та ефективність.

5. Новизна наукових положень, висновків та рекомендацій

Наукова новизна результатів дисертаційного дослідження така:

– удосконалено інтегральний критерій якості захисних перетворень, який поєднує різні метрики якості шифрування (кореляційні, ентропійні та метрики резистентності), що побудований методом ідеальної точки, що дозволило проводити комплексне оцінювання якості шифрування та проводити обґрунтований вибір потокових та блочних шифрів;

– запропоновано метод захисного перетворення зображень на основі хаотичного відображення Тент з управлінням, що дозволило на підставі короткого ключа (насіння) згенерувати довгу псевдовипадкову послідовність, що значно підвищило швидкодію шифрування та дешифрування при збереженні стійкості шифрування за інтегральним критерієм якості;

– отримала подальший розвиток модель побудови псевдовипадкових послідовностей, яка заснована на зв'язку між похідними поліномів Чебишева другого роду та поліномами Чебишева, а також на зв'язку згорнутих чисел k-перетину послідовності Фібоначчі з похідними поліномів Чебишева другого роду через числа Люка, що дало можливість отримати сімейство узагальнених послідовностей Фібоначчі, які можуть бути використані для підвищення рівня забезпечення цілісності інформації при її обміні у групі довірених користувачів;

– розроблено метод обміну зображеннями групи довірених користувачів, який відрізняється багаторівневим захистом з застосуванням захистного перетворння на основі модифікованого хаотичного відображення Тент та швидкодіючого протоколу на основі еліптичних кривих Монтґомері, що дозволило підвищило швидкодію шифрування та дешифрування при збереженні стійкості.

Сформульовані положення наукової новизни тісно пов’язані з тематикою та метою дисертаційної роботи, отримані результати повністю досягнуті, а рівень методологічної підготовки здобувача відповідає вимогам до виконання самостійного наукового дослідження.

6. Рекомендації щодо використання результатів дисертації

Розроблені у дисертаційній роботі моделі та методи доцільно використовувати в інформаційних системах, де обмін даними, в тому числі і зображеннями, по відкритим каналам потребує забезпечення конфіденційності та цілісності у режимі реального часу.

Розроблені теоретичні підходи мають високий потенціал та можуть бути застосовані:

– дискретна динамічну систему, а саме узагальнене відображення Тент з керуванням, для шифрування даних, наприклад, зображень та захисту інформації від несанкціонованого доступу;

– сімейство узагальнених послідовностей зі зростанням вищого порядку і складнішими коефіцієнтами зв'язку ніж у відомих послідовностей Фібоначчі є перспективними для стиснення розріджених даних, вирішення низки завдань у сфері перетворення інформації при підвищенні надійності інформаційних систем.

Отримані результати доцільно використовувати при розробці методів захисних перетворень зображень, що ґрунтуються на хаотичних для підвищення

конфіденційності та цілісності обміну зображеннями для групи довірених користувачів.

Крім того, матеріали та результати дисертаційної роботи можуть бути використані в освітньому процесі під час викладання дисциплін, пов'язаних із дискретною математикою, захисними перетвореннями інформації, розробкою сучасних протоколів обміну зображеннями у інформаційних системах, а також у науково-дослідній роботі студентів і аспірантів.

7. Повнота викладу в наукових публікаціях, зарахованих за темою дисертації, відсутність порушення академічної доброчесності

Основні наукові положення та практичні результати дисертаційного дослідження були апробовані і обговорені на міжнародних та всеукраїнських науково-практичних конференціях, зокрема: на XI Міжнародній науково-практичній конференції «ІНФОРМАТИКА. КУЛЬТУРА. ТЕХНІКА» «ІКТ-25»; на 8-й Міжнародній науково-практичній конференції «Global Directions in Scientific Research and Technological Development» (квітень 2026, Валенсія, Іспанія); на Міжнародній науково-практичній конференції (квітень 2026, Дубай ОАЕ; на 2-й Міжнародній науково-практичній конференції (квітень 2026, Харків-Яремче); на XVI Міжнародній науковій конференції «Modern Information Technology – 2026» (травень 2026, Одеса); на 5^{th} Міжнародній науково-практичній конференції "Modern technologies of biomedical engineering" (травень 2026, Одеса).

Участь у зазначених наукових заходах сприяла удосконаленню отриманих результатів, а також підтвердила їх наукову актуальність.

Основні результати дисертаційної роботи викладено у 13 наукових публікаціях, серед яких статті у фахових виданнях України категорій «А» та «Б», зарубіжні наукові журнали, що індексуються у міжнародних наукометричних базах, а також тези доповідей міжнародних наукових конференцій. Таким чином, вимоги щодо кількості та рівня наукових публікацій за темою дисертації виконано у повному обсязі.

Публікація результатів дослідження у рецензованих наукових виданнях і матеріалах конференцій, які передбачають попередню перевірку рукописів на наявність запозичень, є підтвердженням дотримання здобувачем принципів академічної доброчесності. Аналіз змісту дисертаційної роботи та відповідних публікацій свідчить про відсутність порушень академічної доброчесності.

8. Зауваження згідно змісту та оформлення дисертаційної роботи

1. В 1-му розділі слід було додати обговорення 2D хаотичних відображень, провести їх порівняльний аналіз і чітко спрямувати дослідження на одновимірні відображення.

2. Виглядає недостатньо обґрунтованим використання автором в якості основного шифру Вернама на тлі багаточисельних сучасних швидкодіючих потокових шифрів.

3. Розділ 3 містить детальну і змістовну модель побудови псевдовипадкових послідовностей на основі згорнутих чисел k-перетину послідовності Фібоначчі, демонструється її висока якість. Але далі розроблена модель зустрічається лише в кінці розділу 4. Виникає питання: чому розроблена модель не використовувалася на основних етапах шифрування.

4. Розроблений в розділі 4 метод оперативного обміну конфіденційними зображеннями для групи довірених користувачів включає шість рівнів захисту зображень, слід було б виділити серед них головні і другорядні.

5. У тексті дисертаційної роботі присутні певні граматичні, стилістичні та термінологічні неточності.

Наведені зауваження не впливають на загальну позитивну оцінку дисертаційної роботи та не знижують її наукової новизни і практичної цінності.

9. Загальний висновок

В цілому вважаю, що дисертаційна робота Хамітова Віталія Миколайовича «Моделі та методи підвищення конфіденційності та цілісності обміну зображеннями для групи довірених користувачів», є завершеною кваліфікаційною науковою роботою, яка має наукову новизну та практичне значення, тема і зміст якої відповідає спеціальності 122 «Комп’ютерні науки».

Вона містить незахищені раніше наукові положення і нові науково обґрунтовані результати в галузі комп’ютерних наук. Отримані результати можуть бути рекомендовані до використання у науково- дослідних установах, організаціях та компаніях, що займаються питанням підвищення конфіденційності та цілісності обміну зображеннями по відкритих каналах зв’язку, а також у навчальному процесі закладів вищої освіти.

Дисертаційна робота «Моделі та методи підвищення конфіденційності та цілісності обміну зображеннями для групи довірених користувачів» за своїм змістом відповідає вимогам «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти,

наукової установи про присудження ступеня доктора філософії», затвердженому Постановою Кабінету Міністрів України від 12 січня 2022 р. No44, а її автор Хамітов Віталій Миколайович заслуговує на присудження йому наукового ступеня доктора філософії за спеціальністю 122 – Комп'ютерні науки, галузь знань 12 – Інформаційні технології.

Офіційний опонент,
доктор технічних наук, професор,
завідувачка кафедри інформаційних технологій
Одеського національного університету
імені І.І. Мечникова Надія КАЗАКОВА