

ЗАКЛЮЧЕНИЕ ДИССЕРТАЦИОННОГО СОВЕТА Д 002.077.05,
СОЗДАННОГО НА БАЗЕ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО
БЮДЖЕТНОГО УЧРЕЖДЕНИЯ НАУКИ ИНСТИТУТА ПРОБЛЕМ
ПЕРЕДАЧИ ИНФОРМАЦИИ им. А. А. ХАРКЕВИЧА
РОССИЙСКОЙ АКАДЕМИИ НАУК
ПО ДИССЕРТАЦИИ НА СОИСКАНИЕ УЧЕНОЙ СТЕПЕНИ
ДОКТОРА НАУК

аттестационное дело № _____

решение диссертационного совета

от «18» октября 2021 года, протокол № 51

О присуждении Лебедеву Владимиру Сергеевичу, гражданину Российской Федерации ученой степени доктора физико-математических наук.

Диссертация «Коды для каналов множественного доступа и задачи комбинаторного поиска» по специальности 05.13.17 – Теоретические основы информатики (физико-математические науки), принята к защите 5 июля 2021 года, протокол № 50, диссертационным советом Д 002.077.05, созданном на базе Федерального государственного бюджетного учреждения науки Института проблем передачи информации им. А. А. Харкевича Российской академии наук (127051, Москва, Б. Каретный пер., 19, строение 1, приказ о создании диссертационного совета от «10» июля 2015 года № 784/нк).

Соискатель Лебедев Владимир Сергеевич, 04 февраля 1965 года рождения.

Диссертацию на соискание ученой степени кандидата физико-математических наук на тему «Некоторые задачи оценивания в случайных гауссовских полях» по специальности 01.01.05 – Теория вероятностей и

математическая статистика защитил 18 июня 1991 года в Совете Московского института электронного машиностроения.

Работает старшим научным сотрудником лаборатории № 4 - Добрушинская математическая лаборатория - Федерального государственного бюджетного учреждения науки Института проблем передачи информации им. А.А. Харкевича Российской академии наук (ИППИ РАН).

Диссертация на соискание ученой степени доктора физико-математических наук выполнена в Добрушинской математической лаборатории Федерального государственного бюджетного учреждения науки Института проблем передачи информации им. А.А. Харкевича Российской академии наук.

Официальные оппоненты:

1. Дьячков Аркадий Георгиевич, доктор физико-математических наук, профессор, профессор кафедры теории вероятностей механико-математического факультета Федерального государственного образовательного учреждения высшего профессионального образования «Московский государственный университет имени М.В.Ломоносова»,
2. Кротов Денис Станиславович доктор физико-математических наук, профессор РАН, главный научный сотрудник лаборатории алгебраической комбинаторики Федерального государственного бюджетного учреждения науки Института математики им. С. Л. Соболева Сибирского отделения Российской академии наук,
3. Леонтьев Владимир Константинович доктор физико-математических наук, профессор, главный научный сотрудник отдела 13 отделения 1 Федерального исследовательского центра «Информатика и управление» Российской академии наук

дали *положительные* отзывы о диссертации.

Ведущая организация – Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет «Высшая школа экономики» (далее НИУ ВШЭ) - в своем *положительном* отзыве, подписанном заместителем директора Московского института электроники и математики им. А.Н.Тихонова (МИЭМ) НИУ ВШЭ, кандидатом технических наук, доцентом Аксеновым Сергеем Алексеевичем, профессором МИЭМ НИУ ВШЭ, доктором технических наук, профессором Нефедовым Сергеем Игоревичем и утвержденном доктором экономических наук профессором Радаевым Вадимом Валерьевичем, первым проректором НИУ ВШЭ указала, что выводы и подходы диссертации могут быть полезны для различного рода приложений. Практическая ценность полученных результатов определяется тем, что они могут применяться в дальнейших исследованиях в области теории кодирования, криптографии и комбинаторного поиска. Отзыв рассмотрен и одобрен на заседании НТС Московского института электроники и математики им. А.Н.Тихонова федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский университет «Высшая школа экономики», протокол № 1 от «25» сентября 2021 года.

Соискатель имеет 42 опубликованных работы, из них 31 по теме диссертации (в рецензируемых научных изданиях 17 работ) общим объемом 237 машинописных страниц, в том числе с соавторами 22 работы (вклад соискателя 173 страницы). В работах, опубликованных в соавторстве, Лебедеву Владимиру Сергеевичу принадлежат идеи доказательств всех основных результатов диссертации, а соавторам принадлежат доказательства некоторых утверждений, не вошедших в диссертацию.

Наиболее значимые работы по теме диссертации:

1. Делле, К. Задача группового тестирования с двумя дефектами / К. Делле, В. С. Лебедев // Проблемы передачи информации — 2013. — Т.49, №.4. — С. 87-94.

2. Лебедев, В. С. Асимптотическая верхняя граница для скорости кодов, свободных от (w,r) -перекрытий / В. С. Лебедев // Проблемы передачи информации — 2003. — Т.39, No.4. — С. 3-9.
3. Лебедев, В. С. Кодирование при наличии бесшумной обратной связи / В. С. Лебедев // Проблемы передачи информации — 2016. — Т.52, No.2. — С. 3-14.
4. Deppe, C. Algorithms for q-ary error-correcting codes with limited magnitude and feedback / C. Deppe, V. Lebedev // Discrete Mathematics. — 2021. — V. 344, No. 2. — P. 112199.
5. Kim, H. K. On Optimal Superimposed Codes / H. K. Kim , V. S. Lebedev // Journal of combinatorial designs. — 2004. — V. 12, No. 2. — P. 79-91.

На диссертацию и автореферат поступило 6 отзывов, включая отзывы официальных оппонентов и ведущей организации, каждый из которых содержит положительную оценку работы Лебедева В.С. и вывод о её соответствии требованиям, предъявляемым Высшей аттестационной комиссией к докторским диссертациям на соискание степени доктора физико-математических наук по специальности 05.13.17 – «Теоретические основы информатики».

В отзыве ведущей организации сделаны следующие замечания, которые не оказывают влияния на общую положительную оценку работы.

1. Автор вводит понятие композиционного расстояния, которое правильно называть не расстоянием, а весом или нормой, так как это одноместная, а не двухместная функция.
2. Там же, в третьей главе, получена рекуррентная верхняя граница для скорости кодов, свободных от перекрытий, теорема 8. К сожалению, автор не исследовал детально, что даст эта рекуррента в наиболее простом, как нам кажется, случае $w=r$, когда представляется возможным осуществить рекуррентный спуск без особо громоздких вычислений.

В отзыве официального оппонента доктора физико-математических наук, профессора Дьячкова Аркадия Георгиевича отмечены некоторые недостатки, которые не снижают научную ценность работы, а именно:

1. в диссертации имеются грамматические ошибки и опечатки, затрудняющие ее чтение;
2. также стоило дать более подробный литературный обзор главы 2;
3. некоторые результаты исследований дизъюнктивных кодов заслуживают более полного их изложения.

В отзыве официального оппонента доктора физико-математических наук, профессора Леонтьева Владимира Константиновича к недостаткам диссертации отнесены следующие моменты, связанные с изложением результатов.

1. Недостаточная продуманность в порядке изложения результатов.
2. Описание основных моделей (К.М.Д, дизъюнктивный канал, К.М.Д с суммированием) даются очень кратко и формально без достаточного числа пояснений и примеров.

В отзыве официального оппонента доктора физико-математических наук, профессора РАН Кротова Дениса Станиславовича есть следующие замечания, которые не умаляют значимости для теории и практики результатов диссертационной работы Лебедева В.С.

1. Формальные определения не всегда самодостаточны и даже корректны, их бывает трудно понять без окружающего контекста.
2. Обозначения $[N]$, $[i,j]$ определяются в разделе 2.2, а используются гораздо раньше.
3. Имеются отдельные несогласования падежей и потери управления словами.

В отзыве на автореферат доктора технических наук Беззатеева Сергея Валентиновича, заведующего кафедрой технологий защиты информации Санкт Петербургского государственного университета

аэрокосмического приборостроения имеются следующие замечания.

1. Из приведенного на стр.9 описания задачи Станислава Улама неясно, что понимается под недвоичным случаем.
2. Из описания на странице 15 неясно, почему длина информационной последовательности равна $n-(r+1)t$, это косвенно поясняется только на стр. 16.
3. К сожалению, автор не привел заявленный алгоритм поиска двух дефектных элементов.

На странице 18 речь идет о решении задачи поиска активных пользователей «Во втором разделе второй главы изучается задача нахождения одного из нескольких активных пользователей» однако, к сожалению, не приводится результат решения этой задачи, так как далее автор пишет о дефектных элементах.

В отзыве на автореферат доктора технических наук Трифонова Петра Владимировича, профессора факультета безопасности информационных технологий Федерального государственного автономного образовательного учреждения высшего образования «Университет ИТМО» отмечены следующие недостатки.

1. Несмотря на то, что коды для каналов множественного доступа вынесены в название работы, в автореферате не приведено сравнение полученных результатов с применяемыми в настоящее время конструкциями, включая недавно предложенные методы неортогонального множественного доступа, в частности SCMA.
2. В автореферате не описаны алгоритмы декодирования предложенных кодов.
3. На стр. 3 в предложении «...что математическая КМД представляет из себя...», вероятно, пропущено слово.

Выбор официальных оппонентов и ведущей организации обосновывается их компетентностью в исследуемой области, что подтверждается научными публикациями. Доктор физико-математических наук, профессор Дьячков Аркадий Георгиевич является авторитетным специалистом в области теории кодирования и комбинаторного поиска, автором множества научных работ в наиболее выдающихся журналах в этой области. Доктор физико-математических наук, профессор РАН Кротов Денис Станиславович является признанным специалистом в области теории графов, теории кодирования и защиты информации и имеет множество работ в высокорейтинговых математических журналах. Доктор физико-математических наук, профессор Леонтьев Владимир Константинович является авторитетным специалистом в области теории кодирования и защиты информации, является автором множества работ по этой тематике. Ведущая организация Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет «Высшая школа экономики» выполняет теоретические исследования в области передачи и защиты информации, результаты которых публикуются в ведущих международных рецензируемых научных изданиях.

Диссертационный совет отмечает, что на основании выполненных соискателем исследований:

разработан комбинаторный подход рассмотрения задач поиска с точки зрения методов теории кодирования, позволивший получить важные научные результаты;

предложен новый метод исправления ошибок для q -ичного канала с безошибочной обратной связью, позволяющий строить новые коды для решения задач передачи и защиты информации;

доказана оптимальность алгоритма 1-удаления для большой доли ошибок в канале, теорема о свойствах адаптивного алгоритма поиска двух дефектных

элементов, которая позволила уточнить и улучшить ранее известные результаты, теорема об оптимальности некоторых кодов, свободных от перекрытий, теоремы о скорости кодов, свободных от перекрытий, позволившая получить наилучшие на настоящее время результаты о верхней границе скорости таких кодов;

предложен новый алгоритм поиска для канала множественного доступа с двумя входами, позволяющий получить оптимальную константу при главном члене асимптотического разложения для общего числа пользователей;

введено понятие композиционного расстояния и получена граница на скорость кодов с таким композиционным расстоянием.

Теоретическая значимость исследования обоснована тем, что: применительно к проблематике диссертации, результативно использован комбинаторный подход, позволяющий получать более точные оценки характеристик некоторых кодов, используемых для передачи и защиты информации, доказаны теоремы, вносящие вклад в расширение представлений о структуре кодов, свободных от перекрытий, изучены естественные обобщения хорошо известных и популярных задач комбинаторной теории поиска, проведена модернизация методов, обеспечивающих получение новых верхних границ на скорость кодов, свободных от перекрытий, исследована проблема нахождения одного из нескольких дефектных элементов.

Значение полученных соискателем результатов исследования для практики подтверждается тем, что они могут применяться в дальнейших исследованиях в области теории кодирования, криптографии и комбинаторного поиска. Также результаты работы могут быть использованы в разных практических областях: в практической криптографии, медицине, биологии и др.

Оценка достоверности результатов исследования выявила: идеи, позволяющие получать новые результаты, базируются на обобщении передового опыта, в том числе на обобщении идей предыдущих исследователей, теория построена на известных опубликованных в ведущих математических журналах фактах, все результаты обоснованы строгими математическими доказательствами, положения и выводы, сформулированные в диссертации, получили квалифицированную апробацию на международных и российских научных конференциях и семинарах, достоверность также подтверждается публикациями результатов исследования в рецензируемых научных изданиях, в том числе, рекомендованных ВАК.

Личный вклад соискателя состоит в том, что все результаты диссертации получены лично автором или непосредственно при его участии.

В ходе защиты диссертации были высказаны замечания о невозможности существования на практике каналов множественного доступа с мгновенной обратной связью.

Соискатель Лебедев В.С. аргументировано ответил на замечания, высказанные в отзыве на автореферат Трифоновым П.В., согласился с остальными замечаниями и ответил на все задаваемые ему в ходе заседания вопросы.

Содержание диссертации соответствует паспорту специальности 05.13.17 – теоретические основы информатики, в частности, пунктам:

- п. 11 – Разработка методов обеспечения высоконадежной обработки информации и обеспечения помехоустойчивости информационных коммуникаций для целей передачи, хранения и защиты информации; разработка основ теории надежности и безопасности использования информационных технологий.

На заседании 18 октября 2021 года диссертационный совет принял решение, что диссертация Лебедева Владимира Сергеевича «Коды для каналов множественного доступа и задачи комбинаторного поиска» является законченной научно-квалификационной работой на актуальную тему, в которой на основании выполненных диссертантом исследований разработаны теоретические положения, совокупность которых можно квалифицировать как научное достижение в области разработки методов обеспечения помехоустойчивости информационных коммуникаций для целей передачи и защиты информации. Диссертационный совет решил присудить Лебедеву Владимиру Сергеевичу ученую степень доктора физико-математических наук по специальности 05.13.17 – Теоретические основы информатики.

При проведении тайного голосования диссертационный совет в количестве 28 человек, из них 5 докторов наук по специальности и отрасли наук рассматриваемой диссертации, участвовавших в заседании, из 36 человек, входящих в состав совета, проголосовали: за присуждение учёной степени – 28, против присуждения учёной степени – 0.

Заместитель председателя

диссертационного совета Д 002.077.05



Соболевский А.Н.

Ученый секретарь

диссертационного совета Д 002.077.05

Цитович И.И.

18 октября 2021 г.