ОТЗЫВ

об автореферате диссертации Таранникова Ю. В. на тему: «Конструкции и свойства корреляционно-иммунных и платовидных булевых функций» на соискание ученой степени доктора физико-математических наук по специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность»

В наше время одним из наиболее важных и распространенных способов защиты информации является использование криптографических шифров, в которых роль одного из ключевых использующихся примитивов часто играют булевы функции. В зависимости от типов рассматриваемых шифров, на них предложены различные криптографические атаки. Эти атаки используют определенные параметры входящих в шифр компонент, в частности, булевых функций, как средство для эффективного нахождения ключа. Существует много криптографических атак, которые позволяют противнику, если фильтр выбран неподходящим образом, эффективно раскрыть ключ. Среди таких атак наиболее распространены корреляционные атаки. Поэтому разработка конструкций и изучение свойств криптографически важных классов булевых функций, в частности, корреляционно-иммунных и платовидных, является важной целью как в теоретическом, так и практическом отношении.

В этой связи тема диссертации Таранникова Ю.В., посвящённая обеспечению стойкости систем защиты информации против корреляционных криптографических атак в математических моделях информационной безопасности, является актуальной с позиции развития теории и практики методов защиты информации и информационной безопасности.

К достоинствам диссертации можно отнести следующее.

Во-первых, автор разработал новые методы построения устойчивых булевых функций с максимально высокой для данного порядка устойчивости нелинейностью и предложил эффективные способы их схемной и программной реализации.

Во-вторых, в работе предложено много новых сильных оценок на криптографически важные параметры булевых функций.

В-третьих, в диссертации получены результаты о математических объектах, как являющихся промежуточным звеном для построения криптографически важных булевых функций, так и представляющих самостоятельное значение.

Эти и другие элементы составляют научную суть рецензируемой диссертации и являются новыми научными результатами.

Вместе с тем, целесообразно сформулировать некоторые критические пожелания по содержанию автореферата, в частности имеется некоторое количество опечаток, повторяющихся слов и ссылок, некоторые определения даны не совсем привычным образом. Например, несколько странным выглядит то, что несущественная

переменная считается нелинейной (как видно из формулировки теоремы 3.12), хотя это, может быть, и удобно с точки зрения компактности представления результатов и изложения доказательств.

Эти замечание не затрагивает научной сути диссертации, а скорее касаются способа изложения материалов диссертации в автореферате. В целом диссертация Таранникова Ю.В. на тему: «Конструкции и свойства корреляционно-иммунных и платовидных булевых функций» соответствует требованиям, предъявляемым к диссертациям на соискание учёной степени доктора физико-математических наук, содержит новые научные результаты и развивает теорию и практику методов защиты информации.

Учитывая все вышеизложенное, считаю, что Таранников Ю.В. заслуживает присуждения ученой степени доктора физико-математических наук по специальности 2.3.6 – Методы и системы защиты информации, информационная безопасность.

д.т.н., профессор, главный научный сотрудник ФГУП НИИ “КВАНТ”

Корнеев Виктор Владимирович

тел.: 499 153 47 00
адрес: 125438 Москва, 4-й Лихачёвский пер., д. 15
электр. адрес: korv@rdi-kvant.ru

Подпись Корнеева В.В. заверяю