В. В. Агафоненко, Л. В. Петроченко
(ВА РБ, Минск)

АППАРАТНАЯ РЕАЛИЗАЦИЯ АЛГОРИТМА КРИПТОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ НА ОСНОВЕ ТЕХНОЛОГИИ ПРОГРАММИРУЕМЫХ ЛОГИЧЕСКИХ ИНТЕГРАЛЬНЫХ СХЕМ

Решение сложных задач криптографического преобразования информации сопровождается большим количеством вычислений, которые необходимо выполнять в режиме реального времени.

В настоящее время для решения такого рода задач разработано достаточно большое количество средств, базирующихся на использовании программных, программно-аппаратных и аппаратных способов шифрования информации.

Криптографические алгоритмы характеризуются высоким уровнем параллелизма и цикличностью производимых вычислений при изменяющихся параметрах.

Оптимальная реализация алгоритма криптографического преобразования предполагает наличие специализированных вычислительных средств, архитектура которых в наибольшей степени соответствует классу решаемых задач.

В качестве технологической платформы для аппаратной реализации алгоритма криптографического преобразования целесообразно использовать программируемые логические интегральные схемы (ПЛИС) с архитектурой FPGA (Field Programmable Gate Array), которые наряду с высокой производительностью и логической емкостью позволяют генерировать структуры, функциональность которых может видоизменяться в процессе работы.

Это дает возможность быстрой адаптации вычислительной системы под конкретную задачу, широкие функциональные возможности и значительное повышение качества защиты информации.

В докладе рассматривается вариант аппаратной реализации алгоритма криптографического преобразования для систем обработки информации в сетях электронных вычислительных машин, отдельных вычислительных комплексах и ЭВМ на основе технологии ПЛИС.