Экз. № 1

УТВЕРЖДАЮ
Заместитель начальника Академии
ФСО России
доктор социологических наук,
профессор

В.И. Козачок

"11" декабря г.

ОТЗЫВ

на автореферат диссертационной работы Тихонова Сергея Владимировича на тему: «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"

Побочные атаки на сегодняшний день являются наиболее действенным методом взлома программно-аппаратных систем, содержащих в своём составе блоки, выполняющие процедуры идентификации и аутентификации. Защититься от таких атак значительно сложнее, по сравнению с «классическими» криптографическими атаками, так как они предполагают использование утечек информации при аппаратной реализации алгоритма, перекрыть которые полностью является чрезвычайно нетривиальной задачей. Наиболее действенной и эффективной в реализации является побочная атака, использующая утечку информации по цепи электропитания чипа (в частности атака DPA). Такая атака позволяет, на примере известных зарубежных защитных преобразований (DES, AES), извлечь секретный ключ выполняемого чипом шифра за несколько часов, причём не требуется использования значительных вычислительных ресурсов, а общие вложения в оборудование являются относительно небольшими. Задача исследования побочных атак по цепям электропитания применительно к отечественным шифрам ГОСТ является чрезвычайно актуальной для области информационной безопасности. В частности, тема диссертации Тихонова С.В. является весьма актуальной ещё и за счёт того, что не-

смотря на активные исследования в этой области за рубежом, в отечественной литературе до сих пор отсутствовали открыто опубликованные комплексные исследования по данному направлению.

Цель исследования диссертации состояла в повышении безопасности информационно-коммуникационных технологий в части реализации защитных преобразований, выполняемых интегральными чипами. Из автореферата следует, что в ходе достижения цели исследования автором получены следующие научные результаты, выносимые на защиту:

1) Архитектура средства моделирования побочных атак по цепям электропитания. Модель «утечки» информации, обрабатываемой интегральным чипом, по цепи электропитания, основанная на результатах проведённого комплекса измерений.

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

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

Полученные научные результаты имеют несомненную практическую ценность и теоретическую значимость. Их обоснованность и достоверность основаны на строгих теоретических доказательствах, результатах моделирования и эксперимента, более того, подкрепляется актом о внедрении и публикациями в рецензируемых изданиях. Необходимо особо отметить как общее количество публикаций, так и то, что, что половина всех работ написана Тихоновым С.В. лично. Все это характеризует автора как научного исследователя, обладающего достаточной степенью квалификации и самостоятельности.

Новизна диссертационной работы определяется следующими факторами:

1) Предложена архитектура измерительной установки, представляющей собой отдельную плату с АЦП. Что позволяет значительно сократить расходы на оборудование, требующееся для реализации атаки и делает исследования в этой области более доступными.

2) Существенно дополнена модель атаки DPA детальными экспериментальными данными исследования утечек информации от реального чипа.

3) Оценена эффективность реализации атаки DPA при использовании расчёта ковариационных и корреляционных векторов.

4) Представлена модель атаки DPA на российские блочные шифры ГОСТ, произведено сравнение эффективности реализации атаки на эти шифры и осуществлён натурный эксперимент взлома реализованного на чипе шифра ГОСТ.

5) Разработан оригинальный метод защиты от атак DPA, обладающий такими преимуществами над известными аналогами как универсальность, скорость и относительно низкие требования к дополнительным аппаратным ресурсам чипа.

Судя по автореферату, материалы диссертации достаточно полно опубликованы в 13 научных трудах, из которых 6 размещены в изданиях, рекомендованных ВАК при Минобрнауки, прошли широкую апробацию на всероссийских, межвузовских и межведомственных научно-технических конференциях. В качестве недостатков (на сколько можно судить по автореферату) необходимо отметить:

1) В качестве вывода по работе, в первую очередь, следует предложить нашей промышленности, для реализации программ импортозамещения, наладить выпуск отечественных чипов, в которых, в качестве базовых элементов используются не усилители с общим эмиттером, а дифференциальные, позволяющие на самом низком уровне обеспечить компенсацию не только утечек по электропитанию, но и излучения по ПЭМИ и Н.

2) В работе справедливо замечено, что эффективность криптоанализа аппаратных реализаций отечественных шифров сильно зависит от способа их реализации. Кроме того, все производители при выполнении программной или аппаратной реализации «приспосабливают» соответствующий алгоритм для достижения предъявляемых требований. В этой связи, автору следовало рассмотреть эффективность анализа не только своей реализации, но и оценить уязвимость других «приспособленных» алгоритмов, например описанных в материалах Mikhail Borodin, Andrey Rybkin, Alexey Urivskiy «High-Speed Software Implementation of the Prospective 128-bit Block Cipher and Streebog Hash-Function», 3rd Workshop on Current Trends in Cryptology (CTCrypt 2014), pp 189 – 197.

3) В автореферате имеются недостатки, связанные с ясностью излагаемых суждений так:

– на третьей странице, при описании научной новизны и практической значимости (в первых пунктах) автор указывает, что для снятия данных об энергопотреблении чипа, вместо осциллографа, он предлагает использовать АЦП. Учитывая тот факт, что АЦП входит в состав любого осциллографа, возникает некоторая путаница;

– на рисунке 1 дана блок-схема измерительной установки, однако не описывается назначение приведённых на рисунке узлов;

– в таблицах 2 и 3 непонятно, какая модель используется при совершении атаки с использованием комбинации сохраняемой в предварительно заполненную ячейку: модель расстояния или веса Хэмминга.

Перечисленные замечания не снижают научной, теоретической и практической ценности работы и не изменяют общей положительной оценки полученных научных результатов.

ВЫВОД:

В целом, судя по автореферату и публикациям автора, диссертационная работа выполнена на достаточном научно-техническом уровне. Содержание диссертации соответствует специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность». Несмотря на отмеченные недостатки, диссертационная работа как квалификационный труд по новизне, научному уровню и практической значимости отвечает требованиям «Положения о присуждении ученых степеней», предъявляемым к кандидатским диссертациям, а ее автор, Тихонов Сергей Владимирович, заслуживает присуждения ученой степени кандидата технических наук.

Отзыв рассмотрен и одобрен на заседании кафедры. Протокол № 6 от 05.12.2017 г.

Сотрудник
кандидат технических наук, доцент

Борисенко Николай Павлович

«11» декабря 2017 г.

Наши реквизиты: федеральное государственное казенное военное образовательное учреждение высшего образования «Академия Федеральной службы охраны Российской Федерации»
юр. адрес: ул. Приборостроительная, 35, Орёл, 302015, тел. 8(4862) 54-95-27, факс: 8(4862) 54-95-27, E - mail: sec@academ.msk.rsnet.ru