МОДУЛЬ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИ СО ВСТРОЕННЫМИ СРЕДСТВАМИ ДИАГНОСТИРОВАНИЯ

Слипченко Т.С.

Национальный технический университет «Харьковский политехнический институт, г. Харьков

В данной работе рассмотрены вопросы достижения высоких показателей надежности вычислительных систем. Эффективным и перспективным путем является построение вычислительных систем на базе использования самопроверяемых средств функционального диагностирования.

Самопроверяемые средства функционального диагностирования, распределенные внутри этих систем по отдельным функциональным узлам, дают возможность использовать промежуточные точки съема контрольной информации, тем самым значительно облегчая обнаружение возникающих неисправностей, выдачу сообщения о них и обеспечивая высокую полноту охвата контролем аппаратуры вычислительных систем. Кроме того, самопроверяемость позволяет упростить тестовый контроль, обслуживание и восстановление отказавших систем, при этом предоставляется достоверная информация об источнике неисправности.

Для крупных структурных блоков сложных вычислительных систем (таких как реконфигурируемая система-на-кристалле) самопроверяемые средства встроенного контроля можно построить на основе иерархической системы самопроверяемых средств контроля их составных узлов и за счет сжатия сигналов контроля в обобщенный выходной вектор. Такой подход более экономичен, чем построение системы контроля структурного блока в целом, без доступа к его внутренним точкам.

Для обеспечения самопроверяемости предложено использовать самодвойственные булевы функции, свойства которых полностью удовлетворяют условиям построения самопроверяемых средств встроенного контроля и позволяют получить схемы устройств с минимальной избыточностью.

В данной работе была разработана встроенная самопроверяемая система функционального диагностирования подстановочного блока системы криптографической защиты информации, которая обнаруживает одиночные константные неисправности типа н-к-0 и н-к-1, возникающие на входах, выходах и внутренних соединениях системы.