ОТЗЫВ официального оппонента
на диссертацию на соискание ученой степени
кандидата физико-математических наук
Карелиной Екатерины Константиновны
на тему: «Методы синтеза корреляционно-иммунных функций
на основе минимальных функций»
по специальности 2.3.6 — методы и системы защиты информации,
информационная безопасность

Актуальность исследования. Диссертация Карелиной Екатерины Константиновны «Методы синтеза корреляционно-иммунных функций на основе минимальных функций» посвящена вопросам разработки методов построения корреляционно-иммунных и минимальных корреляционно-иммунных функций с заданными метрическими и криптографическими характеристиками, а также изучению ряда свойств указанных функций и их множеств. В настоящее время наблюдается широкое распространение информационных систем во многих областях жизни и деятельности общества и человека. В связи с этим особое значение приобретает обеспечение безопасности применения таких систем как для отдельных людей, так и для общества в целом. Разрабатываются различные подходы, обеспечивающие определенный уровень безопасности информационных систем, в частности, изучается построение подходящих математических моделей и их свойств. Среди прочих рассматриваются модели, которые опираются на булевы функции, имеющие определенные криптографические свойства (уравновешенность, нелинейность, корреляционная иммунность, алгебраическая иммунность, др.). Криптографические свойства булевых функций исследуются в множестве современных работ как в нашей стране, так и за рубежом. Одним из криптографических свойств функций является корреляционная иммунность. Содержательно корреляционная иммунность булевой функции описывает устойчивость функции к корреляционной атаке (T.Siegenthaler, 1985). Свойства корреляционно-иммунных булевых функций, в том числе в соединении с другими свойствами функций, а также вопросы

порождения таких функций рассматривались в работах T.Siegenthaler, P.Camion, C.Carlet, C.-K.Wu, E.Dawson, A.Bernasconi, О.В.Денисова, А.А.Ботева, Ю.В.Таранникова, Е.К.Алексеев, О.А.Логачева и др. Следовательно, тема диссертационного исследования является актуальной.

Содержание работы. Диссертация состоит из введения; четырех глав, разбитых на разделы; заключения; списка литературы и приложения. Во ***введении*** сначала обосновывается актуальность исследования и приводится обзор работ, в которых изучаются корреляционно-иммунные булевы функции и методы построения таких функций. Затем описываются цели и задачи диссертационного исследования; положения, которые выносятся на защиту, и их практическая значимость; публикации и апробация работы. Далее приводится изложение содержания работы по главам и разделам. ***Первая глава*** диссертации целиком посвящена введению основных определений и утверждений, относящихся к булевым функциями, корреляционной иммунности функций и необходимым смежным понятиям. ***Вторая глава*** посвящена описанию основного разработанного диссертантом метода построения корреляционно-иммунных и минимально корреляционно-иммунных булевых функций. Сначала приводится описание метода, его обоснование и доказательство ряда его свойств, а также разбираются примеры применения его основного отображения к некоторым корреляционно-иммунным функциям (разделы 2.1–2.3). Затем доказывается критерий равенства получаемых функций (раздел 2.4), на основании которого находятся верхние и нижние оценки мощности множества корреляционно-иммунных функций, порожденного применением основного отображения этого метода к заданной корреляционно-иммунной функции (разделы 2.5 и 2.6). Далее применением основного отображения совместно с последующим суммированием получаемых корреляционно-иммунных функций с непересекающимися носителями построены некоторые корреляционно-иммунные функции от 7, 8, 9, 10 и 11 переменных,

обладающие дополнительными криптографическими характеристиками (раздел 2.7). Раздел 2.8 целиком посвящен классификации корреляционно-иммунных булевых функций от 4, 5 и 6 переменных относительно группы Джевонса, в том числе минимальных функций. В ***третьей главе*** изучаются свойства минимальных корреляционно-иммунных функций. В частности, обоснованы достаточное условие существования минимальных корреляционно-иммунных функций заданного веса (раздел 3.1), критерий минимальности корреляционно-иммунной функции (раздел 3.2) и существенность переменных таких функций (раздел 3.3); уточнена верхняя оценка веса минимальной корреляционно-иммунной функции (раздел 3.4). В разделах 3.5 и 3.6 приводятся некоторые возможности усложнения имеющихся функций с помощью минимальных корреляционно-иммунных функций и найдены разложения корреляционно-иммунных функций от 4 и 5 переменных на минимальные корреляционно-иммунные функции. В ***четвертой главе*** найдены верхние оценки числа корреляционно-иммуннных функций заданного веса, а также асимптотики этого числа при росте числа переменных функций. В ***заключении*** приведены основные результаты диссертации и выводы. ***Список литературы*** содержит 45 наименований. ***Приложение*** содержит таблицы корреляционно-иммунных (представителей классов эквивалентности) и минимальных корреляционно-иммунных функций от 4 переменных с их основными криптографическими характеристиками (разделы 4.4 и 4.5); таблицы мощностей множеств корреляционно-иммунных функций, полученных применением основного отображения разработанного метода к корреляционно-иммунным функциям от 4, 5 и 6 переменных некоторых весов (раздел 4.6). Объем диссертации составляет 125 страниц, из которых страницы 110–125 занимает приложение.

Научная новизна, обоснованность и достоверность положений работы. На мой взгляд, основными достижениями исследования являются разработка метода построения корреляционно-иммунных и минимальных

корреляционно-иммунных булевых функций, а также построение с помощью этого метода таблиц корреляционно-иммунных функций с определенными свойствами. Привлекательность применения этого метода заключается в простоте и прозрачности его составляющих, а именно, основного отображения и суммирования функций с непересекающимися носителями. Метод позволяет развивать исследование корреляционно-иммунных функций, являющихся минимальными (понятие минимальных корреляционно-иммунных функций введено в работе Е.К.Алексеева, 2010). В диссертации показаны возможности применения этого метода. В частности, диссертация содержит большое число таблиц корреляционно-иммунных и минимальных корреляционно-иммунных функций, полученных компьютерными вычислениями с применением разработанного метода. Эти таблицы могут быть полезны для практического применения. Список литературы отражает состояние дел в области исследований, относящихся к корреляционно-иммунным функциям. Достоверность результатов работы подтверждается их публикациями в ведущих научных журналах, а также их представлениями на научных семинарах и на международной конференции. Автореферат правильно отражает содержание работы.

Замечания по работе.

1. Можно было бы провести сравнение разработанного метода построения корреляционно-иммунных булевых функций с существующими другими методами решения этой задачи (например, по характеристикам получающихся функций, по мощности получаемых множеств функций и т.д.).

2. Часть результатов получена при помощи компьютерных вычислений (например, результаты в разделах 2.7, 2.8, 3.5, 3.6, 4.3–4.6). Однако в работе об этом не написано явно; не указана информация о программах, о характеристиках вычислительной техники и о том, где эти результаты опубликованы. Кроме того, не указано, какие из полученных корреляционно-

иммунных функций были известны ранее, а какие из них найдены впервые (в частности, для функций из разделов 2.7 и 3.5).

3. Можно было бы в начале каждого раздела указать, в какой статье автора опубликованы основные результаты этого раздела.

4. На стр. 16 указаны опубликованные статьи автора с соавторами. Однако сначала приведены выходные данные статьи только с одним автором — автором диссертации, а затем — выходные данные статьи со всеми соавторами. Непонятно, зачем так сделано.

5. На стр. 16–17, где указаны статьи автора диссертации с соавторами, описаны результаты в статьях, которые получили соавторы. Обычно в таких случаях выделяют и описывают результаты автора диссертации.

6. На источники 3, 16, 27, 28, 34, 36, 43 из списка литературы отсутствуют ссылки в тексте работы.

7. Некоторые замечания по оформлению работы:

1) не введены некоторые определения и обозначения (например, определения лексико-графического порядка, полинома Жегалкина, расстояния до множества функций; обозначение <x,u> в разделе 1.1);

2) при ссылках на теоремы, предложения, др. слова «теорема», «предложение», др. написаны с большой буквы (например, на стр. 27, 36, 48, 51, 53, 56, 64, 71, 97, 99), но в научных работах на русском языке эти слова пишутся с маленькой буквы;

3) в некоторых строках оставлен большой пустой промежуток справа (например, на стр. 7, 14, 15, 20, 31, 38, 39); а также другие мелкие замечания.

Однако указанные замечания являются несущественными и не снижают общего положительного впечатления о диссертационном исследовании и его значимости.

Заключение. Оценивая работу в целом, отмечу, что диссертация Карелиной Екатерины Константиновны «Методы синтеза корреляционно-иммунных функций на основе минимальных функций» является завершенным научным

исследованием, в котором получены новые важные результаты в области исследования и построения корреляционно-иммунных функций. Диссертация отвечает требованиям, установленным Московским государственным университетом имени М.В.Ломоносова к работам подобного рода. Содержание диссертации соответствует специальности 2.3.6 — методы и системы защиты информации, информационная безопасность (по физико-математическим наукам), а именно, следующим направлениям:

1. Теория и методология обеспечения информационной безопасности и защиты информации;

19. Исследования в области безопасности криптографических алгоритмов, криптографических примитивов, криптографических протоколов. Защита инфраструктуры обеспечения применения криптографических методов;

а также критериям, определенным пп. 2.1–2.5 Положения о присуждении ученых степеней в Московском государственном университете имени М.В.Ломоносова; работа оформлена согласно требованиям Положения о совете по защите диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук Московского государственного университета имени М.В.Ломоносова. Таким образом, соискатель Карелина Екатерина Константиновна заслуживает присуждения ученой степени кандидата физико-математических наук по специальности 2.3.6 — методы и системы защиты информации, информационная безопасность.

Официальный оппонент:

доктор физико-математических наук,
профессор кафедры математической кибернетики
факультета вычислительной математики и кибернетики
федерального государственного бюджетного
образовательного учреждения высшего образования
«Московский государственный университет имени М.В.Ломоносова»

Селезнева Светлана Николаевна

10.12.2024 г.

Контактные данные:

Специальность, по которой официальным оппонентом
защищена диссертация:
01.01.09 – дискретная математика и математическая кибернетика

Адрес места работы:

119991, ГСП-1, Москва, Ленинские горы, МГУ имени М.В. Ломоносова, д. 1, стр. 52, 2-й учебный корпус, факультет ВМК,
Московский государственный университет имени М.В. Ломоносова,
факультет вычислительной математики и кибернетики,

Подпись сотрудника факультета вычислительной математики и кибернетики
Московского государственного университета имени М.В.Ломоносова
Селезневой Светланы Николаевны удостоверяю:

Декан факультета ВМК МГУ
академик РАН

М.В. Ломоносова
И.А. Соколов