САНКТ-ПЕТЕРБУРГСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И

ОПТИКИ

На правах рукописи

Таранов Сергей Владимирович

**МЕТОДЫ ОБЕСПЕЧЕНИЯ ЦЕЛОСТНОСТИ
ИНФОРМАЦИИ НА ОСНОВЕ ВЕЙВЛЕТНЫХ
ПРЕОБРАЗОВАНИЙ ДЛЯ ЗАЩИТЫ СРЕДСТВ
ХРАНЕНИЯ ИНФОРМАЦИИ**

Специальность 05.13.19 —Методы и системы защиты информации,

информационная безопасность

Диссертация на соискание учёной степени
кандидата технических наук

Научный руководитель: кандидат физико-математических наук Левина Алла Борисовна

Санкт-Петербург — 2018

Оглавление

Стр.

[Введение 4](#bookmark1)

[Глава 1. Коды, ориентированные на безопасность, как метод](#bookmark3)

[обеспечения целостности в средствах хранения данных](#bookmark3) 13

1. [Модель алгебраических манипуляций 13](#bookmark5)
2. [Моделирование угроз для средств хранения информации 15](#bookmark9)
3. [Модель угроз для средств хранения данных в](#bookmark10)

соответствии с отечественными стандартами 16

1. [Построение модели угроз для средств хранения](#bookmark13)

информации на основе CIAA подхода 22

1. [Обзор существующих средств и методов обеспечения](#bookmark17)

[целостности информации 28](#bookmark19)

1. [Помехоустойчивое кодирование как метод защиты информации . 31](#bookmark21)
2. [Линейные коды и основные принципы помехоустойчивого](#bookmark24)

[кодирования 37](#bookmark26)

1. [Нелинейные надежные коды Марка Карповского, их применение](#bookmark31)

для защиты информации 42

1. [Коды, обнаруживающие алгебраические манипуляции 46](#bookmark36)
2. [Линейные коды с комплементарной дуальностью 49](#bookmark38)
3. [Выводы к 1 Главе 51](#bookmark44)

[Глава 2. Построение новых методов обеспечения целостности](#bookmark45)

на основе вейвлетных разложений 52

1. [Вейвлетные преобразования и их применение в кодах 53](#bookmark47)
2. [Построение линейных кодов на основе вейвлетных преобразований](#bookmark57) 56
3. [Построение надежных кодов на основе вейвлетных линейных кодов](#bookmark68) 60
4. [Конструкции кодов, обнаруживающих алгебраические](#bookmark74)

манипуляции, на основе вейвлетных разложений 63

1. [Коды, исправляющие ошибки, на основе сплайн-вейвлетных](#bookmark84)

[разложений второго порядка 68](#bookmark86)

1. [Проверка устойчивости разработанных конструкций к](#bookmark100)

изменениям в распределении входных кодовых слов 76

1. [Выводы ко 2 Главе 90](#bookmark116)

[Глава 3. Практические рекомендации по применению](#bookmark117)

разработанных кодовых конструкций 91

1. [Применение разработанных конструкций для защиты средств](#bookmark119)

хранения, использующих технологию NAND флеш 91

1. [Области использования NAND флеш памяти 91](#bookmark122)
2. [Методы обнаружения и исправления ошибок,](#bookmark123)

применяемые для защиты NAND флеш 94

1. [Программно-аппаратная система обнаружения ошибок в](#bookmark128)

системе сжатия и обработки видео ADV612 98

* 1. [Другие области применения вейвлетных AMD кодов 107](#bookmark140)
		1. [Защита кэш-памяти микропроцессора 107](#bookmark141)
		2. [Защита линейных частей криптоалгоритмов при атаках](#bookmark147)

[на основе внедрения ошибок 113](#bookmark149)

* 1. [Общие рекомендации по применению разработанных методов](#bookmark150)

[обеспечения целостности 116](#bookmark152)

* 1. [Выводы к 3 Главе 118](#bookmark154)

[Заключение 119](#bookmark155)

[Список сокращений и условных обозначений 120](#bookmark158)

[Список литературы 122](#bookmark159)

[Приложение А. Листинги программного кода для анализа и](#bookmark228)

моделирования предлагаемых методов обеспечения целостности 131

[Приложение Б. Параметры кодовых конструкций на основе](#bookmark230)

вейвлетных разложений 159

Приложение В. Акты о внедрении 162

Введение

Актуальность темы исследования. В настоящее время помехоустой­чивое кодирование является одним из основных методов обеспечения целостно­сти информации. Коды, обнаруживающие и исправляющие ошибки, применя­ются в средствах хранения, обработки и передачи данных уже на протяжении многих лет. В связи с постоянно растущими объемами информации и повышени­ем требований к ее целостности задача построения новых кодовых конструкций с лучшими показателями скорости кодирования и надежности, а также разра­ботка механизмов, улучшающих существующие коды, остается актуальной.

Одним из недостатков, с точки зрения безопасности, у существующих ме­тодов обеспечения целостности является их способность обнаруживать наибо­лее вероятные ошибки при условии определенных ограничений таких, как рав­номерное распределение входных значений для защищаемого средства. Кроме того, ограничением в стандартных подходах является независимость внедряе­мых ошибок от внешних факторов, влияющих на защищаемое средство, в каче­стве таких факторов могут выступать действия злоумышленника или воздей­ствие со стороны технического средства. Именно поэтому стандартные методы не подходят для случаев, когда закон распределения внедряемых ошибок не может быть точно спрогнозирован или контролируется злоумышленником. В связи с этим использование технических решений и научно-методического ап­парата обеспечения информационной безопасности средств хранения информа­ции затруднено вследствие особой структуры объектов защиты, моделей угроз и злоумышленника.

Коды, ориентированные на безопасность, способны обнаруживать ошибки любой кратности с ненулевой вероятностью. Основными параметрами данного типа кодов являются множество необнаруживаемых ошибок *R(e)* (количество кодовых слов для рассматриваемой ошибки, которые она маскирует), скорость кода *к/п* (отношение количества информационных символов к общей длине), максимальное значение вероятности маскировки ошибки *Q(e)* (отношение ко­личества маскируемых кодовых слов к общему числу кодовых слов). Коды, ори­ентированные на безопасность, направлены на минимизацию параметров *R(e)* и *Q(e)* и достижению как можно большей скорости кода *к/п.* Параметры, пред­ставленные выше, позволяют оценить опасность внедрения ошибки злоумыш­ленником. Использование линейных структур в стандартных методах помехо­устойчивого кодирования приводит к тому, что атакующий имеет возможность, проанализировав вероятность маскировки ошибки, внедрить ошибку в устрой­ство хранения и исказить хранящуюся в данном устройстве информацию.

Ранние исследования кодов, ориентированных на безопасность, предпо­лагают, что все кодовые слова появляются на входе защищаемого устройства с равной вероятностью. Однако, если некоторые кодовые слова имеют низкую вероятность быть отправленными/полученными, то ошибки, маскирующие ко­довые слова, не будут обнаружены, либо вероятность их обнаружения будет крайне мала. Таким образом, коды, ориентированные на безопасность, которые были созданы для обеспечения целостности при равномерном законе распре­деления вероятности появления кодовых слов, будут малоэффективны в слу­чае неравномерного распределения. Данная диссертационная работа предлагает использовать вейвлетные коды и дополнительные преобразования (такие, как маскирование, перестановки, преобразование Грея) для обеспечения целостно­сти, если кодовые слова появляются в соответствии с неравномерным законом распределения вероятности.

Согласно ФСТЭК СТР-К от 2001 года *целостностью информации* на­зывается устойчивость информации к несанкционированному или случайному воздействию на нее в процессе обработки техническими средствами, результа­том которого может быть уничтожение или искажение информации. Целост­ность информации в средствах обработки, передачи и хранения информации определяется целостностью всех компонентов системы, а также способностью сохранять целостность при несанкционированном или случайном воздействии техническими средствами. Выделим *объекты защиты,* для которых исследуе­мые и разработанные методы обеспечения целостности информации являются наиболее актуальными:

* Кэш память процессоров, оперативная память, флеш-память (из-за вы­сокой скорости работы данных типов памяти применение в них крип­тографических методов обеспечения целостности затруднено, так как сильно влияет на производительность);
* Арифметические и логические операции в микропроцессорах и микро­схемах;

— Технические средства хранения данных, для которых актуальны угро­зы типа: внедрение ошибок, коррелированных со входными данными; координированное изменение внутреннего состояния и внешних фак­торов. В этом случае предлагаемые методы обеспечения целостности обычно идут как составная часть некоторого подхода, например, схемы одновременного обнаружения ошибок (concurrent error detection).

Степень разработанности темы. Все известные подходы к обеспече­нию целостности информации при неравномерном распределении входных ко­довых слов можно разделить на две группы:

1. Создание новых кодов, способных обнаруживать любые ошибки с неко­торой вероятностью без каких-либо дополнительных ограничений (тру­ды М. Карповского, Р. Крамера и других [[1](#bookmark161)[-7]](#bookmark167));
2. Корректировка входных значений с целью их согласования с требова­ниями стандартных методов помехоустойчивого кодирования (работы В.И. Коржика, К. Оснат и других [[8]](#bookmark168)).

Первая группа подходов - это коды, обнаруживающие любую комбинацию ошибок с отличной от нуля вероятностью. Одними из первых кодовых кон­струкций, способными функционировать в модели с алгебраическими манипу­ляциями, являются *надежные коды* Марка Карповского [[2](#bookmark162)[-5]](#bookmark165). В конструкциях Карповского предлагается использовать PN и APN функции, как наиболее оп­тимальные функции кодирования для обнаружения аддитивных ошибок любой комбинации. В работах Рональда Крамера и его учеников [[1](#bookmark161); [6](#bookmark166); [7]](#bookmark167) предлагаются конструкции нелинейных кодов, обобщающие теорию надежных кодов М. Кар- повского и использующие вероятностное кодирование с целью усложнить атаки злоумышленника на модель алгебраических манипуляций. Коды, предложен­ные Р. Крамером, получили название *кодов, обнаруживающих алгебраические манипуляции (AMD коды).* Различные конструкции AMD кодов продолжают исследоваться и находят широкое применение для обеспечения целостности со­временных средств хранения информации.

Вторая группа подходов - разработка преобразований входных значений с целью их согласования с корректирующими способностями методов помехо­устойчивого кодирования. Поискам согласующих преобразований посвящены работы О. Керен и И. Шумского [[8](#bookmark168); [9]](#bookmark0), Е.Т. Мирончикова и М.О. Алексее­ва [[10](#bookmark169)[-12]](#bookmark170), Л.М. Финка и В.И. Коржика [[13]](#bookmark171). Примерами согласующих преоб­разований являются согласование метода модуляции сигнала и помехоустойчи­вого кода (Л.М. Финк, В.И. Коржик [[13]](#bookmark171)), декорреляция, преобразование Грея входных значений в предопределенное множество (О. Керен [[8]](#bookmark168)).

В рамках диссертационной работы преимущественно рассматривается первый подход, для которого характерно использование APN и PN функций в качестве основной составляющей метода кодирования. Представленные ко­довые конструкции, построенные на вейвлетных разложениях, позволяют до­биться высокой скорости кодирования информации, а также обеспечивают воз­можность обнаружения и исправления ошибок в средствах, использующих вей- влетные преобразования (видеокодеки, средства сжатия и хранения видео и изображений) [[14](#bookmark172); [15]](#bookmark173).

Цели и задачи. Целью исследования является снижение вероятности маскировки ошибки в устройствах хранения информации при неравномерном распределении входных кодовых слов.

Для достижения поставленной цели были решены следующие частные за­дачи:

1. Проанализированы потенциальные угрозы нарушения целостности ин­формации для устройств хранения информации, а также существу­ющие методы обеспечения целостности для защиты от выделенных угроз;
2. Исследованы основные показатели существующих методов обеспечения целостности, использующихся для оценки устойчивости при неравно­мерном распределении входных кодовых слов такие, как вероятность маскировки ошибки, множество необнаруживаемых ошибок, надеж­ность;
3. Разработаны методы обеспечения целостности на основе сплайн вей- влетных преобразований второго порядка;
4. Разработаны методы обеспечения целостности на основе вейвлетных преобразований, APN и PN функций;
5. Исследованы характеристики разработанных методов, проведено срав­нение с существующими аналогами, исследовано поведение конструк­ций в случае неравномерного распределения входных значений;
6. Сформированы практические рекомендации для применения разрабо­танных методов в целях обеспечения целостности информации в тех­нических средствах хранения.

Научной задачей является разработка методов обеспечения целостности информации, способных обнаруживать ошибки в средствах хранения инфор­мации в случае алгебраических манипуляций и имеющих низкую вероятность маскировки ошибок при неравномерном распределении входных кодовых слов.

Объектом диссертационного исследования являются средства хранения информации, для которых актуальны угрозы нарушения целостности на основе алгебраических манипуляций.

Предметом исследования являются методы обеспечения целостности ин­формации для средств хранения информации.

Научная новизна. Научная новизна основных научных результатов со­стоит в следующем:

1. Предлагаемый метод обеспечения целостности информации на основе вейвлетных линейных кодов, в отличие от известных методов, исполь­зует формулы декомпозиции и реконструкции сплайн-вейвлетных раз­ложений второго порядка, а также их сводимость, при определенных ограничениях, к совершенно нелинейной функции;
2. Предлагаемый метод обеспечения целостности на основе вейвлетных нелинейных кодов, в отличие от существующих методов, использует теорию вейвлетных преобразований в конечных пространствах, совер­шенно нелинейные и почти совершенно нелинейные функции, что в ито­ге позволяет обеспечить защиту от атак на основе алгебраических ма­нипуляций при неравномерном распределении входных кодовых слов, усложнить проведение злоумышленником атак, целью которых явля­ется раскрытие функции кодирования, а также повысить максимум ве­роятности маскировки ошибки при неравномерных распределениях;
3. Предлагаемые рекомендации позволяют внедрить разработанные мето­ды обеспечения целостности в средствах хранения информации с уче­том возможности реализации угроз нарушения целостности, использу­ющих зависимости между входными значения и ошибками.

Теоретическая и практическая значимость работы. Теоретическая значимость научных положений, изложенных в работе, состоит в следующем:

* предлагаемый метод обеспечения целостности информации на основе вейвлетных линейных кодов развивает и дополняет теорию кодов, об­наруживающих алгебраические манипуляций в том числе для случая неравномерного закона распределения входных кодовых слов;
* теоретическая значимость второго результата заключается в том, что полученный результат развивает и дополняет теорию кодов, обнаружи­вающих алгебраические манипуляций, теорию PN и APN функций, а также теорию вейвлетных кодов над конечными пространствами;
* теоретическая значимость практических рекомендаций заключается в том, что они расширяют существующий научно-методический аппарат по использованию, настройке и модификациям кодов, ориентированных на защиту от алгебраических манипуляций.

Практическая значимость исследований, проведенных в диссертации, со­стоит в следующем:

* разработанные методы обеспечения целостности информации могут быть использованы в средствах обработки и хранения информации с целью повышения устойчивости к изменениям распределений входных кодовых слов;
* полученные в данной диссертационной работе алгоритмы оценки веро­ятности маскировки ошибок могут применяться для анализа нелиней­ных функций кодирования, в том числе PN и APN функций;
* предлагаемые рекомендации могут использоваться при разработке ме­тодов и систем обеспечения целостности, включающих вейвлетные ко­ды, коды на основе PN и APN функции, а также ряд других кодов, ориентированных на безопасность.

Разработанные методы включены в исследования кафедры «Проектиро­вания и безопасности компьютерных систем» Университета ИТМО, в том числе в НИР №713552 «Исследование уязвимостей систем для защиты от атак по сто­ронним каналам», НИР №617026 «Технологии киберфизических систем: управ­ление, вычисления, безопасность»;

Материалы диссертации включены в отчет о результатах выполнения про­екта по «Конкурсу грантов для студентов вузов, расположенных на территории Санкт-Петербурга, аспирантов вузов, отраслевых и академических институтов, расположенных на территории Санкт-Петербурга», проводимым Комитетом по науке и высшей школе в 2015 году;

Разработанные методы обеспечения целостности внедрены в производ­ственную деятельность предприятия ООО «ВЕСТ-ТЕР». Внедрение резуль­татов позволило существенно повысить вероятность обнаружения искажений в средстве хранения данных системы видеонаблюдения «ПИЛОТ-В», удалось снизить шанс подмены управляющей информации, хранимой и обрабатывае­мой, в энергозависимой памяти данной системы;

Методы обеспечения целостности на основе вейвлетных кодов внедрены в производственную деятельность предприятия ООО «Технологии безопасности» в виде программной реализации методов для защиты видеоинформации, хра­нимой в системе видеонаблюдения, построенной на основе систем безопасности «TIGRIS». Также были разработаны практическое руководство и рекомендации по использованию и настройке разработанного программного средства, включа­ющие создание каталога типовых настроек программы для различных случаев изменений в распределении входных кодовых слов.

Методология и методы исследования. В данном диссертационном исследовании были использованы методы измерения вероятности маскировки ошибок в помехоустойчивых кодах, методы измерения показателей нелинейно­сти функций кодирования на основе производной по направлению. В дополне­ние к вышеперечисленным методам в диссертации использовались методы ли­нейной алгебры, теории полей, теории вейвлетных разложений над конечными пространствами, а также методы математического моделирования и численного анализа данных.

Положения, выносимые на защиту:

1. Метод обеспечения целостности информации на основе вейвлетных ли­нейных кодов и преобразования Грея, позволяющий обеспечивать за­щиту от атак на основе алгебраических манипуляций в случае нерав­номерного распределения входных кодовых слов;
2. Метод обеспечения целостности на основе вейвлетных нелинейных ко­дов, обладающих минимальным порядком дифференциальной равно­мерности функции кодирования и обеспечивающих защиту от атак на основе алгебраических манипуляций при неравномерном распределе­нии входных кодовых слов;
3. Практические рекомендации по применению разработанных методов обеспечения целостности для защиты средств хранения информации.

Степень достоверности подтверждается корректностью постановок за­дач, применением строгого математического аппарата. Отсутствуют противоре­чия между результатами диссертационной работы и общеизвестными научны­ми фактами. Все основные результаты прошли апробацию в печатных трудах Scopus и ВАК, а также докладах на отечественных и международных конфе­ренциях.

Апробация результатов. Основные результаты работы докладыва­лись на конференциях

* The 2015 International Conference on Soft Computing and Software Engineering, SCSE’15, University of California, Berkeley, Suta, USA, 2015;
* Computer, Communication, Control and Information Technology, Academy of Technology, India, 2015;
* Codes, Cryptology and Information Security, Mohammed V University, Rabat, Morocco, 2015;
* Information Security and Protection of Information Technology, Универси­тет ИТМО, Санкт-Петербург, 2015;
* XLIV научная и учебно-методической конференция Университета ИТ­МО, Университет ИТМО, Санкт-Петербург, 2015;
* IV Всероссийский конгресс молодых ученых, Университет ИТМО, Санкт-Петербург, 2015;
* 18th Conference of Open Innovations Association FRUCT, Университет ИТМО, Санкт-Петербург, 2016;
* VII Всероссийская научно-техническая конференция «Проблема ком­плексного обеспечения информационной безопасности и совершенство­вание образовательных технологий подготовки специалистов силовых структур», Университет ИТМО, Санкт-Петербург, 2016;
* The 20th Conference of Open Innovations Association FRUCT, Санкт-Петербургский электротехнический университет ЛЭТИ, Санкт- Петербург, Россия, 2017;
* XLVII Научная и учебно-методическая конференция Университета ИТ­МО, Университет ИТМО, Санкт-Петербург, 2018;
* VII Международная научно-техническая и научно-методическая кон­ференция «Актуальные проблемы инфокоммуникаций в науке и обра­зовании», Санкт-Петербургский государственный университет телеком­муникаций им. проф. М.А. Бонч-Бруевича, Санкт-Петербург, 2018;
* VII Всероссийский конгресс молодых ученых, Университет ИТМО, Санкт-Петербург, 2018;
* Electromagnetics Research Symposium, Singapore, 2017.

Публикации. Основные результаты по теме диссертации изложены в 17

печатных изданиях, 9 из которых находятся в изданиях, индексированных в Scopus [[14](#bookmark172)[-22]](#bookmark176), 3 — издано в журналах, рекомендованных ВАК [[23](#bookmark177)[-25]](#bookmark178), 5 — в иных изданиях [[26](#bookmark179)[-30]](#bookmark180).

Личный вклад. Все теоретические и практические выводы, разработка методов обеспечения целостности информации, написание программных моде­лей и алгоритмов, анализ результатов измерений, содержащиеся в данной дис­сертационной работе, выполнены автором самостоятельно.

Объем и структура работы. Диссертация состоит из введения, трех глав, заключения и двух приложений. Полный объём диссертации составляет 163 страницы с 28 рисунками и 17 таблицами. Список литературы содержит 84 наименования.

Заключение

В результате данного диссертационного исследования:

1. Были проанализированы потенциальные угрозы целостности информа­ции в системах обработки и хранения данных;
2. Исследованы показатели устойчивости существующих методов нели­нейного кодирования (вероятность маскировки ошибки, множество необнаруживаемых ошибок, надежность);
3. Разработаны методы обеспечения целостности на основе вейвлетных преобразований;
4. Исследованы разработанные конструкции, проанализировано поведе­ние конструкций в случае неравномерного распределения входных зна­чений;

Сформированы практические рекомендации для применения предло­женных методов обеспечения целостности для защиты средств хране­ния информации.