РЕЦЕНЗІЯ

офіційного рецензента, кандидата технічних наук, доцента, доцента кафедри комп'ютеризованих систем та програмних технологій Навчально-наукового інституту комп'ютерних систем Національного університету «Одеська політехніка» Сперанського Віктора Олександровича на дисертаційну роботу здобувача Хамітова Віталія Миколайовича на тему «Моделі та методи підвищення конфіденційності та цілісності обміну зображеннями для групи довірених користувачів», що подану до захисту в разову спеціалізовану вчену раду Національного університету «Одеська політехніка» Міністерства освіти і науки України 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 (супутникова передача, телемедицина, криміналістика) постійно зростає обсяг зображень високої роздільної здатності. Передача таких даних по відкритих каналах вимагає забезпечення їхньої конфіденційності у режимі реального часу.

Існуючі методи захисних перетворень (шифрування) зображень не завжди здатні забезпечити необхідний баланс між надійністю та швидкістю. Їх застосування обмежується як вимогами до безпеки, а й високими показниками ресурсоємності і залежність від програмно-апаратної реалізації. Таким чином, виникає суперечність між високою потребою в ефективних методах шифрування (включаючи методи на основі хаотичних відображень) та обмеженнями щодо їх швидкодії в реальних умовах. Необхідність розв'язання цієї суперечності визначає актуальність цього дослідження.

Тому дисертаційна робота Хамітова Віталія Миколайовича, яку направлено на усунення цієї суперечності та присвячено вирішенню важливої науково-практичної задачі підвищення конфіденційності та цілісності обміну зображеннями для групи довірених користувачів, є актуальною та відповідає сучасним потребам розвитку інформаційних технологій.

2. Ступінь обґрунтованості наукових положень, висновків і рекомендацій сформульованих у дисертації

Наукові положення та висновки, викладені у дисертаційній роботі,

сформульовано на основі цілісної методології дослідження. Обрані методи дослідження відповідають поставленим завданням і забезпечують коректне розв’язання поставлених задач. Математичний і алгоритмічний апарат, використаний у роботі, узгоджується з загальноприйнятими підходами в галузі комп’ютерних наук і базується на перевірених концепціях. Усі припущення, які покладено в основу запропонованих моделей, є чітко визначеними, внутрішньо несуперечливими та такими, що не виходять за межі сучасних наукових уявлень. Вагомим аргументом на користь обґрунтованості отриманих результатів є їх систематична перевірка в ході експериментальних досліджень. Отримані експериментальні дані узгоджуються з теоретичними положеннями роботи та підтверджують доцільність запропонованих підходів. З урахуванням наведеного можна зробити висновок, що наукові положення, висновки та рекомендації дисертаційної роботи є методологічно виваженими, логічно обґрунтованими та підтвердженими результатами експериментальної перевірки.

3. Наукова новизна одержаних результатів

Наукові завдання дослідження сформульовано на основі детального аналізу сучасної фахової та періодичної наукової літератури відповідно до тематики роботи. Наукова новизна результатів дисертаційного дослідження полягає у наступному:

- 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 захисного перетворення на основі модифікованого хаотичного відображення Тент та швидкодіючого протоколу на основі еліптичних кривих Монтґомері, що дозволило підвищило швидкодію шифрування та дешифрування при збереженні стійкості.

Положення, що визначають наукову новизну та виносяться на захист, сформульовані з урахуванням тематики дослідження, узгоджуються з метою дисертаційної роботи та реалізовані у повному обсязі, що свідчить про належний рівень володіння здобувачем методологією наукової діяльності.

4. Повнота викладення результатів дисертації в опублікованих працях

Результати дисертаційного дослідження послідовно відображені в опублікованих наукових працях здобувача, які охоплюють усі ключові напрями та етапи виконаної роботи. Публікації відображають розвиток основних наукових ідей дисертації – від постановки задачі та вибору методів до аналізу отриманих результатів і формулювання узагальнених висновків. Аналіз змісту наукових праць і внеску здобувача свідчить, що результати, винесені на захист, отримані ним особисто впродовж 2024-2026 років та систематизовані при підготовці дисертаційної роботи. Основні положення дисертації апробовані у 13 публікаціях, зокрема 6 статей, з них – 4 статті у фахових періодичних виданнях України з технічних наук, з яких 2 – у категорії А (індексується в Scopus); 2 – у категорії Б, 2 статті у інших виданнях, 7 тез доповідей у матеріалах міжнародних наукових конференцій. Загалом обсяг і характер публікацій свідчать про достатню повноту викладення результатів дисертаційного дослідження та їх відповідність вимогам до робіт освітньо-наукового рівня.

5. Значення роботи для науки та практики

Одержані у дисертаційній роботі результати мають вагоме значення для розвитку наукових підходів у галузі безпеки обміну інформацією. Запропоновані методи та моделі доповнюють існуючі дослідження у сфері захисних перетворень зображень для забезпечення їх конфіденційності та цілісності при обміні зображеннями для групи довірених користувачів. Практична цінність роботи полягає у можливості застосування отриманих результатів у реальних інформаційних системах, де є затребуваним забезпечення конфіденційності обміну зображеннями для групи довірених користувачів, наприклад, у таких галузях як інтернет речей, супутникова передача, телемедицина, криміналістика, військове забезпечення тощо. Розроблені рішення реалізовані у формі програмних компонентів, придатних для інтеграції. Практична придатність результатів

підтверджується їх використанням у діяльності державного підприємства «Український науково-дослідний інститут медицини транспорту Міністерства охорони здоров'я України», у діяльності Військово-медичного клінічного центру Південного регіону, у навчальному та науково-дослідницькому процесі Національного університету «Одеська політехніка». Це довело ефективність запропонованих рішень.

6. Відсутність (наявність) порушення академічної доброчесності

Дисертація містить результати власних досліджень автора. Всі використані ідеї, результати і текст інших авторів мають посилання на відповідне джерело. Фактів порушення академічної доброчесності в дисертації здобувача не виявлено.

7. Дискусійні положення та зауваження щодо змісту дисертації

До роботи є наступні дискусійні положення та зауваження:

- доцільно було б навести більш розширене пояснення щодо використання еліптичних кривих Монтґомері в контексті загальної архітектури запропонованого протоколу;
- бажано розширити опис програмної реалізації алгоритму на базі хаотичного відображення Тент, зокрема в частині роботи з типами даних із плаваючою комою;
- обґрунтування вибору вагових коефіцієнтів для інтегрального критерію якості (с. 95) потребує більшої формалізації, оскільки посилання на «досвід моделювання» без наведення відповідного математичного апарату чи статистичних даних знижує відтворюваність результатів;
- при порівнянні зі стандартом DICOM доцільно було б додатково виділити специфічні сценарії, де запропонований метод має переваги над класичними підходами;
- результати оцінки підвищення швидкодії виглядали б більш переконливо, якби було наведено детальніший опис конфігурації тестового стенду;
- використання автором в 4-му розділі роботи багаточисельних англомовних термінів упереміш з українськими ускладнює сприйняття викладеного;
- в заключному розділі дисертації слід було б окреслити обмеження розроблених моделей і методів.

Зазначені зауваження мають дискусійний характер, не впливають на загальну позитивну оцінку дисертаційної роботи та не знижують наукової і практичної цінності отриманих результатів.

8. Загальний висновок про відповідність роботи встановленим вимогам

Дисертаційна робота Хамітова Віталія Миколайовича на тему «Моделі та

методи підвищення конфіденційності та цілісності обміну зображеннями для групи довірених користувачів» є логічно завершеним, самостійно виконаним науковим дослідженням, що характеризується цілісністю викладу та науково-прикладною спрямованістю. Тема та зміст роботи повністю відповідають вимогам спеціальності 122 – Комп'ютерні науки.

Беручи до уваги актуальність обраної тематики, рівень обґрунтованості наукових положень, висновків і рекомендацій, їх наукову новизну та практичну значущість, повноту відображення результатів у наукових публікаціях, а також відсутність порушень принципів академічної доброчесності, можна зробити висновок, що дисертаційна робота відповідає вимогам «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 із змінами. У зв'язку з цим автор роботи, Хамітов Віталій Миколайович, заслуговує на присудження наукового ступеня доктора філософії у галузі знань 12 – Інформаційні технології за спеціальністю 122 – Комп'ютерні науки.

Офіційний рецензент:
кандидат технічних наук,
доцент кафедри комп'ютеризованих систем
та програмних технологій
навчально-наукового інституту
комп'ютерних систем
Національного університету
«Одеська політехніка» Віктор СПЕРАНСЬКИЙ