

УДК 004.3:004.9

Зуб Р.І.¹, Грушко С.С.²

¹ студ. гр. КНТ-515м НУ «Запорізька політехніка»

² доц. НУ «Запорізька політехніка»

ІНТЕГРОВАНА КОМП'ЮТЕРНА FPGA-СИСТЕМА ПЕРЕВІРКИ ЦІЛІСНОСТІ ДАНИХ

Зростаючі обсяги даних та ускладнення кіберзагроз у системах IoT, хмарних сервісах, блокчейн-платформах і кіберфізичних комплексах вимагають надійних та продуктивних механізмів перевірки цілісності інформації. Сучасні програмні рішення ґрунтуються на криптографічних бібліотеках і утилітах операційних систем: OpenSSL забезпечує підтримку численних хеш-функцій і цифрових підписів для мережових протоколів та контролю файлів, але обробка великих обсягів даних істотно навантажує центральний процесор; вбудовані утиліти командного рядка та інші програмні засоби підтримують обмежений набір алгоритмів, мають невисоку

продуктивність на великих масивах і нерідко є надмірно складними для задач простої перевірки цілісності [1-4].

Найвищу продуктивність і енергоефективність у криптографічних обчисленнях демонструють спеціалізовані апаратні рішення, зокрема ASIC-пристрої для майнінгу, апаратні модулі безпеки та модулі довіреної платформи, однак їх висока вартість розробки та вузька спеціалізація обмежують доцільність застосування у системах загального призначення [5-7]. FPGA натомість забезпечують гнучке перепрограмування логіки, можливість оптимізації під конкретні алгоритми та прийнятний компроміс між вартістю, продуктивністю й енергоефективністю; сучасні роботи з апаратно-програмних моделей обробки сигналів і спеціалізованих обчислювачів підтверджують перспективність такого підходу для завдань контролю цілісності [8-10]. На цій основі сформульовано висновок про доцільність використання FPGA як платформи для побудови систем перевірки цілісності даних у широкому спектрі застосувань.

Для демонстрації принципів побудови інтегрованих FPGA-систем обрано алгоритм MD5 як компроміс між простотою апаратної реалізації та достатньою функціональністю в задачах некриптокритичної перевірки цілісності. Попри відомі криптографічні обмеження, MD5 зберігає актуальність як швидкий механізм контролю даних, а запропонована архітектура передбачає можливість подальшої адаптації до сучасних алгоритмів SHA-256 і SHA-3 [11-13]. Мета дослідження полягає у створенні інтегрованої комп'ютерної системи перевірки цілісності на основі FPGA, здатної забезпечити потрібний баланс між швидкодією, енергоефективністю та гнучкістю конфігурації для вбудованих пристроїв, телекомунікаційного обладнання та кіберфізичних систем.

Запропонована архітектура побудована за модульним принципом і складається з інтерфейсного модуля та модуля хешування з чітким розподілом функцій. Інтерфейсний модуль слугує шлюзом між зовнішніми інтерфейсами й обчислювальним ядром, приймає та буферизує дані, автоматично формує необхідне доповнення згідно зі специфікацією MD5 та керує етапами обробки за допомогою компактного кінцевого автомата; модуль хешування реалізує повний цикл алгоритму на рівні базових логічних операцій і циклічних зсувів, послідовно обробляючи блоки даних і формуючи фінальне хеш-значення, причому використання конвеєрного підходу дозволяє підвищити пропускну здатність без значного збільшення ресурсів FPGA.

Функціональна верифікація системи виконана шляхом порівняння отриманих хеш-значень з еталонними результатами незалежних онлайн-генераторів для набору тестових повідомлень різної довжини й структури, що підтвердило коректність реалізації алгоритму, правильність

формування доповнення та відповідність вимогам стандарту MD5. Теоретичний аналіз енергоспоживання й завантаження логічних ресурсів показав переваги FPGA-реалізації над програмними рішеннями на універсальних процесорах та наявність резерву для подальшого масштабування або паралельної обробки кількох потоків даних, а модульна структура створює передумови для адаптації під сучасні криптографічно стійкі алгоритми й інтеграції у складніші апаратно-програмні комплекси захисту інформації.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Матюшенко І.Ю. Теоретичні аспекти розвитку конвергентних технологій в Україні в умовах нової промислової революції : дисертація. Харків : НДЦ ІПР НАН України, 2017. 661 с.
2. Остапов С.Е., Євсєєв С.П., Король О.Г. Кібербезпека: сучасні технології захисту : навчальний посібник. Львів : Новий світ, 2020. 678 с.
3. How to get the checksum for a file on Windows. URL: https://www.carehart.org/blog/2018/9/20/how_to_get_checksum_on_windows (дата звернення: 14.09.2025).
4. Аналіз програмного комплексу криптографічного захисту інформації / К.В. Терещенко та ін. *Кібербезпека: освіта, наука, техніка*. 2025. № 4(28). С. 599–618.