ВІДГУК ОФІЦІЙНОГО ОПОНЕНТА

доктора технічних наук, професора,
професора кафедри кібербезпеки
Національного технічного університету «Харківський політехнічний інститут»
Мілова Олександра Володимировича
на дисертаційну роботу Кулини Сергія Васильовича
на тему «Методи та алгоритми захищеного розподіленого зберігання даних на основі надлишкової системи залишкових класів»,
подану на здобуття наукового ступеня доктора філософії
за спеціальністю 125 – Кібербезпека

Актуальність обраної теми

Широкомасштабне впровадження інформаційних систем, які збирають та обробляють великі обсяги даних потребує надійних ресурсів для надійного та захищеного зберігання. Згідно світової практики, для зменшення втрат інформації застосовують різноманітні методи розподіленого зберігання та резервного копіювання даних, а також методи їх зберігання в режимі реального часу.

Використання системи залишкових класів, зокрема 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 захищеності систем зберігання даних шляхом 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 використання додаткових обчислень і відповідно потребують вдосконалення. Тому я вважаю, що дисертація Кулини Сергія Васильовича, яка присвячена розробленню та удосконаленню методів і алгоритмів підвищення захищеності та надійності систем зберігання даних, є актуальною.

Зв'язок роботи з науковими програмами, планами і темами

Дисертація Кулини С.В. виконана на кафедрі кібербезпеки Західноукраїнського національного університету. Тема дисертації відповідає пріоритетним напрямкам науково-дослідних робіт відповідно до координаційних планів Міністерства освіти і науки України. Зокрема, 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).

Оцінка обґрунтованості наукових положень, висновків і рекомендацій

При вирішенні поставлених у дисертації задач, створенні наукових положень, висновків та рекомендацій здобувачем 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 створені наукові положення, висновки та рекомендації можна вважати достатньо обґрунтованими. Крім того, обґрунтованість наукових положень, висновків та рекомендацій підтверджується результатами моделювань, даними експериментальних досліджень та практичними результатами, що підтверджуються наведеними актами впровадження.

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.

Наукова новизна наукових положень, висновків і рекомендацій, сформульованих у дисертації.

Дисертація вирішує актуальну науково-практичну задачу підвищення захищеності та надійності зберігання даних у локальних та мережевих сховищах, шляхом розробки методів і алгоритмів шифрування та забезпечення цілісності даних на основі надлишкової системи залишкових класів.

Робота містить раніше незахищені наукові положення та отримані автором нові науково обґрунтовані результати. А саме:

- *вперше* розроблено метод надійного зберігання даних на основі коригуючих кодів системи залишкових класів, який, на відміну від відомих,

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;

- *вперше* отримано аналітичні вирази для оцінки криптографічної стійкості шифрування даних в системі залишкових класів із врахуванням мінімальної довжини файлу, що дало змогу 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, що забезпечило вищу, в середньому у три рази, криптографічну стійкість при заданій розрядності модулів.

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

Основні положення та практичні результати дисертації доповідалися і обговорювались на таких конференціях: Міжнародних науково-практичних конференціях «Фізико-технологічні проблеми передавання, оброблення та зберігання інформації в інфокомунікаційних системах» (Чернівці, Україна, 2018 р.), «Прикладні науково-технічні дослідження» (Івано-Франківськ, Україна, 2019 р.), «Автоматизація та комп'ютерно-інтегровані технології» (Тернопіль, Україна, 2021-2023 рр.), «Кібербезпека та комп'ютерно-інтегровані технології» (Тернопіль, Україна, 2022 рр.), «Економічний і соціальний розвиток України в XXI столітті: національна візія та виклики глобалізації» (Тернопіль, Україна, 2023 р.), Міжнародній науково-технічній конференції «Захист інформації і безпека інформаційних систем» (Львів, Україна, 2023 р.), Міжнародних конференціях 10th International Conference on Advanced Computer Information Technologies ACIT' 2020 (Deggendorf, Germany, 2020), IEEE 5th International Symposium on Smart and Wireless Systems within the Conferences on Intelligent Data Acquisition and Advanced Computing Systems IDAACS-SWS (Dortmund, Germany, 2020), VIII-th International Scientific and Technical Conference «Information protection and information systems security» (Lviv, Ukraine, 2021).

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.

Публікація автором результатів досліджень у рецензованих виданнях, які передбачають попередню перевірку матеріалів на відсутність запозичень, є одним із елементів підтвердження відсутності порушень академічної доброчесності. В цілому у дисертації порушень академічної доброчесності не виявлено.

Аналіз змісту та форми дисертації.

Робота написана на достатньому мовно-стилістичному рівні та складається із вступу, п'яти розділів, висновків, списку використаних джерел і додатків.

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.

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 *висновках* сформульовано основні результати дисертаційної роботи.

У *додатках* представлено акти впровадження та додаткові матеріали.

Анотація дисертації коректно відображає її основні положення.

Зауваження та дискусійні положення щодо змісту дисертації.

1. У першому розділі недостатньо висвітлено атаки на дані та методи захисту від них.
2. Не обґрунтовано вибір програм, що представлені у додатку А.
3. Не в повній мірі проведено аналіз коригуючих кодів, які використовуються в системах зберігання даних.
4. Недостатньо обґрунтовано вибір М-послідовностей в якості секретного ключа при шифруванні даних, представлених в системі залишкових класів.
5. В описі наукової новизни дисертант наводить ефективність тільки для системи із чотирьох модулів, невідомо чи зберігається залежність при іншій кількості модулів і якщо змінюється то в сторону покращення чи погіршення результатів.
6. У пункті 3.1 велика кількість таблиць, вміст яких потім повторюється у додатку Б.
7. У тексті представленої роботи зустрічається ряд стилістичних і орфографічних неточностей.

Загальні висновки та оцінка дисертації.

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, яка містить обґрунтовані наукові результати.

У дисертації 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.

Отримані наукові положення та практичні результати є значущими для

галузі інформаціях технологій в цілому та кібербезпеки зокрема. Тема, зміст дисертації та отримані наукові результати відповідають предметній області спеціальності 125 Кібербезпека.

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,
професор кафедри кібербезпеки
Національного технічного університету
«Харківський політехнічний інститут». _____ Олександр МІЛОВ

Підпис проф. Олександра Мілова
ЗАСВІДЧУЮ:
ВЧЕНИЙ СЕКРЕТАР
НАЦІОНАЛЬНОГО ТЕХНІЧНОГО УНІВЕРСИТЕТУ
"ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ"
_____
"___" _____ 20___ р.

ЗАСВІДЧУЮ
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний технічний університет "Харківський політехнічний інститут"
код 02071180