КІБЕРНЕТИКА

УДК 621.391:519.2:519.7

В.К. ЗАДІРАКА
Інститут кібернетики ім. В.М. Глушкова НАН України, Київ, Україна,
e-mail: *zvk140@ukr.net.*

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.*

І.В. ШВІДЧЕНКО
Інститут кібернетики ім. В.М. Глушкова НАН України, Київ, Україна,
e-mail: *inetsheva@gmail.com*.

КРИПТОСИСТЕМИ, СТІЙКІ В ПЕВНИХ МОДЕЛЯХ ОБЧИСЛЕНЬ

Анотація. Розглянуто проблему оцінювання стійкості криптографічних перетворень у сучасній криптографії, яке зазвичай реалізується з використанням аксіоматичного або доказового підходу. Оскільки квантова модель обчислень змінює складність певних обчислювальних задач (наприклад, задач факторизації цілих чисел), у криптографії вивчають класи алгоритмів, які залишатимуться стійкими в квантовій моделі обчислень — так звані «постквантові криптографічні алгоритми». Узагальненням цієї постановки задачі є дослідження моделей обчислень, що містять алгоритми криптоаналізу, найкращий з яких має експоненційну складність або наближену до неї. Розглянуто узагальнення проблеми існування криптосистем, стійких у постквантовому світі, а саме криптосистем, стійких у певних моделях обчислень, а також можливість практичного застосування таких моделей. Основним результатом роботи є створення універсальної обчислювальної моделі, яка узагальнює цілий клас перспективних обчислювальних моделей, зокрема квантової, та побудова криптосистеми, стійкої у межах такої обчислювальної моделі.

Ключові слова: постквантова криптографія, релятивістська криптографія, моделі обчислень, генетичні алгоритми, обернені обчислення, блокчейн.

ВСТУП

Доведені оцінки стійкості криптографічних систем до криптоаналізу отримують зазвичай з використанням аксіоматичного або доказового підходу. Він полягає або у зведенні стійкості криптографічних алгоритмів до стійкості криптографічних примітивів із відомою стійкістю, або до розв'язання певних обчислювальних задач, складність яких добре вивчена. Оскільки квантова модель обчислень змінює складність окремих обчислювальних задач (наприклад, задач факторизації цілих чисел), у криптографії вивчають класи алгоритмів, які залишатимуться стійкими в квантовій моделі обчислень — так звані «постквантові криптографічні алгоритми».

Постквантова криптографія виникла як реакція на застосування реальної моделі обчислень до задач криптоаналізу, натомість важливою є також обернена задача: дослідження впливу абстрактних моделей обчислень на стійкість