УДК 004.274:004.056

С.Я. Гільгурт, к.т.н.
Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, Київ

ПОРІВНЯЛЬНИЙ АНАЛІЗ ПІДХОДІВ ДО ПОБУДОВИ КОМПОНЕНТІВ РЕКОНФІГУРОВНИХ ЗАСОБІВ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Останнім часом у зав'язку зі сталим зростанням мережевого трафіку, кількості та витонченості кібератак, а також через зупинення частоти універсальних мікропроцесорів програмна реалізація складних засобів технічного захисту інформації, таких як системи виявлення вторгнень або додатки проти вірусів та спаму вже не відповідають вимогам щодо їх швидкодії. Тому розробники звертаються до реконфігуровних рішень на базі програмованих логічних інтегральних схем (ПЛІС), які поєднують в собі продуктивність спецпроцесорів і гнучкість програмного забезпечення. Найбільш ресурсномісткою задачею реального часу в апаратних засобах технічного захисту інформації є множинне розпізнавання фіксованих послідовностей символів (патернів). Від того, наскільки успішно вдасться вирішити цю задачу, залежить ефективність системи захисту в цілому.

Існує багато підходів різної природи до побудови апаратних схем множинного розпізнавання патернів. Як свідчить аналіз численних публікацій, найкращі здібності в сенсі ефективності при побудові схем множинного розпізнавання патернів продемонстрували наступні три підходи (а також їх модифікації, технології, на яких вони базуються, та техніки покращення відповідних рішень):

– асоціативна пам'ять на базі цифрових компараторів;

– фільтр Блума на базі геш-функцій;

– алгоритм Ахо–Корасік на базі скінченних автоматів.

Асоціативна пам'ять (АП), є класом пристроїв, які створювалися саме для швидкого розпізнавання кодів і виконують функцію, протилежну традиційному ОЗП – за змістом відшукують місце розташування даних в пам'яті або свідчать про їх відсутність. Швидкодіючою основою АП на ПЛІС є цифрові компаратори.

Фільтр Блума (ФБ) – це абстрактний пристрій, який складається з комплекту з K блоків обчислення геш-функції $h_1(x)$, $h_2(x)$, …, $h_K(x)$ та масиву з M бітових комірок (МБК). В початковому стані МБК

заповнений нулями. На етапі програмування на входи геш-функцій послідовно подаються всі патерни словнику, для кожного з них обчислюється *K* геш-функцій, значення котрих інтерпретуються як адреси комірок у МБК, в які заносяться одиниці. В процесі функціонування фільтра Блума на його вхід подається фрагмент вхідної послідовності символів, і також обчислюються значення всіх *K* геш-функцій. По отриманим адресам здійснюється звернення до комірок МБК. Якщо у всіх позиціях, на які вкажуть геш-функції, містяться одиниці, вважається, що вхідна комбінація символів з певною вірогідністю співпадає з одним з патернів, що приймали участь у програмуванні ФБ.

Алгоритм Ахо–Корасік (АК) є прикладом засобу, який на відміну від багатьох відомих алгоритмів одиночного розпізнавання виявляє у вхідних даних одночасно кілька зразків. На етапі побудови АК з наданого набору патернів за певними правилами створюється детермінований скінченний автомат – розпізнавач. Під час функціонування такий автомат на кожному такті в залежності від вхідного символу переходить з одного стану в інший згідно функції переходів поки не опиниться в одному з так званих прийнятних станів, що означає факт розпізнавання певного слова (рядка символів) зі словника патернів.

Щоб оцінювати та порівнювати технічні рішення щодо реконфігуровних засобів технічного захисту інформації, потрібно визначитися з критеріями їх ефективності та відповідними показниками. Аналіз світового досвіду дозоляє створити ієрархію показників ефективності (ПЕ) таких засобів. Всі ПЕ можна поділити на три категорії: основні (вартісні показники, показники продуктивності та функціональні показники), проміжні (що пов'язують деякі з основних) та похідні (що формуються з кількох інших).

Як свідчать результати порівняльного аналізу, жоден з досліджених підходів не демонструє явних переваг перед іншими. Кожен має позитивні риси та недоліки, але не перевершує конкурентні рішення за всіма ПЕ. Отже, виникає потреба в методах поєднання різних підходів в єдиному пристрої із забезпеченням максимальної реалізації переваг кожного з підходів.