О научно-педагогической деятельности заслуженного деятеля науки Российской Федерации, профессора кафедры радиотехники и систем управления Московского физико-технического института (государственного университета) Габидулина Эрнста Мухамедовича

Э. М. Габидулин родился 4 июня 1937 года в рабочем поселке Кок-Янчак (Киргизия). Позже родители переехали в Казахстан, и юный Эрнст закончил школу с медалью в 1953 году в посёлке Мерке. В этом же году он приехал в Москву и поступил в МФТИ. Закончил институт с отличием в 1959 году. Заведующий кафедрой радиотехники Е. И. Манаев с согласия Комиссии по распределению молодых специалистов-выпускников МФТИ пригласил его на работу на кафедру. С этого года и вплоть до настоящего времени Эрнст Мухамедович работает на этой кафедре сначала как ассистент, после защиты кандидатской диссертации в 1975 году как доцент, после защиты докторской диссертации в 1985 году как профессор, а с 1987 года в течение 20 лет являлся заведующим кафедрой радиотехники. В настоящее время ведёт учебную и научную работу в должности профессора. В 2007 году Э. М. Габидулин получил звание заслуженного деятеля науки Российской Федерации.

Эрнст Мухамедович Габидулин является известным ученым в области теории информации, теории связи, алгебраической теории кодирования, криптографии и теории последовательностей. В 1986 году им в соавторстве с профессором В. Б. Афанасьевым опубликована монография «Кодирование в радиоэлектронике», а к настоящему времени опубликовано в отечественных и зарубежных журналах около 200 статей, содержащих ряд фундаментальных научных результатов.

Научные работы Э. М. Габидулин ведёт в следующих направлениях.

1. Исследования в области теории информации

Основной проблемой в математической теории связи является нахождение характеристик (вероятности ошибок, сложность и др.) для различных сценариев передачи и выбора входных сигналов. В раннем цикле работ Э. М. Габидулин исследовал сначала потенциальные возможности линейных, групповых и смежногрупповых кодов. Было показано, что роль пропускной способности в этом случае играет средняя взаимная информация между входом и выходом канала связи при равномерном распределении на входе. Далее были предложены оригинальные методы для решения трудной задачи: вычисления функций надежности для широкого класса каналов, таких как каналы с конечной памятью, каналы с вычислимыми состояниями.

2. Исследования в области алгебраической теории кодирования

В этом цикле Э. М. Габидулин разработал полную теорию групповых и смежногрупповых кодов в самом общем случае, когда для различных компонент кодовых векторов используются различные алфавиты. Было показано, что общий случай алфавитов в виде произвольных групп сводится к случаю, когда порядки всех групп являются различными степенями одного и того же простого числа. Выведены производящие функции, позволяющие вычислять различные средние характеристики групповых и смежно-групповых кодов. Найдено необходимое и достаточное условие, которому должен удовлетворять некоторый код, чтобы двойственный к нему код имел заданное расстояние. Найдены общие нижние границы для объема оптимальных кодов. Предложены конструкции новых кодов, в частности, класс кодов с максимально достижимым расстоянием, получивший в дальнейшем название ранговых кодов Габидулина. В теории сверточных кодов был обнаружен эффект

неустойчивости декодера при однократном неконтролируемом внешнем воздействии на состояние декодера. Предложены также коды с большим свободным расстоянием. Ряд работ посвящен метрикам в теории кодирования и кодам в этих метриках. Выбор метрики важен при согласовании кода и канала связи. Наиболее вероятным ошибкам должны соответствовать векторы с малой нормой. Было предложено несколько классов метрик, перспективных с практической точки зрения. Комбинаторные метрики, введенные Э. М. Габидулиным, полезны для каналов с аддитивным шумом. Изучены общие свойства комбинаторных метрик. Найдены верхние и нижние границы для объема оптимального кода, исправляющего ошибки в ранговой метрике. Получено много конкретных результатов для известных и вновь введенных метрик: найдены верхние и нижние границы для пакетной и более общей пакетно-хэмминговой метрики, для неравномерной метрики Хэмминга, для модульной метрики. Другой класс метрик – проективные метрики – был введен и изучен в связи с задачами криптографии.

3. Методы кодирования для параллельных каналов и ранговая метрика

Параллельные каналы являются одним из наиболее важных для изучения объектов как в теории связи, так и в прикладной теории информации. Такие каналы подвержены не только воздействию естественных шумов, но и воздействию намеренных и непреднамеренных помех искусственного происхождения. Сигналы, передаваемые по параллельным каналам, можно интерпретировать как матрицы. Типичные ошибки имеют решетчатую структуру: искажаются некоторые строки и некоторые столбцы. Впервые в мировой литературе такая модель была рассмотрена в работе Э. М. Габидулина, В. И. Коржика «Коды, исправляющие ошибки решетчатой конфигурации» (Изв. вузов. Радиоэлектроника. 1982. Т. 15, № 4), а также относящихся к этому же времени докладах Э. М. Габидулина на международных и всесоюзных конференциях. Адекватной метрикой для такого канала является граничноранговая метрика. Однако построить оптимальные коды в этой метрике удалось только в некоторых частных случаях. Позднее Э. М. Габидулин ввел другую метрику, названную ранговой метрикой (Оптимальные коды, исправляющие ошибки решетчатой конфигурации // Тр. VI Междунар. симп. по теории информации, Ч. II, М.-Ташкент, 1984; Теория кодов с максимальным ранговым расстоянием // Проблемы передачи информации. 1985. Т. 21, № 1). Была разработана законченная теория кодов в этой метрике. Именно для всех допустимых параметров найдены оптимальные коды, исправляющие ранговые ошибки, в том числе и гранично-ранговые ошибки. Найдены быстрые алгоритмы кодирования и декодирования, делающие этот класс кодов пригодным для практики. Идея ранговых кодов оказалась плодотворной и вызвала поток статей других исследователей, не прекращающийся до сих пор.

4. Работы по криптологии

С середины 80-х годов прошлого века алгебраические методы кодирования, в частности линейные коды, начали использоваться в криптосистемах с открытым ключом. Первоначально использовались коды в метрике Хэмминга. Однако размер открытого ключа оказался слишком велик для практических применений. Э. М. Габидулин и его ученики А. В. Парамонов и О. В. Третьяков предложили криптосистему, основанную на ранговых кодах, с приемлемым размером ключа. Эта система использует ранговую метрику в чистом виде. Однако в последующих работах были привлечены и другие проективные метрики, введенные Э. М. Габидулиным. Наиболее проработанными являются криптосистемы на основе проективной метрики Вандермонда и проективной метрики Фробениуса. Таким образом, сложилось целое направление, посвященное разработке криптосистем, основанных на линейных кодах в различных метриках.

5. Исследования по теории последовательностей

Цикл работ Э. М. Габидулина посвящен построению последовательностей с «хорошими» корреляционными свойствами. Последовательность комплексных чисел называется совершенной, если при любом ненулевом сдвиге соответствующий периодический корреляционный коэффициент равен нулю. Такие последовательности имеют многочисленные

практические применения. В работах Э. М. Габидулина исследовался вопрос о частичной классификации совершенных унимодальных последовательностей. Впервые показано, что если длина последовательности – простое число или число, свободное от квадратов, то число совершенных последовательностей конечно с точностью до эквивалентности. Если длина последовательности – степень простого числа, то множество совершенных последовательностей образует многообразие, размерность которого равна степени того же простого числа на единицу меньшей. Разработано большое количество конкретных конструкций совершенных последовательностей.

6. Организационная научная и педагогическая деятельность

Э. М. Габидулин в течение многих лет член диссертационных советов ФРТК и ФУПМ МФТИ (ГУ) по защите кандидатских и докторских диссертаций. Он является экспертом журнала РАН «Проблемы передачи информации». Э. М. Габидулин был членом Оргкомитетов и Программных комитетов многих Международных симпозиумов и конференций, а также организатором и председателем Оргкомитета Международной конференции по теории информации (1994 г., Москва). С 1995 года в течение 15 лет ежегодно во время летних отпусков работал в университетах Нидерландов, Англии, Германии, Франции, Испании, Швеции, Норвегии, Бразилии. Научные контакты с учеными этих стран, а также США, Канады, Японии, Китая, Австралии продолжаются до сих пор. С самого начала педагогической деятельности Э. М. Габидулин читает лекции по радиотехнике и пишет учебные пособия. Первые пять учебных пособий по радиоэлектронике были написаны в 1972, 1973, 1978, 1979 и 1980 годах в соавторстве с Л. П. Куклевым. Им введены и прочитаны новые курсы в МФТИ по теории информации и защите информации. Изданы пособия «Лекции по теории информации» (2007 г., соавтор Н. И. Пилипчук), «Защита информации» (2011 г., соавторы – А. С. Кшевецкий, А. И. Колыбельников), «Криптографические методы защиты информации» (2016 г., соавторы – С. М. Владимиров, А. И. Колыбельников, А. С. Кшевецкий).

Под его руководством 12 человек защитили кандидатские диссертации. В настоящее время Э. М. Габидулин является руководителем научного коллектива из 10 человек, который проводит научные исследования по теме «Развитие теории сетевого кодирования и защиты информации в телекоммуникационных сетях». Финансовая поддержка – гранты РФФИ по трём проектам (2009–2011, 2012–2014, 2015–2017).

С осеннего семестра 2016 г. он является научным руководителем двух аспирантов МФТИ (из Вьетнама) – Ван Ву Киена и Нгуена Зы Хоана на четырёхлетний период аспирантуры. В мае с.г. запланирована защита кандидатской диссертации О. В. Трушиной.

Э. М. Габидулин является руководителем постоянно действующего научного семинара кафедры, состоялось 293 заседания. Научная работа успешно продолжается: за период с 2015 г. по настоящее время опубликовано 10 научных статей в соавторстве с отдельными членами руководимого им научного коллектива.