РЕАЛІЗАЦІЯ ШИФРУВАННЯ ЗА ДОПОМОГОЮ ГРАФІЧНОГО ПРИСКОРЮВАЧА НА БОРТОВОМУ КОМП’ЮТЕРІ БПЛА

Зуєв А. О., Караман Д. Г.
Національний технічний університет «Харківський політехнічний інститут», м. Харків

Сучасні БПЛА і системи, які їх використовують, потребують забезпечення належного рівня кібербезпеки, для зберігання та передачі критично важливої інформації про об'єкт моніторингу та його оточення з використанням мереж передачі даних загального призначення [1].

Типова схема БПЛА, з використанням комп'ютера-компаньйона, що набула широкого поширення, оскільки має істотну перевагу: контролер управління польотом і бортовий комп'ютер розділені, і функціонально не залежать один від одного що підвищує надійність всієї системи в цілому.

Особливістю комп'ютера-компаньйона, який знаходяться в основі системи, є наявність вбудованого графічного прискорювача (GPU), який може бути використаний для проведення розрахунків загального призначення. GPU функціонує незалежно від CPU, таким чином, розрахунки можуть виконуватися одночасно з основним процесом управління БПЛА. Перевагою роботи шифрування на GPU є те, що цей процес вимагає істотних обчислювальних ресурсів, а обчислювальне навантаження на GPU, зазвичай незначне.

Для виконання процесу шифрування прикладних даних на борту БПЛА був обраний блоковий симетричний алгоритм шифрування «Калина», який був прийнятий як національний стандарт України ДСТУ 7624 до: 2014 [2]. Але для реалізації алгоритму шифрування на GPU потрібно зробити його адаптацію, щоб забезпечити ефективну роботу. Наведене рішення працює без використання спеціалізованих API, прив'язаних до апаратного забезпечення будь-якого з виробників [3], дозволяє знизити навантаження на CPU бортового комп'ютера, найбільш ефективно використовувати можливості апаратної платформи БПЛА.

Література:

1. Javaid A. Y. Cyber security threat analysis and modeling of an unmanned aerial vehicle system/ A. Y. Javaid, W. Sun, V. K. Devabhaktuni, M. Alam. Homeland Security (HST), 2012 IEEE Conference on Technologies for, pp. 585–590, IEEE, 2012.

2. ДСТУ 7624:2014. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення. [Текст]. – Введ. 01–07–2015. – К.: Мінекономрозвитку України, 2015.

3. K. Iwai, T. Kurokawa, and N. Nishikawa, “AES encryption implementation on CUDA GPU and its analysis,” Proc. of 2010 First International Conference on Networking and Computing, 2010, pp.209-214, doi:10.1109/IC-NC.2010.49.