ОТЗЫВ

на автореферат диссертационной работы Тихонова Сергея Владимировича «Исследование и разработка модификаций аппаратно-реализованных защитных блоковых преобразований, устойчивых к побочным атакам по цепям электропитания», представленной к защите на соискание ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации информационная безопасность» (технические науки).

Актуальность темы диссертации

Задачи разработки методов обеспечения защиты информации от утечки по техническим каналам приобрели в последние годы особое значение в связи с распространением киберпреступности. Представляют практический интерес различные подходы для решения этих задач, в том числе базирующиеся на применении некриптографических методов, специализированных устройств защиты и др. В связи с этим, разработка устройств и методов, предотвращающих несанкционированный доступ к защищаемой информации на основе анализа атак по побочных каналам на устройства – носители защитных преобразований, является актуальной.

Диссертация Тихонова С.В. направлена на разработку конструкции программно-аппаратного комплекса, предназначенного для анализа утечек информации по цепям электропитания, оценке эффективности реализации побочных атак по этим цепям и метода защиты от них.

Научная новизна результатов диссертации

В ходе диссертационного исследования автором решены следующие научные задачи:

1. Предложена архитектура средства моделирования побочных атак по цепям электропитания, а также модель утечки информации, обрабатываемой интегральным чипом, по цепи электропитания, основанная на результатах проведенного комплекса измерений.

2. Доказана возможность успешного применения побочных атак по цепям электропитания к аппаратным реализациям шифров ГОСТ.

3. Разработан метод защиты преобразований на интегральных чипах от побочных атак по цепям электропитания.

Практическая значимость результатов диссертационной работы

Важный практический результат определяется предложенными автором моделью утечки информации, моделью побочной атаки, методом защиты информации от такого рода атак и архитектурой средства их моделирования.

Достоверность результатов

Достоверность полученных результатов обеспечивается использованием методов исследования, соответствующих задачам, корректным применением апробированного математического аппарата, что подтверждается согласованностью полученных результатов с результатами компьютерного моделирования и натурных экспериментов. Материалы диссертации обсуждались и получили одобрение на всероссийских и международных конференциях, внедрены в практику.

Замечания

В качестве замечаний отмечено следующее:

1. В автореферате диссертации не описана предложенная автором архитектура измерительной системы, предназначенная для снятия данных об энергопотреблении чипа, что не позволяет в полной мере оценить полученные в диссертации результаты.

2. Отсутствует описание и условия проведения натурного эксперимента, подтверждающего приведенные в диссертации результаты, что позволяет усомниться в достоверности полученных результатов.

Однако замечания не снижают общего положительного мнения о качестве подготовленной диссертации. Исследование Тихонова С.В. обладает научной новизной, имеет практическую направленность и является завершенной работой.

Список публикаций и докладов на конференциях говорит о достаточно полном отражении проведенных исследований.

Автореферат отражает основные результаты диссертационной работы,

стиль изложения материала, последовательность и содержание соответствуют требованиям, предъявляемым ВАК РФ к диссертационным исследованиям.

Автор диссертации Тихонов С.В. заслуживает присуждения ему ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации информационная безопасность» (технические науки).

Профессор кафедры инфокоммуникационных систем и технологий
доктор технических наук, профессор
заслуженный работник высшей школы РФ
(специальность 05.13.19) Н.С. Хохлов

Доцент кафедры инфокоммуникационных систем и технологий
кандидат технических наук, доцент
(специальность 05.12.04) А.Н. Глушков

« 29 » ноября 2017 г.

ФГКОУ ВО «Воронежский институт МВД России»
Адрес: 394065, г. Воронеж, Проспект Патриотов, 53.
Телефон: 8 (473) 247-67-07
Факс: 8 (473) 200-55-00
E-mail: vrnin@mvd.ru

Подпись Хох
удостоверяю
начальник отдел
делопроизводств
Воронежского ин
МВД России