ПРАКТИЧЕСКОЕ ПРИМЕНЕНИЕ ГРАФИЧЕСКОГО СОПРОЦЕССОРА ДЛЯ ЗАШИФРОВАНИЯ ДАННЫХ НА БОРТОВОМ КОМПЬЮТЕРЕ БПЛА

Караман Д. Г., Зуев А. А.

Национальный технический университет «Харьковский политехнический институт», ул. Кирпичева 2, Харьков 61002, Украина

БПЛА используются для решения задач в различных областях человеческой деятельности. Однако, за последнее десятилетие произошло множество инцидентов, связанных с безопасностью как гражданских, так и военных БПЛА [1, 2].

Среди множества целей злоумышленников можно выделить две основные: захват контроля над управлением БПЛА и перехват прикладных данных, которые собирает БПЛА. Вмешательство в систему контроля управлением БПЛА требует от злоумышленника значительных материальных и организационных ресурсов, тогда как перехват прикладных данных может оказаться значительно проще и выгоднее. Кроме того, в последнем случае требуется привлечение минимального числа векторов атак.

В качестве прикладной вычислительной системы на борту БПЛА используют одноплатные микрокомпьютеры (микро-ПК), построенные по схеме SoC (System-on-Chip), которые имеют малое энергопотребление и небольшую массу. Особенностью таких микро-ПК, является наличие встроенного графического ускорителя (GPU), который может быть использован для проведения расчетов общего назначения, так как является, по сути, организованным массивом параллельных вычислителей. GPU функционирует независимо от центрального микропроцессора (CPU), таким образом, расчеты на нем могут выполняться одновременно с основным процессом СПО бортового компьютера БПЛА. Ресурсы GPU могут использоваться как для первичной обработки данных, поступающих с сенсоров, так и ряда специализированных задач, например, процедур шифрования. Предпочтение в использовании GPU обосновывается еще и тем, что процесс шифрования требует существенных вычислительных ресурсов, а вычислительная нагрузка на GPU, обычно незначительна, тогда как CPU практически полностью загружен задачами обработки и сохранения поступающей с сенсоров информации.

Для реализации прикладных алгоритмов и программ на GPU требуется их анализ и адаптация, чтобы учесть вышеперечисленные особенности и обеспечить их эффективную работу на GPU.

В докладе предложено практическое решение для обеспечения оперативного зашифрования прикладных данных, получаемых БПЛА, для которого используются возможности графического ускорителя бортового

компьютера. Предложенное решение помимо надежной защиты получаемых прикладных данных с помощью современного криптоустойчивого алгоритма шифрования «Калина» [5] позволяет снизить нагрузку на центральный процессор бортового компьютера и наиболее эффективно использовать возможности аппаратной платформы БПЛА.

Предложенная реализация процедуры зашифрования на GPU может быть использована не зависимо от применяемого графического API под любой ОС, для GPU любого производителя.

В процессе практической реализации механизма криптографической защиты прикладных данных БПЛА был проведен анализ алгоритмических структур и математического аппарата алгоритма шифрования «Калина», среди них были выделены наиболее ресурсозатратные части. По некоторым криптографическим преобразованиям предложен ряд оптимизаций для реализации алгоритма «Калина» на GPU. Выполнена практическая реализация метода на GPU бортового микро-ПК и показана возможность его эффективного применения на устройствах с высокими требованиями к производительности и строгим ограничениям по доступным ресурсам.

Список литературы

1. Kim A. Cyber attack vulnerabilities analysis for unmanned aerial vehicles / A. Kim, B. Wampler, J. Goppert, I. Hwang, H. Aldridge. // Infotech@Aerospace, – 2012.

2. 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. // 2012 IEEE Conference on Technologies for Homeland Security (HST). – 2012. – pp. 585–590.

3. N.Nishikawa, K Iwai, and T.Kurokawa, «High-Performance Sysmmetric Block Ciphers on CUDA,» // Proc. of 2011 Second International Conference on Networking and Computing(ICNC). – 2011. – pp. 221-227.

4. Qinjian Li, Chengwen Zhong, Kaiyong Zhao, Xinxin Mei, Xiaowen Chu. (2012) Implementation and Analisys of AES Encryption on GPU. // IEEE 14th International Conference on High Performance Computing and Communication & 2012 IEEE 9th International Conference on Embedded Software and Systems. DOI: 10.1109/HPCC.2012.119.

5. Горбенко И. Д. и др. Симметричный блочный шифр «Калина» – новый национальный стандарт шифрования Украины. – Радиотехника. – 2015. – Вып. 181 – с. 5-22.

6. Совин Я. Р., Отенко В. І., Штефанюк Є. Ф. Ефективна реалізація алгоритму блокового симетричного шифрування ДСТУ 7624:2014 («Калина») для 8/16/32-бітових вбудованих систем. – Сучасний захист інформації. – №2(30), – 2017. – с. 6-16.