УДК 621.391:519.2:519.7

А.М. КУДІН
Фізико-технічний інститут Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»; Національний банк України, Київ, Україна, e-mail: *pplayshner@gmail.com*.

І.А. КУДІН
Фізико-технічний інститут Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна, e-mail: *mmzi.cat@gmail.com*.

В.З. ЧІХЛАДЗЕ*
Фізико-технічний інститут Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна, e-mail: *the.vaho1337@gmail.com*.

ЗАСТОСУВАННЯ ЗАГАЛЬНОЇ ТЕОРІЇ ОПТИМАЛЬНИХ АЛГОРИТМІВ У КРИПТОГРАФІЇ, СТЕГАНОГРАФІЇ ТА БЛОКЧЕЙН-ТЕХНОЛОГІЇ

Анотація. Аналіз та синтез односторонніх функцій та односторонніх функцій з лазівкою є основою для оцінювання стійкості та побудови криптографічних перетворень, стеганографічних систем та протоколів консенсусу блокчейнів. Розглянуто інформаційно-обчислювальний підхід до побудови таких функцій на основі загальної теорії оптимальних алгоритів та їхнє застосування в криптографії, стеганографії, аналізі та синтезі протоколів консенсусу блокчейнів.

Ключові слова: загальна теорія оптимальних алгоритмів, односторонні функції, односторонні функції з лазівкою, оцінки стійкості криптосистем, стеганографія, блокчейн.

ВСТУП

Основою для багатьох методів захисту є односторонні перетворення інформації. Так, гіпотеза про існування односторонніх (іноді вживають терміни односпрямовані чи важкообернені) функцій є підґрунтям сучасної криптографії та стеганографії [1], багатьох протоколів консенсусу блокчейн-систем, систем контролю доступу тощо. Відомі підходи до побудови односторонніх перетворень інформації лежать або в площині статистичної незалежності вхідних / вихідних даних [2], або в обчислювальній складності виконання оберненого перетворення [3]. Але на сьогодні проблема побудови чи навіть існування односторонніх функцій далека від розв'язання.

Причинами цього можна вважати практичну відсутність математичних моделей оцінювання рівнів кібербезпеки та безпеки інформації в розподілених та децентралізованих інформаційних системах із заздалегідь невідомими множинами інформаційних ресурсів; нерозв'язність проблеми отримання нетривіальних нижніх оцінок стійкості асиметричних криптосистем та стегосистем; відсутність досліджень із забезпечення захисту криптосистем від атак на реалізацію для децентралізованих розподілених інформаційних систем.

У статті запропоновано застосування загальної теорії оптимальних алгоритмів [4–6] для побудови односторонніх перетворень інформації, що дає змогу розв'язати зазначені вище проблеми побудови односторонніх функцій та односторонніх функцій з лазівкою із використанням нового комплексного інформаційно-обчислювального підходу. Розглянуто основи застосування запропонованого підходу до розв'язання різних задач теорії захисту інформації та низки прикладних задач.

ІНФОРМАЦІЙНО-ОБЧИСЛЮВАЛЬНИЙ ПІДХІД ДО ПОБУДОВИ ОДНОСТОРОННІХ ФУНКЦІЙ ТА ОДНОСТОРОННІХ ФУНКЦІЙ З ЛАЗІВКОЮ

Уведемо деякі означення [1, 3].

Означення 1. Чесною функцією назвемо функцію $f : \{0,1\}^n \to \{0,1\}^{m(n)}$, якщо $n \le q(m(n))$, де $q(x)$ — деякий поліном степеня, не вищого за n_0, для всіх $n \ge n_0$. Степінь полінома визначається залежно від обчислювальної моделі.