УДК 004.056.5:004.056.55

В. А. Руденко, С. Г. Шило, О. М. Кулабухов

УДОСКОНАЛЕННЯ КРИПТОГРАФІЧНОГО ГЕШУВАННЯ ДЛЯ ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ ДАНИХ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІЙ СИСТЕМІ ПОВІТРЯНИХ СИЛ

Анотація: *розглянуто актуальність забезпечення цілісності інформаційних ресурсів інформаційно-комунікаційних систем спеціального призначення в умовах збройної агресії російської федерації проти України. Проаналізовано можливості застосування геш-функцій для виявлення несанкціонованих змін інформації та визначено основні проблеми, пов'язані з обчислювальною складністю їх реалізації. Запропоновано підхід до вдосконалення геш-функції «Купина» на основі розпаралелювання оброблення вхідних даних, що передбачає їх розподіл на окремі блоки для організації паралельних обчислень. Розглянуто потенційні переваги такого підходу щодо підвищення швидкодії та ефективності оброблення інформації. Застосування запропонованого підходу може сприяти вдосконаленню засобів криптографічного захисту інформації та підвищенню рівня захищеності інформаційних ресурсів систем спеціального призначення.*

Ключові слова: *цілісність інформації, геш-функція, «Купина», розпаралелювання обчислень, криптографічний захист інформації, інформаційно-комунікаційні системи.*

Abstract: *the integrity of information resources in special-purpose information and communication systems is of particular importance in the context of the Russian Federation's armed aggression against Ukraine. The application of hash functions to detect unauthorized modifications to information is considered, and the main challenges associated with their computational complexity are identified. An approach to improving the Kupyna hash function through parallel processing of input data is proposed. This approach involves dividing input data into separate blocks to enable parallel computations. The potential advantages of this approach in terms of processing speed and computational efficiency are examined. The implementation of the proposed approach may contribute to the improvement of cryptographic information protection mechanisms and enhance the security of information resources in special-purpose systems.*

Keywords: *integrity, hash function, Kupyna, parallel computing, cryptographic information protection, information and communication systems.*

В умовах збройної агресії російської федерації проти України особливого значення набуває забезпечення належного рівня захисту інформаційних ресурсів. Однією з ключових складових інформаційної безпеки є цілісність даних, яка передбачає їх захист від несанкціонованої модифікації, пошкодження та підміни під час зберігання й передавання. Це зумовлює необхідність удосконалення методів контролю цілісності інформації в інформаційно-комунікаційних системах і електронних комунікаційних мережах спеціального призначення [1,3].

Одним із поширених засобів контролю цілісності інформації є криптографічні геш-функції, які перетворюють вхідні дані довільної довжини на геш-значення встановленого розміру. Різні алгоритми гешування відрізняються структурою, кількістю раундів перетворення, довжиною вихідного геш-коду, швидкодією та рівнем криптографічної стійкості. Водночас ефективність їх застосування залежить від здатності забезпечувати необхідний рівень захисту за прийнятних обчислювальних витрат.

Попри широке використання геш-функцій у сучасних системах захисту інформації, їх обчислення може потребувати значних ресурсів, особливо під час оброблення великих обсягів даних. Це зумовлює актуальність дослідження методів оптимізації обчислювальних процесів без порушення основних криптографічних властивостей алгоритмів [2].

Одним із можливих напрямів підвищення продуктивності є застосування паралельних обчислень, які дають змогу розподіляти обчислювальне навантаження між кількома обчислювальними потоками або процесорними ядрами. Водночас реалізація такого підходу має враховувати внутрішню структуру конкретної геш-функції, оскільки послідовність оброблення блоків даних безпосередньо впливає на формування кінцевого геш-значення.

У зв’язку з цим доцільним є дослідження можливостей удосконалення геш-функції «Купина» шляхом організації паралельного оброблення даних. Такий підхід передбачає розроблення відповідного механізму розподілу обчислень і визначення умов, за яких можна підвищити швидкодію алгоритму зі збереженням його криптографічної стійкості. Практична реалізація запропонованого рішення та оцінювання його ефективності можуть стати основою для вдосконалення засобів забезпечення цілісності інформаційних ресурсів у системах спеціального призначення.

Список використанихджерел:

1. Жданова Ю.Д., Спасітєлева С.О., Шевченко С.М., Кравчук К.В. Прикладні та методичні аспекти застосування геш-функцій в інформаційній безпеці. Кібербезпека: освіта, наука, техніка. 2020. №4(8). С. 85-96. https://doi.org/10.28925/2663-4023.2020.8.8596.
2. Фесенко А.С, Гапон Р.О. Порівняння алгоритмів стиснення та геш-функцій готових програмних рішень у розрізі створення власного застосунку. Кібербезпека: освіта, наука, техніка. 2020. №3 (23). С. 186-199. https://doi.org/10.28925/2663-4023.2024.23.284309.
3. Ряполов І.Є., Кметюк Я.І., Дубинець М.С. Аналіз методів підвищення інформаційної безпеки інформаційно-телекомунікаційної системи на основі біотехнологій. Збірник наукових праць Харківського національного університету Повітряних Сил. 2021. № 1(67). С. 74-79. https://doi.org/10.30748/zhups.2021.67.09.

Руденко Віктор Анатолійович – курсант магістратури факультету автоматизованих систем управління та наземного забезпечення польотів авіації Харківського національного університету Повітряних Сил імені Івана Кожедуба, м. Харків, вул. Сумська 77/79, інд. 61009, e-mail: krasava.viktorpro228@gmail.com, ORCID: https://orcid.org/0009-0004-6247-4364.

Шило Сергій Георгович – доцент, кандидат технічних наук, доцент кафедри бойового застосування та експлуатації АСУ факультету автоматизованих систем управління та наземного забезпечення польотів авіації Харківського національного університету Повітряних Сил імені Івана Кожедуба, м. Харків, вул. Сумська 77/79, інд. 61009, e-mail: shilosg@i.ua, ORCID: https://orcid.org/0000-0001-5782-552X.

Кулабухов Олександр Михайлович – старший викладач кафедри бойового застосування та експлуатації АСУ факультету автоматизованих систем управління та наземного забезпечення польотів авіації Харківського національного університету Повітряних Сил імені Івана Кожедуба, м. Харків, вул. Сумська 77/79, інд. 61009, e-mail: O.Kulabukhov@m.hnups.mil.gov.ua, ORCID: https://orcid.org/0000-0002-9836-6646.

Viktor Anatoliovych Rudenko – Master’s cadet at the Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, 77/79 Sumska St., Ind. 61009, e-mail: krasava.viktorpro228@gmail.com, ORCID: https://orcid.org/0009-0005-8207-674X.

Sergiy Georgovych Shilo – Associate Professor, PhD in Technical Sciences Associate Professor at the Department of Combat Employment and Operation of Automated Control Systems, Faculty of Automated Control Systems and Ground Support for Aviation Flights, Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, 77/79 Sumska St., Ind. 61009, e-mail: krasava.viktorpro228@gmail.com, ORCID: https://orcid.org/0000-0003-0113-1849.

Oleksandr Mykhailovych Kulabukhov– Senior Lecturer at the Department of Combat Employment and Operation of Automated Control Systems, Faculty of Automated Control Systems and Ground Support for Aviation Flights, Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, 77/79 Sumska St., Ind. 61009, e-mail: O.Kulabukhov@m.hnups.mil.gov.ua, ORCID: https://orcid.org/0000-0002-9836-6646.