**ВІДГУК**

офіційного опонента

**Охріменко Тетяни Олександрівни**

на дисертацію Грицака Анатолія Васильовича

на тему «Методи побудови ефективних криптографічних функцій гешування»,

представлену на здобуття наукового ступеня кандидата технічних наук

за спеціальністю 05.13.21 – «Системи захисту інформації

**Актуальність обраної теми досліджень та зв'язок її з науковими програмами, планами і темами**

Сьогодні з поширенням електронних засобів, систем електронного документообігу, а також систем надання онлайн-послуг гостро постають питання забезпеченні конфіденційності та перевірки цілісності інформації. Одним з найпоширеніших методів захисту є використання криптографічних методів. Зокрема, функції гешування є одним з основних криптографічних примітивів, які широко використовуються у сучасних інформаційно-комунікаційних системах для надання користувачам таких базових послуг як цілісність, конфіденційність, неспростовність тощо. Однак, за останні роки були виявлені недоліки в відомих методах хешування інформації, зросла кількість відомих атак на геш-функції, адже з стрімким розвитком потужностей комп'ютерної техніки можуть бути реалізовані атаки, які нещодавно були неактуальними через великі обсяги обчислень. Окрім того, при розробці нових алгоритмів симетричного шифрування і геш-функцій повинен використовуватись підхід доказової стійкості (provable security) при обґрунтуванні властивостей, проте в контексті швидкості доказова стійкість шкодить швидкості. Через це необхідно зберігати баланс між швидкістю та стійкістю, та за необхідності – при вирішенні конкретної задачі схилятись в ту чи іншу сторону. Робота Анатолія Васильовича як раз направлена на розв'язання такої актуальної науково-технічної задачі – розробки та дослідження нових ефективних геш-функцій, які при достатньо високій швидкодії забезпечуватимуть необхідний рівень стійкості.

**Наукова новизна отриманих результатів**

Наукова новизна полягає у наступному:

– *вперше розроблено* метод побудови функцій гешування, який базується на структурі Меркла-Демґарда та за рахунок доповнення вхідного повідомлення розміром цього повідомлення та псевдовипадковою послідовністю salt (розраховується на основі вхідного повідомлення), використання у функції стиснення нової послідовності операцій (на основі 6-ти не лінійних функцій,

операцій підстановки, додавання за модулем 2 і $2^n$ , циклічних і лінійних зсувів), дозволив будувати криптостійкі функції гешування;

– *вперше розроблено* метод побудови функцій гешування, який базується на структурі Меркла-Демґарда та за рахунок доповнення вхідного повідомлення псевдовипадковою послідовністю salt (розраховується на основі вхідного повідомлення та його розміру), використання у функції стиснення додаткового вектору внутрішнього стану та нової послідовності операцій (на основі 4-х не лінійних функцій, операцій підстановки, перестановки, додавання за модулем 2 і $2^n$ та циклічного зсуву), дозволив будувати швидкісні функції гешування;

– *удосконалено* метод побудови генераторів псевдовипадкових послідовностей, який за рахунок обробки вектора внутрішнього стану та ключового вектору операціями підстановки, циклічного зсуву, складання за модулем 2 і $2^n$ та 4-ма нелінійними функціями, дозволив будувати ефективні генератори псевдовипадкових послідовностей;

– *удосконалено* метод криптографічного захисту інформації, який за рахунок фіксування інформації про ідентифікатор користувача, ідентифікатор сесії, час відправлення, довжину повідомлення та його порядковий номер, а також використання нової процедури формування сеансового ключа для шифрування, дозволяє забезпечити конфіденційність і цілісність даних в інформаційно-комунікаційних системах.

**Загальна характеристика дисертаційної роботи**

Дисертація складається із анотації, вступу, чотирьох розділів, загальних висновків, списку використаних джерел та додатків.

У **вступі** автором обґрунтовано актуальність теми роботи, визначено мету та основні задачі досліджень, сформульовано наукову новизну і практичну цінність одержаних результатів, вказано дані про апробацію основних положень дисертації.

У **першому розділі** було проведено аналіз сучасних підходів до побудови ефективних функцій гешування, представлено теоретичні відомості з основ криптографії, проведено аналіз програмних модулів захисту таких додатків як месенджери, модулі захисту для цифрового підпису, а також Blockchain системи, проаналізовано існуючі функції гешування, що дало можливість визначити їх основні недоліки та формалізувати завдання дистераційної роботи.

**Другий розділ** містить розробку двох методів побудови функцій гешування – перший метод орієнтований на застосування у системах, для яких критичним є параметр стійкість, а другий – у системах, для яких критичним є параметр швидкість.

**Третій розділ** містить розробку методу побудови генераторів псевдовипадкових послідовностей та методу криптографічного захисту інформації

У **четвертому розділі** представлено методику проведення експериментів, визначено мету та задачі експерименту, вхідні та вихідні параметри, гіпотезу і критерії дослідження, описано послідовність необхідних дій.

У **висновках** стисло сформульовано основні наукові та практичні результати дисертаційної роботи.

У **додатках** розміщено акти впровадження результатів дисертаційної роботи.

**Ступінь обґрунтованості наукових положень, висновків і рекомендацій, сформульованих у дисертації, їх достовірність і новизна**

Викладені наукові положення, висновки повністю обґрунтовані, а достовірність теоретичних положень підтверджується коректним застосуванням відомого математичного апарату, експериментальними даними та результатами верифікації запропонованих моделей та методів, а також впровадженням в практику.

**Повнота викладу результатів дисертації в опублікованих працях**

Основні наукові положення і висновки дисертації висвітлено у 11 наукових працях, 6 з яких опубліковано у наукових фахових виданнях, у тому числі 1 стаття у міжнародному рецензованому періодичному виданні, що входить до бази даних Scopus. Кількість, обсяг та зміст друкованих праць відповідають вимогам МОН України щодо публікацій основного змісту дисертації на здобуття наукового ступеня кандидата наук і надають авторові право публічного захисту дисертації. Автореферат дисертації за своїм змістом повністю відповідає дисертаційній роботі.

**Зауваження до дисертації**

Проте, як і будь-яка робота дисертаційне дослідження Грицака А.В. має певні недоліки, а саме:

1. Перший розділ дисертаційного дослідження, а саме пункт 1.1 переповнений загальновідомими фактами, які можна було не наводити, а більшу увагу приділити аналізу.
2. В пункті 1.3 першого розділу аналізуються навіть ті геш-функції, які вже давно не тільки не рекомендуються до використання, але і не використовуються.
3. У розділі 2 дисертаційної роботи не зовсім зрозуміло обґрунтовано та вибрано прототипи SHA-2 та MD-4.

4. У розділі 2 описано розроблені методи, проте не наведено: оцінки складності реалізації, стійкості до колізій, порівняння з прототипами та іншими алгоритмами.
5. В пункті 3.2 (стр. 71) допущено друкарська помилка – повинен бути прототип методу захисту, а не метод побудови генераторів псевдовипадкових послідовностей.
6. По статистичним характеристикам, запропоновані методи на тому ж рівні як і існуючі, по швидкісним характеристикам не зовсім зрозуміло чому порівняння лише з SHA-512, який заздалегідь відомо не найшвидший, логічніше було проводити порівняння з такими як алгоритм прототипу.
7. У розділі 4, експеримент 3 – не зрозуміло яка стійкість до колізій першого і другого роду.

Однак, варто зазначити, що наведені зауваження та недоліки не є принциповими та суттєво не впливають на *загальне позитивне* враження від роботи, не знижують її якість, наукову цінність чи практичне значення.

**Загальний висновок**

Загалом дисертаційна робота Грицака Анатолія Васильовича є закінченою науковою працею, яка містить нові науково обґрунтовані теоретичні та експериментальні результати.

Вважаю, що дисертаційна робота «Методи побудови ефективних криптографічних функцій гешування» повністю відповідає вимогам МОН України, а її автор Грицак Анатолій Васильович заслуговує присудження наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – «Системи захисту інформації».

**Офіційний опонент**:
кандидат технічних наук,
докторант Національного авіаційного університету Т.О. Охріменко

підпис гр. Охріменко Т.О.
засвідчую
Вчений секретар
Національного авіаційного університету
М. Ленінський

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
01132330
МІСТО КИЇВ