На правах рукописи

ЕВПАК Сергей Александрович

СИСТЕМЫ ЗАЩИТЫ ШИРОКОВЕЩАТЕЛЬНОЙ ПЕРЕДАЧИ ДАННЫХ НА ОСНОВЕ q-ИЧНЫХ КОДОВ РИДА-МАЛЛЕРА

Специальность 05.13.19 — Методы и системы защиты информации, информационная безопасность

Автореферат

диссертации на соискание учёной степени

кандидата технических наук

Ростов-на-Дону — 2018

Работа выполнена на кафедре алгебры и дискретной математики Института математики, механики и компьютерных наук им. И.И. Воровича Федерального государственного автономного образовательного учреждения высшего образования «Южный федеральный университет».

Научный руководитель:	**Деундяк Владимир Михайлович**, кандидат физико-математических наук, доцент, ФГАОУ ВО «Южный федеральный университет», кафедра алгебры и дискретной математики, доцент
Официальные оппоненты:	**Финько Олег Анатольевич**, доктор технических наук, профессор, Краснодарское высшее военное училище имени генерала армии С.М. Штеменко, г. Краснодар, кафедра №4, профессор
	Махмудов Андрей Абдулаевич, кандидат технических наук, «Ростовский-на-Дону НИИ Радиосвязи», г. Ростов-на-Дону, начальник лаборатории
Ведущая организация:	Федеральное государственное бюджетное образовательное учреждение высшего образования «Донской государственный технический университет» г. Ростов-на-Дону

Защита состоится «01» июня 2018 г. в 14.00 на заседании диссертационного совета Д 212.208.25 при Южном федеральном университете по адресу: 347922, Ростовская область, г. Таганрог, ул. Чехова 2, ауд. И-409.

С диссертацией можно ознакомиться в Зональной научной библиотеке Южного федерального университета по адресу: 344090, г. Ростов-на-Дону, ул. Зорге, 21 Ж.

Диссертация в электронном виде доступна по адресу: http://hub.sfedu.ru/diss/announcement/e9051776-322b-480f-800f-f444726b38f6/

Автореферат разослан «26» марта 2018 года.

Ученый секретарь
диссертационного совета Ю.А. Брюхомицкий

Общая характеристика работы

Актуальность темы. В течение последних лет продолжающаяся активная информатизация и глобализация общества все больше способствует популяризации так называемых широковещательных приложений, позволяющих передавать данные по открытому каналу от ее источника (автора) некоторой заинтересованной в ней группе привилегированных подписчиков (пользователей). К сервисам, предоставляемым такими широковещательными приложениями, обычно относят кабельное, спутниковое цифровое телевидение или радиовещание, онлайн-трансляции непубличной информацией, мобильные приложения на основе голосовой связи с возможностью передачи сигнала одновременно только в одном направлении по аналогии с портативными радиостанциями и другие службы доставки тиражируемых данных некоторой группе получателей. Ключевой задачей подобных приложений, как и большинства средств информационного обмена, является, помимо передачи данных адресату, обеспечение их защиты от различных угроз безопасности.

В настоящее время средства доступа и защиты платных цифровых спутниковых, эфирных и кабельных телеканалов и радиостанций (радиоканалов) получили название систем условного доступа (англ., Conditional Access System). Как правило, это сложный аппаратно-программный комплекс, включающий стандартизированные криптографические средства защиты информации, с потенциально возможным обратным каналом связи с пользователями. В данной работе исследуются системы условного доступа, которые не предполагают двустороннего канала связи между пользователями и поставщиком информации и могут применяться для защиты широковещательно распространяемых по другим каналам данных, например, IP-сетях. С одной стороны это может сужать область применения таких систем с точки зрения возможных приложений, но с другой стороны – повышать другие их конкурентные качества, такие как их ценовая общедоступность.

Первые исследования, связанные с функциональными решениями и средствами защиты информации в широковещательных приложениях, появились в девяностых годах в работах С. Берковича, Б. Чора, А. Фиата, М. Нао, Т. Тасса, К. Куросавы, И. Десмедта, Д. Бони, М. Франклина, М. Абдаллы, И. Шавитта, А. Вула, Б. Пинкаса, Б. Фитсмана, И. Вана, Р. Сафави-Найни и др. Одними из фундаментальных способов защиты тиражируемой информации в предлагаемых системах являются сформулированные значительно ранее (см., например, работы Н. Вагнера, Г. Блэкли, К. Медоус и Г. Пёрди) идеи и методы защиты информации правообладателей, в основе которых лежат уникальная маркировка её копий и криптографическая защита данных с уникальными ключами пользователей. Из очевидных недостатков приведенных средств защиты данных в широковещательных приложениях, в отличие от их применения для решения задач защиты авторских прав (англ., Digital Rights Management, DRM), выделяют их дороговизну и затруднительный процесс тиражирования.

Рост числа информационных участников в совокупности с несовершенством используемых методов защиты информации и увеличением многообразия атак на составные элементы систем широковещательного обмена данными, средства защиты которых впоследствии получили название систем широковещательного шифрования (СШШ, англ. Broadcast encryption scheme, BES), а также на систему распределения/генерации ключей (англ., Key Distribution System, KDS), выявил ряд

уязвимостей в широковещательных службах и потребовал изучения, модернизации, совершенствования СШШ. Одним из результатов таких исследований стала идея применения в рассматриваемой области теоретико-кодового метода. Для теории информационной безопасности метод не являлся абсолютно «новым» и активно использовался в различных направлениях защиты информации такими учёными, как В. М. Сидельников, В. И. Коржик, В. А. Яковлев, Э. М. Габидулин, Е. А. Крук и др. Позже некоторые исследователи, например, Д. Берштейн (Иллинойсский университет, г. Чикаго), оценили огромный потенциал теоретико-кодового метода при решении задач защиты информации и выразили уверенность в перспективности его использования в постквантовой криптографии, имеющей целью защитить информацию при появлении квантовых компьютеров и квантовых атак.

В 2000-х годах в работах Г. А. Кабатянского, А. Сильверберг, Дж. Стэддон, Дж. Уолкер, Д. Стинсона, Р. Уэя предлагается идея использования помехоустойчивых кодов для защиты данных от несанкционированного копирования, в частности, в рассматриваемых СШШ. В системах передачи данных, в которых могут применяться такие коды, пользователями используются кодовые вектор-номера для осуществления санкционированного распространителем доступа к данным. Вместе с тем некоторые пользователи, объединившись в коалиции злоумышленников мощности $w \in \mathbb{N}$, могут создавать пиратские вектор-номера, которые в дальнейшем использовать для выполнения нелегального доступа к распространяемым данным. Это может приводить к различным злоупотреблениям. Система защиты предусматривает поиск легальных пользователей, участвующих в создании пиратского вектор-номера.

В настоящее время для использования в таких системах защиты активно исследуются и применяются специальные классы так называемых кодов защиты от несанкционированного копирования. Одному классу принадлежат такие коды, для которых применение к пиратскому вектор-номеру любого декодера, работающего по минимуму кодового расстояния, позволяет гарантированно обнаружить вектор-номер принадлежащего коалиции мощности w злоумышленника (С. Блэкберн, Т. Эцион, М. Блаум и др.). В более широкий другой класс входят такие коды, для которых созданный коалицией мощности w пиратский вектор-номер не может являться вектор-номером пользователя, не принадлежащим коалиции. Данное свойство исключает возможность прямой компрометации пользователей.

Стоит отметить, что кодовая основа данных систем защиты определяет не только степень защиты от угроз коалиционных атак, но такие важные технические характеристики систем, как объем памяти для хранения ключей, объем тиражируемой информации. В этой связи преимуществом обладает та кодовая основа, которая обеспечивает соизмеримое соотношение между коммерческой стоимостью системы и её способностью гарантировать предсказуемое поведение в случае атак коалиции, в том числе большей, чем предусмотрено способом защиты (пороговой) мощности. Идеи, сочетающиеся в себе последние свойства систем широковещательного шифрования, являются достаточно новыми.

До настоящего времени в качестве кодов защиты от копирования всесторонне исследованы популярные во многих приложениях коды Рида-Соломона (М. Фернандес, М. Сориано, Х. Морейра, Г. А. Кабатянский). С точки зрения задач защиты информации, в которых применяются теоретико-кодовые методы, коды Рида-Соломона оказываются очень «хорошими» и даже оптимальными. Тем не менее, исследова-

ние систем широковещательного шифрования и их подсистем распределения ключей на основе кодов Рида-Соломона, выявило уязвимости в таких СШШ в случае превышения пороговой мощности коалиции (например, работы В. М. Сидельникова, Р. Блома). Данный факт позволил предположить о существовании других, более подходящих для систем широковещательного шифрования кодов, как с точки зрения противодействия угрозам коалиционных атак, так и с позиции коммерческой привлекательности.

С учетом вышеуказанного, интерес вызывает поиск, в частности, новых помехоустойчивых кодов с похожими свойствами, но другими, более эффективными параметрами с точки зрения их применения в системах широковещательного шифрования. Для решения этой задачи в работе рассматриваются существенно обобщающие коды Рида-Соломона – коды Рида-Маллера, которые, в том числе благодаря их высокой корректирующей способности при декодировании информации, активно используются в криптоаналитических исследованиях (О. А. Логачёв, А. А. Сальников, В. В. Ященко), а также при моделировании регистров сдвига (О. А. Козлитин, В. Л. Куракин, А. А. Нечаев).

Таким образом, актуальность темы исследования обеспечивается, во-первых, широкой распространенностью систем широковещательного обмена данными и, с учетом роста числа участников и изощренностью атак злоумышленников на данные правообладателей, необходимостью постоянного совершенствования средств защиты в этих системах и их подсистемах распределения ключей, во-вторых, – необходимостью защиты информации от коалиционных атак в системах, и, наконец, в-третьих, используемым теоретико-кодовым методом, который является неотъемлемой составляющей постквантовой криптографии, позволяющей защитить информацию при появлении квантовых компьютеров и квантовых атак, и обладает огромным потенциалом при решении задач защиты информации, а также широкими потенциальными возможностями применяемых в данном исследовании кодов Рида-Маллера.

Целью работы является исследование и разработка новых и совершенствование имеющихся средств защиты информации в системах широковещательного обмена данными в условиях наличия коалиционных атак. Для достижения поставленной цели необходимо решить следующие **задачи**:

- провести обзор и анализ методов и моделей распределения ключей в системах широковещательного шифрования;

- выявить и классифицировать уязвимости полилинейной системы распределения ключей, а также разработать средства противодействия связанным с ними угрозам;

- построить новую модель системы специального широковещательного шифрования на базе q-ичных кодов Рида-Маллера, разработать её программные средства, оценить возможность практического применения модели, сформулировать рекомендации по выбору параметров системы;

- исследовать построенную теоретико-кодовую модель на предмет наличия уязвимостей, связанных с угрозами атак коалиций произвольной мощности, и разработать способы обеспечения защиты передаваемой с её помощью информации.

Объект исследования – системы широковещательного обмена данными.

Предмет исследования – системы защиты широковещательной передачи данных и подсистемы распределения ключей.

Методология и методы исследования. Основу методологии диссертационного исследования составили как теоретические методы, так и экспериментальные. В качестве основных теоретических методов исследования использованы теоретико-кодовый метод, методы теории вероятностей, методы математической статистики, а также методы алгебры и комбинаторики. Экспериментальное исследование произведено методами имитационного моделирования с помощью разработанного программного комплекса.

Основные положения, выносимые на защиту:

1. Системы широковещательного шифрования на базе q-ичных кодов Рида-Маллера, позволяющие противодействовать угрозам атак коалиций с целью предотвращения утечки информации.

2. Теоретические обоснования оценок границ применимости системы широковещательного шифрования, основанной на q-ичных кодах Рида-Маллера, позволяющие прогнозировать поведение данных систем при превышении порога мощности коалиции злоумышленников.

3. Основанные на теоретических и экспериментальных исследованиях способы выбора параметров системы, позволяющие гарантировать защиту тиражируемых данных от коалиционных атак.

4. Классификация уязвимостей кодовой подсистемы распределения ключей системы защиты широковещательной передачи данных при превышении порога мощности коалиции злоумышленников и полученные на основе этой классификации теоретические результаты о вероятностях компрометации ключевой информации пользователей.

5. Способ оценки эффективности кодовых моделей распределения ключей, основанный на спектральных свойствах применяемых в них кодов.

Научная новизна исследования заключается в следующем:

1. Построены новые кодовые системы защиты широковещательной передачи данных, представляющие собой системы условного доступа с программными и криптографическими средствами защиты информации, с доверительным центром и бескоммутационными подсистемами распределения ключей, отличающиеся от существующих отсутствием сложного специального аппаратного обеспечения, гибкими средствами настройки программной и криптографической защиты данных, применением перспективных в задачах защиты информации q-ичных кодов Рида-Маллера, что позволяет повысить конкурентные способности таких систем, удешевляя стоимость их эксплуатации и обслуживания, расширяя сферу их применения, и защитить данные от коалиционных атак, являющихся следствием небольшого размера ключевой информации пользователей в системе. Построенные системы широковещательного шифрования обладают преимуществом перед ранее известными тем, что имеют возможность априорного оценивания вероятности уязвимостей в моделях сервера и генерации закрытого ключа пользователей, что позволяет на этапе проектирования осуществлять такой выбор параметров, который гарантирует системе в ходе ее функционирования противодействие угрозам коалиционных атак на пользовательские ключи, в том числе при превышении пороговой мощности коалиции.

2. Впервые получены теоретические результаты об оценках границ применимости модели системы широковещательного шифрования, основанной на q-ичных

кодах Рида-Маллера, которые позволяют формулировать рекомендации по выбору параметров системы.

3. Впервые на основе разработанной классификации уязвимостей в модели подсистемы распределения ключей в случае превышения пороговой мощности коалиции получены теоретические результаты о вероятностях компрометации конфиденциальных пользовательских данных, позволившие связать возможность осуществления атак таких коалиций в модели со спектральными свойствами применяемых в ней кодов и, в итоге, сформулировать новый способ оценки эффективности кодовых моделей распределения ключей.

Практическая значимость полученных в работе результатов состоит в повышении эффективности противодействия коалиционным атакам ограниченной мощности в кодовых системах защиты широковещательной передачи данных и их подсистемах распределения ключей, при этом проектирование таким систем на основе результатов теоретического и практического исследования гарантирует при превышении пороговой мощности коалиции достаточно низкую вероятность компрометации конфиденциальных пользовательских данных в системе.

Достоверность полученных результатов подтверждается полнотой и корректностью теоретических обоснований и результатов проведенных с помощью разработанного программного пакета экспериментов.

Апробация работы. Основные положения диссертации представлялись на XII Всероссийском симпозиуме по прикладной и промышленной математике (весенняя сессия, г. Казань, 2011 г.), на XIII международной научно-практической конференции «Информационная безопасность-2013» (г. Таганрог, 2013 г.), на IV китайско-российской конференции «Numerical algebra with applications» (г. Ростов-на-Дону, 2015 г.), на международных научных конференциях «Современные методы и проблемы теории операторов и гармонического анализа и их приложения - V», «Современные методы и проблемы теории операторов и гармонического анализа и их приложения - VI», «Современные методы и проблемы теории операторов и гармонического анализа и их приложения - VII» (г. Ростов-на-Дону, 2015-2017 гг.), а также на семинарах «Математические методы защиты информации» в Институте математики, механики и компьютерных наук Южного федерального университета (г. Ростов-на-Дону, 2012-2017 гг.).

Публикации. Основные научные результаты по теме диссертации опубликованы в научных изданиях, в составе которых: 5 работ в изданиях, рекомендованных ВАК РФ, одна из которых – индексирована также в международной базе данных SCOPUS; 10 работ в сборниках научных трудов и материалов конференций; получено 1 свидетельство о государственной регистрации программы для ЭВМ. Общий объем публикаций составляет 9,436 печатных листа, из которых 4,55 печатных листов принадлежит соискателю.

Структура и объем работы. Диссертация состоит из введения, четырех глав, заключения, списка сокращений и условных обозначений, библиографического списка, списка иллюстративного материала и двух приложений. Полный объем диссертации без списка сокращений и условных обозначений, списка литературы, списка иллюстративного материала и приложений с **14** рисунками и **11** таблицами составляет **148** страниц. Список литературы содержит **101** наименование.

Основное содержание работы

Во введении дается общая характеристика работы, и приводятся основные результаты диссертационной работы.

В первой главе приводится обзор существующих решений проблемы защиты информации в актуальных многопользовательских приложениях широковещательной передачи данных. Рассматриваются методы и средства защиты в таких приложениях. Среди множества средств защиты широковещательной передачи данных выделяются аппаратно-программные средства, криптографические средства защиты данных с уникальными пользовательскими ключами и другие средства защиты тиражируемых данных. Приводятся основные принципы и особенности указанных средств.

Из рассмотренных средств выделяются считающиеся наиболее надежными средства защиты широковещательной передачи данных на основе криптографической защиты данных с уникальными ключами пользователей. Указываются базовые эксплуатационные характеристики таких средств, которые могут обуславливать высокую стоимость использующих их систем широковещательной передачи данных: число тиражируемых сообщений по каналам связи и объём памяти для хранения ключей пользователей. Отмечается, что с целью повышения конкурентных качеств в таких системах, получивших впоследствии название систем широковещательного шифрования (СШШ), применяются более слабые ключи пользователей. Данный подход с одной стороны позволяет уменьшить число ключей в системы, а с другой, приводит к возникновению уязвимостей в СШШ, связанных с угрозами коалиционных атак. Отмечается, что на схожих принципах основывается защита информации, распространяемая с использованием ключей систем распределения ключей, например, в кодовых полилинейных системах распределения ключей. Приводятся примеры таких систем и методы, применяемые для нейтрализации возникающих в них уязвимостей.

Далее выделяются перспективные системы, называемые системами специального широковещательного шифрования (ССШШ). Данные системы отличаются от существующих наличием возможности противодействия угрозам коалиционных атак некоторой мощности, при этом объём памяти для хранения ключей пользователей в таких системах значительно меньше, чем в СШШ. В настоящее время ССШШ активно изучаются и совершенствуются, в качестве теоретической базы таких исследований выступают алгебра, теория графов, комбинаторика. Приводятся примеры новых, эффективных ССШШ с противодействием угрозам коалиционных атак на ключевую информацию пользователей на основе помехоустойчивых кодов, в частности, на кодах Рида-Соломона.

В заключении главы рассматривается применение теоретико-кодового метода в задачах защиты информации. Приводятся примеры криптосистем, основанных на различных помехоустойчивых кодах, в том числе на кодах Рида-Маллера. Подчеркивается важная роль помехоустойчивых кодов в обеспечении защиты информации от несанкционированного копирования в системах широковещательной передачи данных, проявляющаяся, в частности, в возможности противодействия угрозам атак коалиций некоторой предусмотренной системой защиты мощности. Обосновывается выбор для дальнейшего исследования существенно обобщающих коды Рида-Соломона q-ичных кодов Рида-Маллера в качестве базовых кодов подсистем рас-

пределения ключей ССШШ, который, кроме того, подкрепляется возникновением уязвимостей в таких подсистемах СШШ на кодах Рида-Соломона в случае превышения пороговой мощности коалиции злоумышленников.

В итоге формулируется как актуальная — задача разработки новых и совершенствование имеющихся средств защиты информации от несанкционированного копирования в системах широковещательной передачи данных в условиях наличия коалиционных атак произвольной мощности, основанных на применении перспективных в задачах защиты информации q-ичных кодов Рида-Маллера.

Во второй главе исследуется наиболее обобщенная среди аналогичных систем играющая важную роль при получении последующих основных результатов теоретико–кодовая полилинейная система распределения ключей, которая обеспечивает безопасность проведения конференции при наличии коалиции злоумышленников мощности, не превышающей некоторого порога. В случае, когда мощность коалиции превышает этот порог, система распределения ключей становится уязвимой.

В начале главы приводится математическая модель предложенной В.М. Сидельниковым кодовой полилинейной системы распределения ключей, разрабатывается классификация уязвимостей. Пусть $\mathbb{N}$ – множество натуральных чисел, $\mathbb{F}_q^u$ – u-мерное пространство над конечным полем Галуа $\mathbb{F}_q$. Под системой $R(N,t,w)$ понимается система распределения ключей с N пользователями, которая для произвольных конференций с t участниками позволяет получить закрытый (конфиденциальный) ключ конференции, неизвестный для тех пользователей, которые не входят в конференцию, при этом ни один ключ произвольной конференции не может быть скомпрометирован любой коалицией наблюдателей (злоумышленников) мощности не более w. Величина w системы $R(N,t,w)$ называется порогом мощности коалиции. Математическая модель системы $R(N,t,w)$ содержит следующие объекты.

1. Множество пользователей U такое, что его мощность $|U| = N$, множество открытых ключей $Q \subset \mathbb{F}_q^u$, $|Q| \geq N$ такое, что любые различные $w+1$ векторов множества Q являются линейно-независимыми над полем $\mathbb{F}_q$. Открытым ключом пользователя $\mathbf{a} \in U$ является вектор $\bar{\mathbf{a}} = (a_1, a_2, \ldots, a_u) \in Q$. Среди прочих множеств открытых ключей Q системы $R(N,t,w)$ В. М. Сидельниковым предложено использовать столбцы проверочной матрицы H некоторого линейного кода C с минимальным расстоянием $d \geq 2+w$.

2. Сервер, который генерирует базисное множество независимых закрытых ключей R системы $R(N,t,w)$ и предоставляет каждому $\mathbf{a}$ пользователю множество его закрытых ключей $R_{\mathbf{a}}$.

2.1. Базисное множество мощности $\binom{u+t-1}{t}$ имеет вид: $R = \{\xi_{i_1,\ldots,i_t} \in \mathbb{F}_q^v | 1 \leq i_1 \leq i_2 \leq \ldots \leq i_{t-1} \leq u\}$, где v – достаточно большое, а $\xi_{i_1,\ldots,i_t}$ – независимые случайные величины, каждая из которых равномерно распределена на элементах множества $\mathbb{F}_q^v$. Далее используется обозначение $\xi_{j_1,\ldots,j_t}$ для произвольных наборов $j_1,\ldots,j_t$, полагая, что $\xi_{j_1,\ldots,j_t} = \xi_{i_1,\ldots,i_t}$, если набор $j_1,\ldots,j_t$ является перестановкой набора $i_1,\ldots,i_t$.

2.2. Множество $R_{\mathbf{a}}$ образовано $\binom{u+t-2}{t-1}$ элементами вида $\xi_{i_1,\ldots,i_{t-1}}(\mathbf{a}) = \sum_{i=1}^{u} a_i \xi_{i_1,\ldots,i_{t-1},i}$, $1 \leq i_1 \leq i_2 \leq \ldots \leq i_{t-1} \leq u$. Полагается, что $\xi_{j_1,\ldots,j_{t-1}}(\mathbf{a}) = \xi_{i_1,\ldots,i_{t-1}}(\mathbf{a})$, если набор $j_1,\ldots,j_{t-1}$ является перестановкой некоторого набора $i_1,\ldots,i_{t-1}$ такого, что $1 \leq i_1 \leq i_2 \leq \ldots \leq i_{t-1} \leq u$.

3. Общеизвестный алгоритм, который позволяет каждому пользователю $\mathbf{a}_i$ из конференции $T = \{\mathbf{a}_1,\ldots,\mathbf{a}_t\}$, используя свое множество закрытых ключей $R_{\mathbf{a}_i}$

и открытые ключи всех участников конференции: $\bar{\mathbf{a}}_j = (a_{j,1}, a_{j,2}, \ldots, a_{j,u})(j = 1, \ldots, t)$, вычислить общий закрытый ключ конференции по формуле $k_T = k_{\mathbf{a}_1,\ldots,\mathbf{a}_t} = \sum_{j_1,j_2,\ldots,j_{t-1}=1}^{u} a_{1,j_1} a_{2,j_2} \ldots a_{t-1,j_{t-1}} \xi_{j_1,\ldots,j_{t-1}}(\mathbf{a}_t) = \sum_{j_1,j_2,\ldots,j_t=1}^{u} a_{1,j_1} a_{2,j_2} \ldots a_{t,j_t} \xi_{j_1,\ldots,j_t}$. Пользователь $\mathbf{a} \in U$ системы, располагая парой $(\bar{\mathbf{a}}, R_{\mathbf{a}})$ из открытого и закрытого ключа, может, используя алгоритм 3, вычислить общий для всех членов некоторой конференции T, членом которой он является, закрытый ключ k_T.

В случае увеличения числа злоумышленников система $R(N,t,w)$ становится уязвимой. Пусть δ – непредусмотренное приращение числа наблюдателей в системе $R(N,t,w)$, $\mathcal{T}_t$ –множество всевозможных конференций пользователей системы $R(N,t,w)$ из t участников, а $\mathcal{W}_{w+\delta}$ – множество всевозможных коалиций из $w+\delta$ наблюдателей системы $R(N,t,w)$. С целью противодействия угрозам атак коалиций мощности $w+\delta$ разработана классификация уязвимостей конференции, коалиции и системы $R(N,t,w)$, введены локальные и глобальные характеристики системы, получены соотношения между ними [1].

1. Пусть множество $\mathcal{W}_{w+\delta,\leq\delta}(T)(\mathcal{W}_{w+\delta,\delta}(T))$ – множество δ-опасных коалиций по отношению к конференции T (в строгом смысле), т.е. множество коалиций размера $w+\delta$, непересекающихся с конференцией T, могущие скомпрометировать ключ конференции T (при этом при удалении хотя бы одного любого члена она перестает быть δ-опасной коалицией). Характеристика данного множества связана с величиной $\deg_{w+\delta,\leq\delta}(T)$ ($\deg_{w+\delta,\delta}(T)$), равной $\frac{1}{\binom{N-t}{w+\delta}}|\mathcal{W}_{w+\delta,\leq\delta}(T)|$ ($\frac{1}{\binom{N-t}{w+\delta}}|\mathcal{W}_{w+\delta,\delta}(T)|$), определяющей вероятность компрометации ключа конференции T непересекающимися с T коалициями из множества $\mathcal{W}_{w+\delta}$.

2. Пусть множество $\mathcal{T}_{t,\delta}(W)$ – множество δ-рисковых конференций по отношению к коалиции W, т.е. множество непересекающихся с W конференций T, ключи которых может скомпрометировать W. Характеристика данного множества связана с величиной $\deg^{\perp}_{t,\delta}(W)$, равной $\frac{1}{\binom{N-w-\delta}{t}}|\mathcal{T}_{t,\delta}(W)|$, определяющей вероятность компрометации коалицией W ключей непересекающихся с W конференций из $\mathcal{T}_t$.

3. Пусть множество $\mathcal{T}_{\delta}(R(N,t,w))$ – множество всех δ-рисковых конференций системы $R(N,t,w)$. Характеристика данного множества связана с величиной $\mathrm{Deg}_{\delta}(R(N,t,w))$, равной $\frac{1}{\binom{N}{t}}|\mathcal{T}_{\delta}(R(N,t,w))|$, определяющей вероятность выбора в $R(N,t,w)$-системе δ-рисковой конференции, ключ которой может скомпрометировать какая-нибудь непересекающаяся с ней коалиция размера $w+\delta$.

4. Пусть множество $\mathcal{W}_{\leq\delta}(R(N,t,w))$ ($\mathcal{W}_{\delta}(R(N,t,w))$) – множество всех δ-опасных коалиций системы $R(N,t,w)$ (множество всех δ-опасных коалиций системы $R(N,t,w)$ в строгом смысле). Характеристика данного множества связана с величиной $\mathrm{Deg}^{\perp}_{\leq\delta}(R(N,t,w))$ ($\mathrm{Deg}^{\perp}_{\delta}(R(N,t,w))$), равной $\frac{1}{\binom{N}{w+\delta}}|\mathcal{W}_{\delta}(R(N,t,w))|$ ($\frac{1}{\binom{N}{w+\delta}}|\mathcal{W}_{\leq\delta}(R(N,t,w))|$), определяющей вероятность выбора в $R(N,t,w)$ системе δ-опасной коалиции, которая может скомпрометировать ключ какой-нибудь непересекающейся с ней конференции.

В результате исследования с использованием теоретико-кодового метода и методов теории вероятностей кодовой полилинейной системы распределения ключей при превышении числа злоумышленников получены оценки возникновения выявленных уязвимостей [2], [3]. Пусть $\omega(\bar{\mathbf{c}})$ – вес кодового слова $\bar{\mathbf{c}} \in C$, последовательность чисел $A_0, A_1, A_2, \ldots, A_N$, где A_i – количество кодовых слов из C веса i, – спектр кода C.

Теорема 1. Для $\mathrm{Deg}_{\delta}^{\perp}(R(N,t,w))$ выполняется следующее равенство

$$\mathrm{Deg}_{\delta}^{\perp}(R(N,t,w)) = \frac{1}{\binom{N}{w+\delta}} \frac{w+\delta+1}{q-1} A_{w+\delta+1}, 1 \le \delta \le N-w-t.$$

Далее приводятся несколько иллюстративных примеров полилинейных систем распределения ключей $R(N,t,w)$ на кодах Хемминга и Голея с вычисленными величинами $\mathrm{Deg}_{\delta}^{\perp}(R(N,t,w))$, формулируется вывод о преимуществах использования кодов Голея для формирования сервером кодовой полилинейной системы распределения ключей открытых ключей пользователей с точки зрения возникающих уязвимостей при превышении пороговой мощности коалиции в сравнении с использованием с этой целью кодов Хэмминга. Построены оценки других локальных и глобальных характеристик систем на основе других более сложных спектральных характеристик применяемого кода. Полученные результаты позволяют сделать выводы серверу о целесообразности применимости в таких системах конкретных кодов; конференции – о целесообразности передачи конфиденциальной информации по открытым каналам с использованием своего ключа; нечестному пользователю – о целесообразности организации коалиции для компрометации ключа конференции.

В заключении главы предлагается новый способ, отличный от предложенных А. Беймелем и Б. Шором и некоторыми другими, оценки эффективности кодовых моделей распределения ключей, в котором впервые в рамках решения рассматриваемых в работе задач применяются спектральные свойства используемых в моделях кодов [4]: характеристики $\mathrm{Deg}_{\delta}(R(N,t,w))$ и $\mathrm{Deg}_{\delta}^{\perp}(R(N,t,w))$. Указанные величины позволяют проектировать системы с гибким реагированием на возможное изменения мощности коалиции, что подтверждает построенная кодовая модель распределения ключей на q-ичных кодах Рида-Маллера, которая имеет лучшие эксплуатационные характеристики при превышении пороговой мощности коалиции в сравнении с этой же системой на кодах Рида-Соломона.

В третьей главе строиться на основе работ Б. Шора, А. Фиата, М. Нао и исследуется в случае превышения допустимого числа членов коалиции злоумышленников модель системы специального широковещательного шифрования на q-ичных кодах Рида-Маллера.

Пусть $\mathbb{N}_1 = \mathbb{N} \setminus \{1\}$, $\mathbb{F}_q = \{0;1;\ldots;\alpha^{q-2}\}$ – поле Галуа, где α – фиксированный примитивный элемент $\mathbb{F}_q$, множество $Q = \{1;\ldots;q\}$, $\mathrm{RM}_q(r,m)(\subseteq \mathbb{F}_q^n)$ – q-ичный код Рида-Маллера над полем $\mathbb{F}_q$ произвольного порядка r с таким m, что $n = q^m$ – длина кода, $\zeta : \mathbb{F}_q \to Q$ – биективное отображение, определяемое правилом: $\zeta(0) = 1, \zeta(\alpha^a) = a+2$, где $a \in \{0;\ldots;q-2\}$, $\lambda : \mathrm{RM}_q(r,m) \to Q^n$ – инъективное отображение, заданное правилом: $\lambda(\nu_1,\ldots,\nu_n) = (\zeta(\nu_1),\ldots,\zeta(\nu_n))$. Математическая модель ССШШ на q-ичных кодах Рида-Маллера содержит следующие объекты.

1. Шифр для защиты блоков тиражируемой информации, определяемый множествами $(X^*, K^*, Y^*, E^*, D^*)$.

2. Правило Ф разделения блокового ключа κ^* – ключа, используемого для защиты конкретного блока текста: $\Phi(\kappa^*) = (\kappa_1^*,\ldots,\kappa_n^*) \in X^n = X \times \ldots \times X$. Правило $\Phi^{(-1)}$ восстановления блокового ключа: $\kappa^* = \Phi^{(-1)}(\kappa_1^*,\ldots,\kappa_n^*), \kappa^* \in K^*$.

3. Шифр для защиты частей блоковых ключей, определяемый множествами (X, K, Y, E, D).

4. Подсистема распределения ключей на q-ичных кодах Рида-Маллера с параметрами q, r, m, которые задают размер матрицы разрешенных ключей для защиты частей блокового ключа: $\Lambda = (k_{i,j})_{i\in\{1;\ldots;n\},j\in\{1;\ldots;q\}}, k_{i,j} \in K, n = q^m$. При этом подсистемой каждому легальному пользователю $\mathbf{u}$ передается следующая ключевая информация:

4.1. Уникальный вектор-номер пользователя $\bar{\mathbf{J}}_{\mathbf{u}}(\in \mathrm{RM}_q(r,m))$ такой, что $\lambda(\bar{\mathbf{J}}_{\mathbf{u}}) = (j_1,\ldots,j_n)$, где $j_1,\ldots,j_n \in \{1;\ldots;q\}$. Для формирования вектор-номера пользователя $\mathbf{u}$ удобно пользоваться кодирующим отображением базового кода $\mathrm{RM}_q(r,m)$, в котором в качестве сообщения выбирать, например, уникальные данные пользователя $\mathbf{u}$.

4.2. Соответствующий вектор-номеру пользователя $\bar{\mathbf{J}}_{\mathbf{u}}(\in \mathrm{RM}_q(r,m))$ вектор-ключ пользователя – уникальный упорядоченный набор частичных ключей: $\bar{\mathbf{K}}_{\mathbf{u}} = (\kappa_1,\ldots,\kappa_n) = (k_{1,j_1},\ldots,k_{n,j_n})$.

Предполагается, что поставщик информации, представляющий собой участника информационного обмена, распространяющего информацию только приобретающим её законным пользователям, для организации системы защиты широковещательной передачи данных определяется с числом пользователей N, заинтересованным в тиражируемой информации, выбирая q-ичный код Рида-Маллера, например, так, чтобы $|\mathrm{RM}_q(r,m)| \geq N$, и формирует матрицу разрешенных ключей Λ. Далее он разбивает данные на блоки и зашифровывает на блоковом ключе $\kappa^* \in K^*$ очередной блок $M \in X^*$: $e^* = E^*_{\kappa^*}(M)$. Блоковому ключу κ^* по правилу разделения Φ ставится в соответствие вектор $\bar{\gamma} = \Phi(\kappa^*) = (\kappa^*_1,\ldots,\kappa^*_n) \in X^n$. Для восстановления κ^* используются все элементы $\bar{\gamma}$. Затем каждая координата κ^*_i зашифровывается на q частичных ключах $\{k_{i,1},\ldots,k_{i,q}\} \subseteq K$ вектора-столбца матрицы Λ: $e_{i,1} = E_{k_{i,1}}(\kappa^*_i),\ldots,e_{i,q} = E_{k_{i,q}}(\kappa^*_i)$. Закрытые тексты e^* и $\Sigma = (e_{i,j})_{i\in\{1;\ldots;n\},j\in\{1;\ldots;q\}}$ поставщик передает по открытому каналу. Легальный пользователь $\mathbf{u}$, получив по каналам шифрограммы e^*, Σ, на основе информации в вектор-ключе $\bar{\mathbf{K}}_{\mathbf{u}}$ может расшифровать каждую из частей блокового ключа: $D_{\kappa_i}(e_{i,j_i}) = D_{k_{i,j_i}}(E_{k_{i,j_i}}(\kappa^*_i)) = \kappa^*_i, i \in \{1;\ldots;n\}$. Вычислив части блокового ключа, пользователь имеет возможность восстановить блоковый ключ $\kappa^* = \Phi^{(-1)}(\kappa^*_1,\ldots,\kappa^*_n)$ и расшифровать блок M тиражируемых данных $D^*_{\kappa^*}(e^*) = D^*_{\kappa^*}(E^*_{\kappa^*}(M)) = M$ [5], [6].

При нелегальном распространении злоумышленником своей ключевой информации (вектор-номер и вектор-ключ) ввиду её уникальности он может быть идентифицирован предусмотренным в системе контролёром. Вместе с тем для данных систем указывается наличие возможности организации нечестными пользователями коалиционных атак, позволяющих передавать распространяемые данные третьим лицам, строится математическая модель таких атак. Для защиты от них приводятся предложенные Дж. Стэддоном, Д. Стинсоном, Р. Уэем специальные классы т.н. кодов защиты от копирования: w-FP-кодов и w-TA-кодов. Множество w-коалиций кода C, представляющего собой множество всех непустых подмножеств C мощности не более $w(\geq 2)$, обозначается через $\mathrm{coal}_w(C)$. С коалицией $C_0 \in \mathrm{coal}_w(C)$ связывается множество её потомков $\mathrm{desc}(C_0)$=$\{\bar{\mathbf{w}} = (w_1,\ldots,w_n) \in \mathbb{F}^n_q$: $w_i \in \{a_i : \bar{\mathbf{a}} \in C_0\}\forall i \in \{1;\ldots;n\}\}$. Под множеством пиратских вектор-номеров коалиции C_0 понимается множество $\mathrm{desc}(C_0) \setminus C_0$. Множество w-потомков кода C определяется $\mathrm{desc}_w(C) = \bigcup_{C_i\in\mathrm{coal}_w(C)} \mathrm{desc}\,(C_i)$.

Код C является w-FP-кодом, если $\forall\bar{\mathbf{z}} \in C\forall C_0 \in \mathrm{coal}_w(C\setminus\{\bar{\mathbf{z}}\}) : \bar{\mathbf{z}} \notin \mathrm{desc}(C_0)\setminus C_0$. Код является w-FP-кодом тогда и только тогда, когда никакая коали-

ция злоумышленников мощности не более w не может скомпрометировать легального не входящего в эту коалицию пользователя путем создания его вектор-номера. Код C является w-ТА-кодом, если $\forall C_0 \in \mathrm{coal}_w(C) \quad \forall \bar{\mathbf{w}} \in \mathrm{desc}(C_0) \quad \forall \bar{\mathbf{z}} \in C \setminus C_0 \quad \exists \bar{\mathbf{y}} \in C_0 : d(\bar{\mathbf{w}}, \bar{\mathbf{y}}) < d(\bar{\mathbf{w}}, \bar{\mathbf{z}})$. Код C является w-ТА-кодом, когда для любого пиратского вектор-номера $\bar{\mathbf{w}} \in \mathrm{desc}_w(C)$ ближайшее кодовое слово – это элемент $\bar{\mathbf{y}}$, входящий в создавшую $\bar{\mathbf{w}}$ коалицию. Следовательно, поиск ближайшего кодового слова к пиратскому вектор-номеру может обнаружить элемент коалиции, принимавший участие в создании этого вектор-номера. Алгоритм поиска элемента $\bar{\mathbf{y}}$ совершенствуется: от переборного декодера в работах Дж. Стэддона, Д. Стинсона, Р. Уэя до списочного декодера, предложенного А. Сильверберг, Дж. Стэддон, Дж. Уолкер.

Впервые доказывается теоретическая возможность применения q-ичных кодов Рида-Маллера в ССШШ для целей защиты от коалиционных атак ограниченной способом защиты мощности [6]. В частности, доказано что q-ичный код Рида-Маллера $\mathrm{RM}_q(r, m)$, $r < q$, является w-ТА-кодом, если выполняется условие

$$w \leq B_0(r) = \left\lceil \sqrt{\frac{q}{r}} - 1 \right\rceil . \tag{1}$$

Построена основанная на списочном декодере Р. Пелликаана q-ичных кодов Рида-Маллера с параметрами, при которых он является w-ТА-кодом, математическая модель эффективной защиты ССШШ от вышеуказанных коалиционных атак [5]; доказывается, что алгоритм работы контролёра в модифицированной ССШШ по злоумышленнику может найти как минимум одного члена коалиции, содействующего преступнику [6]. На основе работ В.В. Мкртичяна отмечаются преимущества такого алгоритма противодействия коалиционным атакам перед существующими: в отсутствии необходимости использования колоссальных вычислительных ресурсов для обнаружения большого числа злоумышленников за приемлемое время.

Далее исследуется модель эффективной ССШШ на базе q-ичных кодов Рида-Маллера и оцениваются возникающие уязвимости, связанные с угрозами коалиционных атак произвольной мощности [7], [8], [9], [10], [11]. Выше приводится условие (1) для q-ичного кода Рида-Маллера, в случае нарушения которого корректная работа модели ССШШ не гарантируется. По аналогии с результатами В.М. Деундяка и В.В. Мкртичяна для ССШШ на кодах Рида-Соломона вводятся множества различных случаев нарушения условия (1), называемые области компрометации q-ичного кода Рида-Маллера.

Пусть $\Omega_{TA;r,m} = \{w \in \mathbb{N}_1 : \exists \bar{\mathbf{v}} \in \mathrm{RM}_q(r, m) \ \exists C_0 \in \mathrm{coal}_w(\mathrm{RM}_q(r, m) \backslash \{\bar{\mathbf{v}}\}) \ \exists \bar{\mathbf{w}} \in \mathrm{desc}(C_0) \backslash C_0 \ \forall \bar{\mathbf{u}} \in C_0 : d(\bar{\mathbf{v}}, \bar{\mathbf{w}}) \leq d(\bar{\mathbf{w}}, \bar{\mathbf{u}})\}$. Область $\Omega_{TA;r,m}$ – это множество мощностей таких коалиций, при которых для некоторого кодового слова $\bar{\mathbf{v}}$ существует коалиция C_0 этой мощности, хотя бы один из потомков которой расположен не далее от $\bar{\mathbf{v}}$, чем от любого элемента C_0. Таким образом, $\Omega_{TA;r,m}$ – множество значений $w \in \mathbb{N}_1$, при которых для кода $\mathrm{RM}_q(r, m)$ при применении декодера, работающего по минимуму расстояния, возможна компрометация некоторого невиновного пользователя $\bar{\mathbf{v}}$.

Пусть $\Omega_{FP;r,m} = \{w \in \mathbb{N}_1 : \exists \bar{\mathbf{v}} \in \mathrm{RM}_q(r, m) \ \exists C_0 \in \mathrm{coal}_w(\mathrm{RM}_q(r, m) \backslash \{\bar{\mathbf{v}}\}) : \bar{\mathbf{v}} \in \mathrm{desc}(C_0) \backslash C_0\}$. Область $\Omega_{FP;r,m}$ есть множество мощностей таких коалиций, при которых для некоторого кодового слова $\bar{\mathbf{v}}$ существует коалиция этой мощности, одним из потомков которой является $\bar{\mathbf{v}}$. Таким образом, $\Omega_{FP;r,m}$ – множество

значений $w \in \mathbb{N}_1$, при которых для кода $\mathrm{RM}_q(r,m)$ возможна прямая компрометация некоторого невиновного пользователя $\bar{\mathbf{v}}$ путем создания его вектор-номера коалицией злоумышленников.

Как отмечено, в работах В.М. Деундяка и В.В. Мкртичяна смещение на некоторый вектор двух точек пространства $\mathbb{F}_q^n$ не изменяет расстояние между ними, а смещение на произвольный кодовый вектор множества потомков коалиции произвольного кода представляет собой множество потомков коалиции, смещенной на тот же вектор. Отсюда следует, что множества $\Omega_{TA;r,m}$ и $\Omega_{FP;r,m}$ состоят из таких $w(\in \mathbb{N}_1)$, при которых существует вероятность соответствующей компрометации любого пользователя.

Множества $\Omega_{TA;r,m}$, $\Omega_{FP;r,m}$ – целочисленные отрезки вида: $\Omega_{TA;r,m} = \{R_{TA}(r,m); ...; \ |\mathrm{RM}_q(r,m)|\}$, $\Omega_{FP;r,m} = \{R_{FP}(r,m); ...; \ |\mathrm{RM}_q(r,m)|\}$, где $R_{TA}(r,m)$, $R_{FP}(r,m)$ – величины, называемые рубежами областей компрометации $\Omega_{TA;r,m}$ и $\Omega_{FP;r,m}$ соответственно. Доказывается, что функции $R_{TA}(r,m)$ и $R_{FP}(r,m)$ являются монотонными по каждой из переменных в отдельности [12].

Расчет рубежей $R_{TA}(r,m)$ и $R_{FP}(r,m)$ является относительно сложной комбинаторной задачей, в связи с этим интерес представляет также задача получения оценок для этих рубежей. Для этого в случае $r < q$ вводятся величины:

$$B_0(r) = \left\lceil \sqrt{\frac{q}{r}} - 1 \right\rceil, B_{FP}(r) = \left\lceil \frac{q}{r} \right\rceil,$$

$$B_{TA}(r,m) = \begin{cases} \left\lceil \sqrt{\frac{q}{r}} \right\rceil, & \text{при } r \geq \left\lfloor \frac{(q^m-q+1)^2}{q^{2m-1}} + 1 \right\rfloor, \\ \left\lfloor \frac{q}{r} + 1 - \frac{1}{rq^{m-2}} + \frac{1}{rq^{m-1}} \right\rfloor, & \text{при } r < \left\lfloor \frac{(q^m-q+1)^2}{q^{2m-1}} + 1 \right\rfloor. \end{cases}$$

Доказывается основной результат о рубежах $R_{TA}(r,m)$ и $R_{FP}(r,m)$ множеств компрометации $\Omega_{TA;r,m}$ и $\Omega_{FP;r,m}$ соответственно.

Теорема 2. Рассмотрим код $\mathrm{RM}_q(r,m)$.

1) Если $r < q$, то $B_0(r) \leq R_{TA}(r,m) \leq B_{TA}(r,m) \leq R_{FP}(r,m) = B_{FP}(r)$.

2) Если $r \geq q$, то $R_{TA}(r,m) = 2$.

В четвертой главе разрабатываются программные средства, реализующие средства защиты информации от несанкционированного копирования в системах широковещательного обмена данными, и формулируются полученные способы выбора параметров системы защиты, позволяющие гарантировать защиту распространяемых данных от коалиционных атак.

В начале главы построены и описаны программные средства защиты системы широковещательной передачи данных, в которых в качестве базовых кодов используются q-ичные коды Рида-Маллера, а в качестве списочного декодера – списочный декодер Р. Пелликаана q-ичных кодов Рида-Маллера. Программные средства включают как защиту протокола передачи данных, так и средство взлома и модифицированные средства защиты исследуемых систем и реализованы на языке C++ с использованием свободно распространяемой криптографической библиотеки Crypto++ и библиотеки теоретико-числовых методов WinNTL, которые предоставляют возможность строить программные средства, независимые от аппаратно-программной платформы [13], [14].

С учетом результатов, полученных в предыдущих главах, далее предлагаются рекомендации по выбору параметров рассматриваемой модели, в частности, по вы-

бору параметров используемых q-ичных кодов Рида-Маллера, в целях защиты передаваемых данных как в случае наличия коалиционных атак ограниченной способом защиты мощности, так и в случае превышения границ областей компрометации пользователей [15], [16].

Пусть N – число пользователей, w – максимальная мощность коалиций злоумышленников, выбранные поставщиком исходя из экономической выгоды и соображений безопасности. Тогда для защиты от коалиционных атак злоумышленников мощности не более w можно использовать q-ичный код Рида-Маллера $\mathrm{RM}_q(r,m)$ с параметрами q, r, m, удовлетворяющими задачам нелинейного программирования с целевыми функциями в зависимости от предпочтений поставщика $R = q^m \to \min_{q,r,m}$ (минимизация объема памяти для хранения ключей пользователей), $\{q^{\binom{r+m}{m}} - B_{TA}(r,m)\} \to \min_{q,r,m}$, $\{q^{\binom{r+m}{m}} - \lceil \frac{q}{r} \rceil\} \to \min_{q,r,m}$ (минимизация мощностей областей компрометации кода) и областью допустимых значений с соответствующими $q = p^i$, p – простое, $r, m, i \in \mathbb{N}$

$$q \geq rw^2 + 1, \tag{2}$$

$$|\mathrm{RM}_q(r,m)| = q^{\binom{r+m}{m}} \geq N. \tag{3}$$

На рисунке 1 для целей демонстрации преимуществ применения в системах кодов Рида-Маллера перед кодами Рида-Соломона приводятся примеры областей допустимых значений рассматриваемой задачи при фиксированных величинах N и w. При этом, плоскость № 2 соответствует уравнению $q = rw^2 + 1$, а поверхность № 3 – уравнению $q^{\binom{r+m}{m}} = N$. Область допустимых значений задачи – пространство (множество) между плоскостью № 2 и поверхностью № 3, включая эти поверхности, ближайшее к плоскости $r = 0$. Данные области содержат целочисленные множества возможных значений параметров q, r, m кода $\mathrm{RM}_q(r,m)$ при фиксированных величинах N и w в случае коалиционных атак мощности не более, чем w.

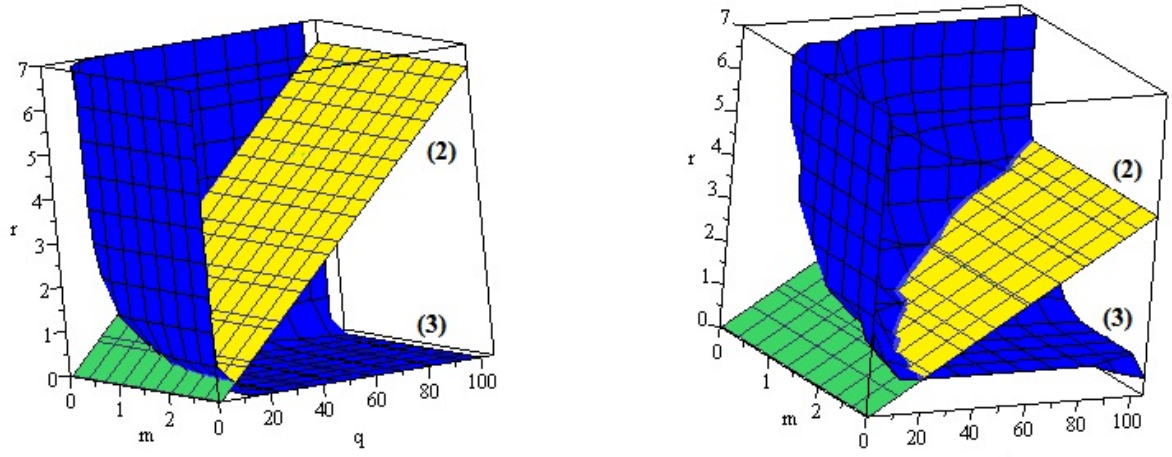

Рисунок 1 – Область возможных значений параметров q, r, m кода $\mathrm{RM}_q(r,m)$ в случае $N = 100$ и $w = 4$ и в случае $N = 1000000$ и $w = 5$

В таблице 1 представлены примеры моделей защиты с соответствующими параметрами применяемого в них кода $\mathrm{RM}_q(r,m)$. Системы с выделенными параметрами кода имеют меньшие области компрометаций пользователей в сравнении с аналогичными системами с параметрами кода, оптимизируемыми по объёму хранения ключей пользователей, что подтверждает в данном случае преимущества ССШШ на q-ичных кодах Рида-Маллера перед ССШШ на кодах Рида-Соломона при превышении пороговой мощности коалиции злоумышленников.

Таблица 1 – Параметры $\{q, r, m\}$ кода $\mathrm{RM}_q(r, m)$, минимизирующие длину вектор-номеров пользователей (1) и области компрометации (2), в зависимости от N и w

$N \backslash w$	2	3	4
1000	$\{11, 2, 1\}^{(1)}$, $\{\mathbf{11}, \mathbf{1}, \mathbf{2}\}^{(\mathbf{2})}$	$\{19, 2, 1\}^{(1)}$, $\{\mathbf{11}, \mathbf{1}, \mathbf{2}\}^{(\mathbf{2})}$	$\{37, 1, 1\}^{(1)}$, $\{37, 1, 1\}^{(2)}$
10000	$\{13, 3, 1\}^{(1)}$, $\{\mathbf{11}, \mathbf{1}, \mathbf{3}\}^{(\mathbf{2})}$	$\{23, 2, 1\}^{(1)}$, $\{\mathbf{23}, \mathbf{1}, \mathbf{2}\}^{(\mathbf{2})}$	$\{37, 2, 1\}^{(1)}$, $\{\mathbf{23}, \mathbf{1}, \mathbf{2}\}^{(\mathbf{2})}$
100000	$\{17, 4, 1\}^{(1)}$, $\{\mathbf{7}, \mathbf{1}, \mathbf{5}\}^{(\mathbf{2})}$	$\{29, 3, 1\}^{(1)}$, $\{\mathbf{19}, \mathbf{1}, \mathbf{3}\}^{(\mathbf{2})}$	$\{47, 2, 1\}^{(1)}$, $\{\mathbf{47}, \mathbf{1}, \mathbf{2}\}^{(\mathbf{2})}$
1000000	$\{17, 4, 1\}^{(1)}$, $\{\mathbf{17}, \mathbf{1}, \mathbf{4}\}^{(\mathbf{2})}$	$\{37, 3, 1\}^{(1)}$, $\{\mathbf{17}, \mathbf{1}, \mathbf{4}\}^{(\mathbf{2})}$	$\{53, 3, 1\}^{(1)}$, $\{\mathbf{17}, \mathbf{1}, \mathbf{4}\}^{(\mathbf{2})}$

Отмечается, что выбор данных параметров кода определяет длину вектор-номера пользователя в ССШШ, длина вектор-ключа, обозначаемая далее λ, может быть выбрана независимо от данных результатов с учетом рекомендаций для длины ключа используемой конкретной криптосистемы.

При получении оценок вероятностей компрометации пользователей использовались методы математической статистики и методика экспериментального исследования, основанная на подходе В.В. Мкртичяна к изучению ССШШ на кодах Рида-Соломона. Полученные результаты подтверждают теоретические выводы главы 3 и с учетом свойств q-ичных кодов Рида-Маллера свидетельствуют о, с одной стороны, небóльших вероятностях компрометации пользователей в ССШШ на q-ичных кодах Рида-Маллера, чем аналогичные вероятности в ССШШ на кодах Рида-Соломона, при одинаковой длине вектор-номера пользователя (например, наборы параметров $\{11, 1, 2\}$ и $\{121, 1, 1\}$ при $N = 1000$ и $w = 3$; вероятность того, что в результате работы контролёра по пиратскому вектор-номеру $\bar{\mathbf{w}}$ будет скомпрометирован вектор-номер невиновного пользователя, не более $2,5 * 10^{-5}$) и, с другой стороны, небóльших длин ключа пользователя ССШШ на q-ичных кодах Рида-Маллера в случае одинаковой вероятности компрометации вектор-номеров пользователей ССШШ на кодах Рида-Соломона.

Далее оцениваются основные характеристики предложенных СШШ на q-ичных кодах Рида-Маллера: объем памяти, необходимый каждому пользователю для хранения ключей, число трансляций распространяемой информации от поставщика покупателям, пороговая величина w, представляющая максимальное число пользователей сообщества (злоумышленников), которые, объединивши свои ключи, могут взломать систему.

Пусть код $\mathrm{RM}_q(r, m)$ является кодом Рида-Маллера над полем $\mathbb{F}_q$ с параметрами q, r, m, удовлетворяющими условию (1) и $r < q$, $n = q^m$. Тогда можно построить ССШШ на базовом коде $\mathrm{RM}_q(r, m)$ с числом пользователей N_1, максимальной мощностью коалиций злоумышленников w_1, длиной пользовательского ключа R_1, и кодовую систему широковещательного шифрования на коде $\mathrm{RM}_q(r, m)$ с числом пользователей N_2, максимальной мощностью коалиций злоумышленников w_2, длиной пользовательского ключа R_2. При этом будут выполняться неравенства

$$N_2 \leq N_1, R_2 \geq R_1, w_2 \geq w_1.$$

Полученные результаты подтверждают выводы о соотношениях между величинами w и R: рост величины w в случае увеличения длины ключа R. Далее указываются преимущества и недостатки исследуемых систем и их использования в различных областях народного хозяйства, а также приводятся иллюстративные примеры длин ключей пользователей систем в зависимости от числа пользователей, в которых длина вектор-ключа λ выбирается для первой СШШ исходя из рекомендаций для длины

ключа используемой конкретной криптосистемы, а для второй СШШ – с целью исключения успешной атаки на систему, основанной на методе полного опробования ключей:

$$N_1 = 1000, w_1 = 2 \Rightarrow \mathrm{RM}_{11}(2,1) \Rightarrow R_1 = 11 + \lambda, R_2 = 8 + 8 * \lambda \Rightarrow N_2 = 11, w_2 = 7,$$
$$N_1 = 10000, w_1 = 3 \Rightarrow \mathrm{RM}_{23}(1,2) \Rightarrow R_1 = 529 + \lambda, R_2 = 526 + 526 * \lambda \Rightarrow N_2 = 529, w_2 = 504,$$
$$N_1 = 100000, w_1 = 4 \Rightarrow \mathrm{RM}_{47}(2,1) \Rightarrow R_1 = 47 + \lambda, R_2 = 44 + 44 * \lambda \Rightarrow N_2 = 47, w_2 = 43,$$
$$N_1 = 1000000, w_1 = 5 \Rightarrow \mathrm{RM}_{79}(3,1) \Rightarrow R_1 = 79 + \lambda, R_2 = 75 + 75 * \lambda \Rightarrow N_2 = 79, w_2 = 74.$$

В заключении главы предлагаются возможные области применения построенных программных средств защиты информации. Отмечается, что программные средства можно использовать в том числе для защиты информации новостных ресурсов сети с платным доступом, баз данных обновляемых программ, правовых и других сведений. При этом основополагающими критериями выбора средств защиты данных систем и их параметров для организации являются количество пользователей системы и объем памяти для хранения ключей, предпочтения тем или иным из которых формируются исходя из масштаба прогнозируемого рынка потребителей широковещательного сервиса и экономических возможностей использующей программные средства организации.

Заключение

В заключении приведены следующие основные результаты работы:

1. Построены новые системы широковещательного шифрования на базе q-ичных кодов Рида-Маллера, позволяющие противодействовать угрозам атак коалиций с целью предотвращения утечки информации.

2. Получены теоретические обоснования оценок границ применимости системы широковещательного шифрования, построенной на основе на кодов Рида-Маллера над полем $\mathbb{F}_q$, представляющие, в частности, математические принципы и решения для создания, изучения и совершенствования перспективных моделей и средств защиты информации с использованием других помехоустойчивых кодов.

3. Получены основанные на теоретических и экспериментальных исследованиях способы выбора параметров системы, позволяющие гарантировать защиту распространяемых данных от коалиционных атак.

4. Разработана классификация уязвимостей кодовой подсистемы распределения ключей системы защиты широковещательной передачи данных в моделях сервера и генерации закрытого ключа конференции при превышении порога мощности коалиции злоумышленников и получены на основе этой классификации теоретические результаты о вероятностях компрометации ключевых данных пользователей.

5. Получен новый способ оценки эффективности кодовых моделей распределения ключей, основанный на спектральных свойствах применяемых в них кодов.

Полученные результаты позволяют безопасно передавать широковещательно распространяемые данные в многопользовательских приложениях, например, тиражирование финансовых новостей и иных закрытых для публичного доступа сведений, цифровой телевидение и др., в условиях небольшого пользовательского ключевого пространства и коалиционных атак.

Список работ, опубликованных автором по теме диссертации

1. Евпак, С. А. Уязвимости полилинейной системы распределения ключей / В. М. Деундяк, С. А. Евпак // Международная научная конференция «Современные методы и проблемы теории операторов и гармонического анализа и их приложения – V» в г. Ростове-на-Дону. Материалы конференции. — 2015. — С. 154–155.
2. Евпак, С. А. Уязвимости полилинейной системы распределения ключей в случае превышения порога мощности коалиции злоумышленников / В. М. Деундяк, С. А. Евпак // Труды научной школы И. Б. Симоненко. Выпуск второй. — Ростов-на-Дону : ЮФУ, 2015. — С. 105–115.
3. Евпак, С. А. Об оценивании вероятности уязвимостей полилинейной системы распределения ключей / В. М. Деундяк, С. А. Евпак, А. А. Таран // Международная научная конференция «Современные методы и проблемы теории операторов и гармонического анализа и их приложения – VI». Материалы конференции. — 2016. — С. 133–134.
4. Евпак, С. А. Вероятностный метод в оценке эффективности систем распределения ключей / С. А. Евпак // Международная научная конференция «Современные методы и проблемы теории операторов и гармонического анализа и их приложения – VII». Материалы конференции. — 2017. — С. 142–142.
5. Евпак, С. А. Применение q-ичных кодов Рида-Маллера в схемах специального широковещательного шифрования / С. А. Евпак, В. В. Мкртичян // Труды научной школы И. Б. Симоненко. — Ростов-на-Дону : ЮФУ, 2010. — С. 93–99.
6. Евпак, С. А. Исследование возможности применения q-ичных кодов Рида-Маллера в схемах специального широковещательного шифрования / С. А. Евпак, В. В. Мкртичян // Известия вузов. Северо-Кавказский регион. Естественные науки. — 2011. — № 5. — С. 11–15.
7. Евпак, С. А. Об исследовании возможности применения q-ичных кодов Рида-Маллера в специальных схемах защиты информации от НСД / С. А. Евпак, В. В. Мкртичян // Обозрение Прикладной и Промышленной Математики. — 2011. — Т. 18, вып. 2. — С. 268–269.
8. Евпак, С. А. О границах применения специальной схемы защиты информации, основанной на q-ичных кодах Рида-Маллера / С. А. Евпак, В. В. Мкртичян // Материалы XIII Международной научно-практической конференции «ИБ-2013». — 2013. – Ч.1. — С. 211–215.
9. Евпак, С. А. О связи границ применения специальной схемы защиты информации, основанной на q-ичных кодах Рида-Маллера / С. А. Евпак, В. В. Мкртичян // Известия ЮФУ. Технические науки. — 2013. — № 12 (149). — С. 194–200.
10. Евпак, С. А. Условия применения q-ичных кодов Рида-Маллера в специальных схемах защиты информации от несанкционированного доступа / С. А. Евпак, В. В. Мкртичян // Владикавказский математический журнал. — 2014. — Т. 16, вып. 2. — С. 27–34.
11. Евпак, С. А. Исследование свойств q-ичных кодов Рида-Маллера как кодов защиты от копирования / В. М. Деундяк, С. А. Евпак, В. В. Мкртичян // Проблемы передачи информации. — 2015. — Т. 51, вып. 4. — С. 110–122.
12. Евпак, С. А. Монотонность рубежей в специальной схеме защиты информации, основанной на q-ичных кодах Рида-Маллера / В. М. Деундяк, С. А. Евпак,

В. В. Мкртичян // Известия ЮФУ. Технические науки. — 2015. — № 5 (166). — С. 56–64.
13. Евпак, С. А. О программной реализации модели распространения данных схемы специального широковещательного шифрования / С. А. Евпак, В. В. Мкртичян // Интегро-дифференциальные операторы и их приложения: Сб. статей / Межвузовский сборник научных трудов. — Ростов-на-Дону : изд. центр ДГТУ, 2008. – Вып. 8. — С. 61–71.
14. Свид. 2013661562 Российская Федерация. Свидетельство о государственной регистрации программы для ЭВМ. Модель распространения данных схемы специального широковещательного шифрования / С.А. Евпак ; заявитель и правообладатель С.А. Евпак. – №2013619311 ; заявл. 17.10.2013 ; опубл. 10.12.2013, Реестр программ для ЭВМ. – 1 с.
15. Yevpak, S. A. The special broadcast security scheme based on RM-codes and the protection from some linear algebraic attacks / S. A. Yevpak // Numerical algebra with applications. Proceedings of Fourth China-Russia Conference. ”— 2015. ”— P. 183–183.
16. Евпак, С. А. Выбор параметров для безопасного функционирования схем специального широковещательного шифрования на q-ичных кодах Рида-Маллера / С. А. Евпак // Труды научной школы И. Б. Симоненко. Выпуск второй. — Ростов-на-Дону : ЮФУ, 2015. — С. 136–143.

Подписано в печать 23.03.2018 г.

Печать ризограф. Бумага офсетная. Гарнитура «Таймс»

Формат 60х84/16. Объем 1,0 уч.-изд.-л.

Заказ № 4931. Тираж 120 экз.

Отпечатано в копировально-множительном центре

www.kcentr.com / +7 863 250 11 25

ул. Суворова, 19

КОПИЦЕНТР

осн.в 1996 году