УДК 004.056 : 004.424.47

АНАЛІЗ МЕТОДІВ ПІДВИЩЕННЯ СТІЙКОСТІ ДО ЗАГАЛЬНИХ АТАК.

Кравчук Т. А.
Науковий керівник – к. т. н., ст. викл. Баришев Ю. В.

Одним з найефективніших методів захисту інформаційних ресурсів є гешування, що використовується для обчислення контрольної суми з метою перевірки автентичності повідомлень, цифрових підписів, пошуку однакових наборів даних, безпечного зберігання паролів в області пам’яті та ін.

Наразі залишається актуальноюпроблема захисту від загальних атак, які використовуютьмультиколізії. Для цього необхідна розробка нових конструкцій гешування, які б мали підвищену стійкість до цих атак. Низка таких конструкцій вже розроблена, проте їх різноманіття породжує невизначеність при виборі однієї з них для певної задачі.

За мету дослідження взято підвищення стійкості геш-функцій до загальних атак шляхом визначення властивостей конструкцій гешування, які збільшують протидію появі загальних атак.

Розглянуто основні геш-конструкції для запобігання загальним атакам і проведено порівняльний аналіз. Серед розглянутих були конструкції широкого каналу та подвійного каналу Штефана Люкса та конструкція криптологічної губки, що використовують розширення розрядності проміжних геш-значень для підвищення стійкості до загальних атак, що використовують мультиколізії. Відзначені переваги та основні недоліки, що ведуть до зниження швидкості виконання алгоритму. Також розглянута конструкція HaIFa, особливістю якої є використання значеннялічильника вже оброблених даних та так званої «солі» як аргументів функції ущільнення. Проаналізовано підхід керованого гешування, запропонованого братамиМолдовянами. Відзначено порівняно високу швидкість виконання алгоритмів двох останніх конструкцій на противагу неістотній стійкості до загальних атак. Також відомий псевдонедетермінований підхіддо гешування, який забезпечує порівняно середню швидкість виконання алгоритму.

В результаті дослідження була складена порівняльна характеристика для геш-конструкцій з різними підходами до гешування, яка дозволяє спростити процес вибору конструкції гешування, необхідної для розв’язання конкретної задачі, керуючись критеріями швидкості виконання та стійкості до загальних атак. В перспективіподальших досліджень планується оцінювання стійкості до загальних атак псевдонедетермінованого підходу до гешування.