МИНИСТЕРСТВО ОБОРОНЫ РОССИЙСКОЙ ФЕДЕРАЦИИ (МИНОБОРОНЫ РОССИИ)

Федеральное государственное военное образовательное учреждение высшего образования «Военный учебно-научный центр Военно-Морского Флота «Военно-морская академия имени Адмирала Флота Советского Союза Н.Г. Кузнецова»»

ВОЕННЫЙ ИНСТИТУТ (ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ)
Юридический адрес: наб. Ушаковская, д. 17/1, Санкт-Петербург, 197045
Почтовый адрес: пр. Малоохтинский, 80/2, Санкт-Петербург, 195112
Тел. (812) 4443543, факс (812) 4443543, e-mail: vsok@vmanavy.ru

Экз. № 1

Председателю диссертационного совета
Д 999.121.03
ФГБОУ ВО «Санкт-Петербургский
государственный университет телекоммуникаций
им. проф. М.А. Бонч-Бруевича»
193232, Санкт-Петербург, пр. Большевиков, д.22,
корп. 1

УТВЕРЖДАЮ
Заместитель начальника Военного института ДПО
ВУНЦ ВМФ «Военно-морская академия»
по учебной и научной работе
кандидат военных наук, до[redacted]
Е. Пахомов
«8» 12 2017 г.

О Т З Ы В

Военного института ДПО ВУНЦ ВМФ «Военно-морская академия» на автореферат диссертационной работы ТИХОНОВА Сергея Владимировича « Исследование и разработка модификаций аппаратно-реализованных защитных блоковых преобразований, устойчивых к побочным атакам по цепям электропитания», представленной на соискание ученой степени кандидата технических наук по специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность».

В современных условиях при высоком уровне развития компьютерных технологий вопросам обеспечения безопасности систем, связанных с хранением, обработкой и передачей информации, уделяется значительное

внимание специалистов. Это является следствием разработки все более изощренных хакерских атак на такие системы, в первую очередь, направленных на взлом криптографической защиты, в основе которой лежат как симметричные, так и несимметричные методы шифрования. Именно это является предметом для первоочередного создания высокоэффективных систем защиты и обеспечения безопасности информации.

Вместе с тем, прекрасно разбираясь в названных системах и понимая общую тенденцию развития направлений защиты информации, злоумышленники ищут и находят наиболее уязвимые места, где обеспечена наименьшая степень безопасности инфокоммуникационных систем. Одной из таких слабых точек в электронных устройствах, где возможна организация эффективной атаки, являются цепи электропитания базовых функциональных блоков — интегральных чипов, выполняющих основные криптографические функции — шифрование и дешифрование информации.

В последнее время появились исследовательские работы, направленные на поиск методов защиты информации от атак по цепям электропитания, являющихся дополнительными каналами утечки информации, но в целом здесь еще остается масса нерешенных задач применительно к отечественным инфокоммуникационным системам. В связи с этим тема диссертационной работы С. В. Тихонова, в которой разрабатывается метод обеспечения безопасности информации в отечественных криптографических аппаратно-программных комплексах при атаках в цепи их электропитания, является актуальной, соответствует современному уровню развития науки и техники и практически значима для современных инфокоммуникационных систем, применяемых в государственных и коммерческих структурах.

Как видно из автореферата, работа С. В. Тихонова содержит новые научные результаты, основными из которых являются:

1. Модель «утечки» информации, обрабатываемой интегральным чипом, по цепи электропитания, основанная на результатах комплекса измерений.

2. Доказательство возможности успешного применения побочных атак по цепям электропитания к аппаратным реализациям шифров ГОСТ РФ.

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

Данные новые результаты представляют собой определенный вклад в теорию и практику современных систем обеспечения безопасности информации некриптографическими методами.

На наш взгляд, как видно из автореферата, более всего заслуживающим внимания специалистов является комплексное исследование, в том числе на основе натурного эксперимента, теоретических и практических аспектов реализации атаки на интегральные чипы,

представляющие собой ядро систем обработки и хранения важной информации. Интересным и перспективным, по нашему мнению, также является применение для оценки эффективности атак аппарата теории помехоустойчивого кодирования, что может получить дальнейшее развитие при последующих исследованиях и разработках. Практически значимыми являются предложения автора по реализации аппаратно-программного измерительного комплекса для оценки степени защищенности реальных инфокоммуникационных систем.

Вместе с тем, по автореферату можно сделать следующие замечания:

1. Для оценки эффективности защиты от атак автор применяет весовые характеристики и расстояние по Хэммингу, но отсутствуют вероятностные оценки эффективности защиты.

2. В четвертой главе своей работы автор предлагает реализацию защиты информации при использовании шифра «Кузнечик» на основе модификации метода балансировки, но нет оценки ее эффективности. Фраза в автореферате: «В целом, требования предложенного метода защиты к дополнительным аппаратным ресурсам чипа можно считать весьма небольшими по сравнению с известными аналогами» не проясняет величину достигаемого эффекта и затрудняет определение сложности и особенностей проектирования для практического применения.

3. Не ясным остается вопрос, каким образом в цепях электропитания с напряжением 220 В и с переменным током 50 Гц удается регистрировать скачки напряжения в интегральных чипах, измеряемые в микровольтах.

4. В автореферате имеются грамматические ошибки и не объясненные аббревиатуры.

Отмеченные недостатки, хотя и несколько снижают общее позитивное впечатление о работе, но не являются определяющими при оценке автореферата диссертации, которая, по нашему мнению, заслуживает итоговой положительной оценки. Видно, что диссертация является завершенным, целостным научно-квалификационным трудом. Материалы диссертации в достаточной степени апробированы на международных научных конференциях и опубликованы в научных трудах по перечню ВАК.

Безусловно, следует считать, что работа соискателя Сергея Владимировича Тихонова отвечает требованиям «Положения о порядке присуждения ученых степеней», и он заслуживает присуждения ему ученой степени кандидата технических наук.

Выводы

Судя по автореферату, можно сделать вывод о том, что диссертационная работа Тихонова Сергея Владимировича на тему «Исследование и разработка модификаций аппаратно-реализованных защитных блоковых преобразований, устойчивых к побочным атакам по

цепям электропитания» является законченной научно-квалификационной работой. Работа отвечает требованиям ВАК РФ, предъявляемым к кандидатским диссертациям и паспорту специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность», а ее автор достоин присуждения ученой степени кандидата технических наук.

Отзыв составил:
Доцент кафедры боевого применения средств связи
Военного института ДПО ВУНЦ ВМФ «Военно-морская академия»
кандидат технических наук, доцент

Мазепа Валерий Андреевич

Отзыв рассмотрен на заседании кафедры боевого применения средств связи Военного института ДПО ВУНЦ ВМФ «Военно-морская академия», протокол № 4/17 от 30 ноября 2017 г.

Начальник кафедры боевого применения средств связи
Военного института (дополнительного профессионального образования)
ВУНЦ ВМФ «Военно-морская академия»

Пучко Евгений Валентинович