

ФОРМИРОВАНИЕ СТЕГО-ПУТИ ВНЕДРЕНИЯ ЦИФРОВОГО ВОДЯНОГО ЗНАКА В ПРОГРАММНЫЙ КОД FPGA-БАЗИРОВАННЫХ УСТРОЙСТВ

Защелкин К.В., Иванова Е.Н.

*Одесский национальный политехнический университет,
г. Одесса*

В последние годы имеет место тенденция увеличения доли использования микросхем FPGA (Field Programmable Gate Array) при построении цифровых вычислительных и управляющих систем. Как и микропроцессоры, FPGA являются программируемыми устройствами, однако за счет естественного параллелизма организации вычислений, они превосходят микропроцессоры по характеристикам производительности [1].

Как для любых программируемых интегральных схем, для FPGA характерна проблема обеспечения целостности программного кода. Одной из основных составляющих обеспечения целостности выступает процесс ее контроля. Контроль целостности программного кода FPGA традиционно решается путем формирования эталонной хэш-суммы программного кода, которая в момент выполнения контроля сравнивается с текущей хэш-суммой. При этом принципиальным вопросом является место хранения эталонной хэш-суммы. В данной работе рассматривается подход, в рамках которого, контрольная хэш-сума внедряется в информационный объект программного кода в виде цифрового водяного знака (ЦВЗ) [2]. Это обеспечивает не только недоступность хэш-суммы, но и делает неочевидным для стороннего наблюдателя сам факт того, что контроль целостности выполняется.

В работе предлагается метод формирования стеганографического пути (стего-пути) внедрения ЦВЗ (содержащего контрольную хэш-сумму), в пространство LUT-контейнера [3], образованного элементарными вычислительными блоками LUT (Look Up Table) FPGA. Стего-путь представляет собой упорядоченное множество элементов, задающее порядок внедрения разрядов ЦВЗ в LUT-контейнер. Каждый из элементов стего-пути описывает отдельный блок LUT микросхемы FPGA, а также содержит информацию, необходимую для внедрения одного разряда ЦВЗ в программный код этого блока. Предлагаемый метод представлен основными, обеспечивающими его положениями и последовательностью действий, приводящих к получению стего-пути внедрения ЦВЗ.

Литература:

1. Vanderbauwhede W. High-performance computing using FPGAs / W. Vanderbauwhede, K. Benkrid. – New-York: Springer, 2016. – 804 p. 2. Zashcholkin K. LUT-object integrity monitoring methods based on low impact embedding of digital watermark / K. Zashcholkin, O. Ivanova // Proceedings of the 14th International Conference «Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET-2018)». – Lviv-Slavske, 2018. – P. 519-523. 3. Защелкин К.В. Развитие метода стеганографического скрывания данных в LUT-ориентированных аппаратных контейнерах / К.В. Защелкин, Е.Н. Иванова // Електротехнічні та комп'ютерні системи. – 2014. – Вип. 13 (89). – С. 231-239.