ВІДГУК

рецензента – доцента кафедри безпеки інформаційних технологій
Національного університету «Львівська політехніка»,
к.т.н, доцента Коробейнікової Тетяни Іванівни
на дисертаційну роботу
Кулини Сергія Васильовича
«Методи та алгоритми захищеного розподіленого зберігання даних на основі надлишкової системи залишкових класів»,
поданої на здобуття наукового ступеня доктора філософії
за спеціальністю 125 «Кібербезпека» (галузь знань 12 «Інформаційні технології»)

Актуальність теми дисертації.

Системи зберігання даних відіграють ключову роль у забезпеченні доступності та цілісності інформації. Завдяки чому дані можуть бути збережені на тривалий термін, упорядковані та організовані таким чином, щоб вони були доступні для потрібних осіб у будь-який момент, що особливо важливо в сучасному світі, де великі обсяги даних збираються з різних джерел, а їхня ефективна організація та доступність допомагають приймати важливі рішення в реальному часі. Одним із завдань систем зберігання даних є забезпечення надійності та конфіденційності даних. Коригуючі коди є однією із ключових складових сучасних систем зберігання та передачі даних. Вони використовуються для виявлення та виправлення помилок, а отже, забезпечують надійність зберігання даних. Система залишкових класів (СЗК) є одним з прикладів коригуючих кодів і базується на додаванні додаткових символів до вихідних даних та застосовується для перевірки цілісності і виявлення помилок.

У дисертаційній роботі Кулини Сергія Васильовича досліджується розробка та удосконалення існуючих методів і алгоритмів, що дозволить підвищити захищеність та надійність систем зберігання даних на основі надлишкової системи залишкових класів.

Зв'язок теми дисертації з науковими програмами, планами і темами.

Наведені у дисертації дослідження виконувались автором у відповідності до наукового напряму кафедри кібербезпеки Західноукраїнського національного університету. Тема дисертаційного дослідження відповідає пріоритетним напрямкам науково-дослідних робіт відповідно до координаційних планів Міністерства освіти і науки України та виконувалася в рамках наукових досліджень держбюджетних науково-дослідних робіт «Теоретичні основи та

апаратні засоби підвищення продуктивності роботи безпровідних сенсорних мереж» (№ державної реєстрації 0117U000414) та з виконання завдань Перспективного плану розвитку наукового напряму «Технічні науки» ЗУНУ (1 етап: «Розробка методів та алгоритмів захищеного зберігання даних», 2 етап: «Розвиток систем підтримки рішень, керованих моделями та даними, в умовах невизначеності», № державної реєстрації 0121U114705), а також, госпдоговірних тем «Розробка алгоритмів надійного розподіленого зберігання даних на основі модулярних коригуючих кодів» (№ державної реєстрації 0118U100457) та «Методи та алгоритми захищеного зберігання даних на основі кодів системи залишкових класів» (№ державної реєстрації 0121U107651).

Наукова новизна результатів дисертаційного дослідження:

- Здобувачем **вперше** розроблено метод надійного зберігання даних на основі коригуючих кодів надлишкової системи залишкових класів. Розроблений метод, у порівнянні з відомими, базується на використанні одного перевірочного символу та обчисленні значення геш-функції від файлів залишків, а його використання дозволило зменшити надлишковість на 33% у порівнянні з використанням коригуючих кодів системи залишкових класів.
- **Вперше** отримано аналітичні вирази для оцінки криптографічної стійкості шифрування даних в системі залишкових класів із врахуванням мінімальної довжини файлу. Використання зазначених аналітичних виразів дало змогу здобувачу встановити оптимальні значення модулів для реалізації захищеного розподіленого зберігання даних в залежності від поставлених завдань.
- Здобувачем **удосконалено** метод шифрування даних в системі залишкових класів шляхом циклічного зсуву позицій залишків з використанням в якості ключа псевдовипадкових послідовностей, що підвищує криптографічна стійкість при заданій розрядності модулів в середньому у три рази.

Ступінь обґрунтованості наукових положень та висновків дисертації та їх достовірність.

При вирішенні поставлених у дисертації задач, створенні наукових положень, висновків та рекомендацій здобувач застосовував дані, що одержані з літературних джерел, з результатів аналізу сучасного стану та перспектив розвитку методів і алгоритмів підвищення захищеності та надійності зберігання даних. Наведені в дисертації результати є достатньо обґрунтованими, що підтверджується даними розрахунків, експериментальних досліджень та

практичними результатами та актами впровадження.

Наукове значення виконаного дослідження.

Отримані здобувачем наукові положення, висновки та практичні результати можуть бути використані при розробці систем зберігання даних на основі надлишкової системи залишкових класів, а також, є значущими для галузі 12 «Інформаційні технології» та спеціальності 125 «Кібербезпека».

Практичне значення одержаних результатів.

Практичне значення одержаних результатів полягає у розробці методу кодування даних на основі надлишкової системи залишкових класів та шифрування вмісту файлів згідно М-послідовності. Побудова прототипу системи захищеного розподіленого зберігання даних дозволила здобувачу виявити та підтвердити переваги запропонованих у роботі методів.

Повнота оприлюднення результатів дисертаційної роботи.

Результати дисертації доповідалися здобувачем та обговорювались на міжнародних науково-практичних та науково-технічних конференціях, що викладено у 15 публікаціях, з них: 4 статі у наукових фахових виданнях України та 11 публікацій у матеріалах та збірниках доповідей наукових конференцій, з яких дві індексуються у наукометричних базах даних Scopus та Web of Science.

Короткий аналіз структури та змісту дисертаційної роботи.

Дисертаційна робота викладена на 203 сторінках та складається із анотації, змісту, переліку скорочень, вступу, п'яти основних розділів, висновків, списку використаних джерел та додатків.

Дисертація написана українською мовою на достатньому мовно-стилістичному рівні, а стиль викладення матеріалу є послідовним та логічним. За своєю структурою, мовою та стилем викладення вона відповідає вимогам МОН України.

У вступі здобувачем обґрунтовано актуальність теми дисертаційного дослідження, сформульовано мету дослідження та науково-прикладні завдання, необхідні для її досягнення, показано зв'язок дослідження з науковими програмами та темами, наведено наукову новизну отриманих результатів, їх практичну цінність та особистий внесок.

У першому розділі проведено аналіз існуючих методів програмного та апаратно-програмного захисту інформації.

У другому розділі досліджено існуючі методи виявлення та виправлення помилок у системах зберігання даних а також, запропоновано метод

захищеного зберігання даних на основі надлишкової системи залишкових класів та геш-функції.

У третьому розділі обґрунтовано вибір оптимального набору модулів для реалізації систем захищеного зберігання даних та досліджено криптографічну стійкість подання даних у системі залишкових класів. Запропоновано для оцінки криптографічної стійкості методу шифрування даних враховувати розмір файлів залишків, оскільки при перехопленні повідомлення зловмиснику невідомі розрядності обраних модулів. А, для підвищення рівня криптографічної стійкості алгоритму шифрування на основі системи залишкових класів запропоновано удосконалення методу шифрування шляхом зміни позицій залишків із використанням в якості секретного ключа М-послідовності.

У четвертому розділі розроблено алгоритми кодування в системі залишкових класів, шифрування та зберігання залишків, на основі яких реалізована захищена система зберігання даних. Описано додаткові умови зберігання залишків на фізичних носіях та виведено математичні формули обчислення кількості помилок в залежності від кількості файлів залишків з підтвердженою цілісністю. Визначено залежність ефективності відновлення файлу від кількості помилок при різній кількості пошкоджених файлів залишків.

У п'ятому розділі розроблено архітектуру системи розподіленого захищеного зберігання даних. Наведено схеми модулів, що забезпечують функціонування розробленої системи та представлено прототип програмного продукту.

У загальних висновках дисертаційної роботи сформульовано основні результати дисертаційної роботи, які узгоджуються з метою та завданнями дослідження.

Список використаних джерел містить 124 найменувань.

У додатках представлено:

- алгоритми та типи шифрування поширених програмних продуктів;
- набори оптимальних модулів для проектування систем зберігання даних на основі СЗК;
- програмний код реалізації системи розподіленого захищеного зберігання даних;
- акти про впровадження результатів дисертаційної роботи.

Зауваження та дискусійні положення щодо змісту дисертації.

1) У першому розділі автором не в повній мірі висвітлено атаки на дані та методи захисту від них.
2) У висновках до розділів 2 та 3 доцільно навести конкретні чисельні

значення та переваги розроблених методів у порівнянні з існуючими.

3) При дослідженні криптографічної стійкості розробленого методу автор розглядає лише атаки грубої сили та не згадує про інші.
4) Наведені у пункті 3.1 таблиці дублюються у додатку Б.
5) У тексті представленої роботи зустрічається ряд стилістичних і орфографічних неточностей.

Слід зауважити, що зазначені зауваження не знижують загальної позитивної оцінки дисертаційної роботи.

Висновок.

Незважаючи на виявлені неточності та зазначені зауваження дисертаційна робота Кулини Сергія Васильовича на тему «Методи та алгоритми захищеного розподіленого зберігання даних на основі надлишкової системи залишкових класів» є завершеною науково-дослідною роботою, яка представлена на здобуття наукового ступеня доктора філософії за спеціальністю 125 «Кібербезпека» (галузь знань 12 «Інформаційні технології»), яка за своїм змістом, структурою, обсягом науковою новизною та практичним значенням відповідає паспорту спеціальності 125 «Кібербезпека» та вимогам «Порядку присудження ступеня доктора філософії та скасування рішень разової спеціалізованої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», затвердженого постановою Кабінету Міністрів України від 12 січня 2022 року № 44 зі змінами згідно з Постановою КМ №9341 від 21.03.2022, а її автор Кулина Сергій Васильович, заслуговує на присудження йому наукового ступеня доктора філософії за спеціальністю 125 – Кібербезпека.

Офіційний рецензент,
кандидат технічних наук, доцент,
доцент кафедри безпеки
інформаційних технологій
Національного університету
"Львівська політехніка" _____ Тетяна КОРОБЕЙНІКОВА

Підпис к.т.н., доцента Коробейнікової Т.І. засвідчую

Вчений секретар
Національного університету
«Львівська політехніка»
к.т.н., доцент _____ Роман БРИЛИНСЬКИЙ