ВІДГУК

офіційного опонента – завідувача кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету, доктора технічних наук, професора Смірнова Олексія Анатолійовича

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»)

1. Актуальність обраної теми.

Системи збору та обробки великих обсягів даних є одним із важливих компонентів при побудові та використанні інформаційних систем. Для функціонування таких систем однією із ключових умов є надійне та захищене зберігання даних, що зазвичай забезпечується різноманітними методами розподіленого зберігання та резервного копіювання даних. Іншою, не менш важливою, умовою функціонування таких систем є забезпечення конфіденційності, що досягається застосуванням методів шифрування даних.

Розширення області досліджень та застосування системи залишкових класів, а саме, методів виправлення помилок та шифрування даних, дає змогу не тільки забезпечити надійне зберігання даних а й підвищити захищеність систем зберігання в цілому. Тому підвищення рівня надійності та конфіденційності систем зберігання даних шляхом розробки методів кодування та шифрування даних в надлишковій системі залишкових класів є актуальною науковою задачею.

При цьому варто врахувати, що рішення побудовані на основі системи залишкових класів потребують розробки додаткових методів та алгоритмів, які б забезпечували необхідні умови для функціонування інформаційних систем.

Актуальність дисертаційної роботи Кулини Сергія Васильовича обумовлена необхідністю розробки та удосконалення існуючих методів і алгоритмів підвищення захищеності та надійності систем зберігання даних.

2. Зв'язок роботи з науковими програмами, планами і темами.

Наведені в дисертації Кулини С.В. основні результати та рекомендації виконані на кафедрі кібербезпеки Західноукраїнського національного університету, а тема дисертації відповідає пріоритетним напрямкам науково-дослідних робіт відповідно до координаційних планів Міністерства освіти і

науки України.

Дисертаційна робота 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).

3. Наукова новизна одержаних результатів.

- **Вперше** розроблено метод надійного зберігання даних на основі коригуючих кодів системи залишкових класів. Цей метод у порівнянні з відомими, базується на використанні одного перевірочного символу та обчисленні значення геш-функції від файлів залишків, що 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 автору встановити оптимальні значення модулів для реалізації захищеного розподіленого зберігання даних.
- **Удосконалено** метод шифрування даних в системі залишкових класів шляхом циклічного зсуву позицій залишків з використанням в якості ключа псевдовипадкових послідовностей. Запропонований автором метод забезпечує вищу, в середньому у три рази, криптографічну стійкість при заданій розрядності модулів.

4. Практичне значення одержаних результатів.

Практичне значення одержаних результатів полягає у побудові прототипу системи захищеного розподіленого зберігання даних, що дозволило автору виявити переваги запропонованих методів над існуючими.

5. Мова та стиль викладання дисертації дозволяють зрозуміти суть розроблених наукових положень та одержаних практичних результатів.

Оформлення дисертаційної роботи відповідає вимогам ДСТУ 3008:2015 – «Інформація та документація. Звіти у сфері науки і техніки. Структура та правила оформлювання» й «Вимог до оформлення дисертації» затверджених наказом Міністерства освіти і науки України від 12.01.2017 № 40, а сам зміст викладено послідовно та логічно.

6. Достовірність наукових положень, висновків і рекомендацій.

Достовірність наукових положень, висновків і рекомендацій, отриманих у дисертації, підтверджена результатами теоретичних та експериментальних досліджень, коректним застосуванням аналітичних розрахунків, а також побудовою прототипу системи розподіленого захищеного зберігання даних на основі надлишкової системи залишкових класів.

7. Повнота оприлюднення результатів дисертаційної роботи.

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

Основні результати дисертації 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.

Таким чином, вимоги «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії» до кількості публікацій виконано.

8. Загальна характеристика структури та змісту дисертаційної роботи.

Дисертаційна робота викладена на 203 сторінках та складається із анотації, змісту, переліку скорочень, вступу, п'яти основних розділів, в яких міститься 55 рисунків та 41 таблиця, висновків, списку використаних джерел із 124 найменувань 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. Подано відомості про апробацію

результатів роботи, особистий внесок автора та його публікації.

Анотація дисертації коректно відображає її основні положення.

У **першому** розділі здійснено 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 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. Для оцінки криптографічної стійкості методу шифрування даних запропоновано 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. Приведено схеми модулів, які забезпечують функціонування розробленої системи. Представлено прототип програмного продукту та проведено дослідження ефективності методів кодування та декодування даних на основі реалізованого методу.

У **загальних висновках дисертаційної роботи** сформульовано основні результати дисертаційної роботи, які узгоджуються з метою та завданнями дослідження. За результатами дисертаційного дослідження зроблено вісім висновків, які повністю відповідають поставленим завданням. В цілому дисертація Кулини Сергія Васильовича є завершеним та повним дослідженням, що містить розробки та відповідні їм перевірки.

9. Зауваження та дискусійні положення щодо змісту дисертації.

1. У пунктах наукової новизни одержаних результатів конкретні цифри, які показують перевагу отриманих результатів над існуючими, наведено не за всіма пунктам наукової новизни.

2. У пункті 1.4 мету дисертаційного дослідження наведено у вигляді списку, доцільніше було сформулювати її у вигляді математичної моделі, яка включала б в себе багатокритеріальну цільову функцію, та відповідну систему обмежень для цієї цільової функції.

3. Не в повній мірі проведено розглянуто чим існуючі методи кодування та шифрування даних не відповідають вимогам, які висуваються до існуючих систем зберігання даних, й що саме відповідно цих критеріїв покращується у даній роботі.

4. У роботі не достатньо обґрунтовано перевагу системи кодування на основі надлишкової системи залишкових класів над іншими системами кодування.

5. У висновках до 2-5 розділів не наведено конкретні чисельні переваги розроблених методів у порівнянні з існуючими.

6. У пункті 3.2 необґрунтовано чому порівняння криптографічної стійкості відбувається саме з алгоритмом AES-128.

7. У пункті 4.2 не наведено, яка саме геш-функція використовується у дисертаційному дослідженні. Відсутнє обґрунтування її вибору.

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

Загальні висновки та оцінка дисертації.

На основі критичного вивчення дисертації та праць здобувача, які опубліковані за темою дисертації об'єктивно встановлено, що:

1. Дисертаційна робота Кулини Сергія Васильовича «Методи та алгоритми захищеного розподіленого зберігання даних на основі надлишкової системи залишкових класів» представлена на здобуття наукового ступеня доктора філософії за спеціальністю 125 Кібербезпека є завершеною науково-дослідною роботою, що містить обґрунтовані наукові результати;

2. У дисертаційній роботі розв'язано актуальну науково-прикладну задачу підвищення захищеності та надійності зберігання даних у локальних та мережевих сховищах шляхом розробки методів шифрування та кодування даних на основі розширеного набору модулів системи залишкових класів;

3. Отримані наукові положення та практичні результати є значущими для галузі інформаціях технологій в цілому та кібербезпеки зокрема. Таким чином, враховуючи актуальність теми дисертації, обґрунтованість наукових положень,

висновків та рекомендацій, сформульованих у дисертації, їх наукову новизну та практичну цінність, відповідність предметній області спеціальності 125 Кібербезпека, повноту викладу у наукових публікаціях, відсутність порушень академічної доброчесності, вважаю, що дисертація повністю відповідає 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 та чинним вимогам МОН України, а її автор Кулина Сергій Васильович, заслуговує на присудження йому наукового ступеня доктора філософії за спеціальністю 125 – Кібербезпека.

Офіційний опонент, доктор технічних наук,
професор, завідувач кафедри кібербезпеки та
програмного забезпечення
Центральноукраїнського
національного технічного університету. _____ Олексій СМІРНОВ

31.08.2023
Підпис Олексія Смірнова
засвідчую ст. інспектор ВК
О. Улійна