ВІДГУК

рецензента – доцента кафедри захисту інформації,
Національного університету «Львівська політехніка»,
к.т.н, доцента Гарасимчука Олега Ігоровича

на дисертацію

Кулини Сергія Васильовича

«Методи та алгоритми захищеного розподіленого зберігання даних на основі надлишкової системи залишкових класів»,

подану на здобуття наукового ступеня доктора філософії за спеціальністю
125 «Кібербезпека»
(галузь знань 12 «Інформаційні технології»)

Актуальність теми дисертації.

Системи зберігання даних в сучасному світі є одними з найбільш важливих компонентів інформаційних систем. Постійне зростання обсягу та складності інформації, яка створюється та обробляється щодня, потребує ефективних, надійних та безпечних систем зберігання та стає невід'ємною складовою розвитку суспільства і бізнесу.

Розширення області досліджень та застосування коригуючих кодів, зокрема на основі системи залишкових класів, є важливим напрямом наукових досліджень. Під час передачі по мережі або запису на носії інформація може піддаватися впливу різноманітних факторів, таких як шум, перешкоди або пошкодження, тому застосування методів виявлення та виправлення помилок із використання системи залишкових класів, забезпечує підвищення рівня захищеності систем зберігання в цілому.

При цьому рішення, що побудовані на основі системи залишкових класів, потребують вдосконалення та розробки додаткових методів та алгоритмів, що забезпечать необхідні умови для функціонування безпечних та надійних систем зберігання даних, що застосовуються у інформаційних системах.

Актуальність дисертаційної роботи Кулини Сергія Васильовича зумовлена необхідністю розробки 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 в дисертації Кулини С.В. дослідження виконувались у відповідності до наукового напряму кафедри кібербезпеки Західноукраїнського національного університету.

Тема дисертації 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 роботи полягає в тому, що автором:

1. **Вперше** розроблено метод надійного зберігання даних на основі коригуючих кодів системи залишкових класів, який у порівнянні з відомими, базується на використанні одного перевірочного символу та обчисленні значення геш-функції від файлів залишків. Використання запропонованого методу дозволило зменшити надлишковість на 33% у порівнянні з використанням коригуючих кодів системи залишкових класів.
2. **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 автору встановити оптимальні значення модулів для реалізації захищеного розподіленого зберігання даних.
3. **Удосконалено** метод шифрування даних в системі залишкових класів шляхом циклічного зсуву позицій залишків з використанням в якості ключа псевдовипадкових послідовностей, завдяки чому криптографічна стійкість при заданій розрядності модулів підвищується 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 автором застосовані дані, які одержані з літературних джерел, з результатів аналізу сучасного стану та перспектив розвитку методів і алгоритмів підвищення захищеності та надійності зберігання даних. Тому наведені в дисертації результати слід вважати достатньо обґрунтованими, що підтверджується даними моделювань, експериментальних досліджень та практичними результатами, що підтверджуються актами впровадження.

Наукове значення виконаного дослідження.

Отримані автором наукові положення та практичні результати можуть бути використані при розробці систем зберігання даних на основі 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 алгоритмів шифрування залишків на основі запропонованого методу циклічного зсуву згідно з М-послідовністю; перевірки цілісності файлів залишків шляхом порівняння геш-значень; відновлення при втраті одного із блоків даних на основі удосконаленого методу проекцій, що дозволило побудувати структурні схеми модулів системи захищеного зберігання даних, а реалізація структурних модулів у відповідному програмному забезпеченні дозволила виявити переваги запропонованих методів над існуючими.

Повнота оприлюднення результатів дисертаційної роботи.

Результати дисертаційної роботи Кулини С.В. доповідалися та обговорювались на міжнародних науково-практичних та науково-технічних конференціях та 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.

За структуро, мовою та стилем викладення дисертація відповідає вимогам МОН України. Робота написана українською мовою на достатньому мовно-стилістичному рівні, а стиль викладення матеріалу є послідовним та логічним.

У вступі 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 здобувача.

У першому розділі проведено аналіз існуючих методів програмного та апаратно-програмного захисту інформації. Встановлено, що використання існуючих методів забезпечення надійності систем зберігання даних має значну надлишковість.

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. 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.

Зауваження та дискусійні положення щодо змісту дисертації.

1. Недостатньо обґрунтовано вибір програм, що розглянуті у розділі 1.

2. Для кращого розуміння роботи автору варто обґрунтувати, чому порівняння криптографічної стійкості відбувається саме з алгоритмом AES-128.

3. Доцільно було провести аналіз основних геш-функцій та сформувати критерії вибору таких функції для використання в запропонованому методі.

4. Аналіз підходів та принципів використання коригуючих кодів, які використовуються в системах зберігання даних, варто було проаналізувати більш детальніше.

5. Не достатньо обґрунтовані підходи по вибору інформаційних модулів та перевірочного модуля для проведення відповідних дисертаційних досліджень.

6. Доцільно було б описати принцип вибору розрядності генератора М-послідовності, який використовується при заміні позицій залишків x_i, а також чи впливає ця розрядність і вибір початкового стану генератора на криптостійкість запропонованого методу.

7. Автором не достатньо обґрунтовано чим існуючі методи кодування та шифрування даних не відповідають критеріям та вимогам, які висуваються до сучасних систем зберігання даних, й що саме відповідно до цих критеріїв покращується у даній роботі.

8. У тексті представленої роботи зустрічається ряд стилістичних і орфографічних неточностей.

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

Висновок

Не зважаючи на виявлені недоліки 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 захисту інформації
Національного університету
"Львівська політехніка" Олег ГАРАСИМЧУК

Підпис к.т.н., доцента Гарасимчука О.І. засвідчую

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