Math-Net.Ru

Общероссийский математический портал

Памяти Алексея Сергеевича Кузьмина (1960–2016), *Матем. вопр. криптогр.*, 2016, том 7, выпуск 4, 5–6

DOI: <https://doi.org/10.4213/mvk209>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.84.234.179

26 апреля 2023 г., 18:02:11

**Памяти Алексея Сергеевича Кузьмина
1960 – 2016**

Отечественная криптографическая школа понесла тяжелую утрату: ушел из жизни ведущий криптограф и организатор научных исследований, действительный член Академии криптографии Российской Федерации

КУЗЬМИН АЛЕКСЕЙ СЕРГЕЕВИЧ

Алексей Сергеевич внес существенный вклад в развитие отечественной теоретической и прикладной криптографической науки.

Областью научных интересов А. С. Кузьмина была алгебра и ее приложения к теоретической криптографии. Эти вопросы были темой его кандидатской диссертации, защищенной в 1986 году под руководством А. А. Нечаева, и докторской диссертации (1995 г.). Алексей Сергеевич получил важные результаты практически во всех направлениях деятельности алгебраической школы А. А. Нечаева.

А. С. Кузьмин и А. А. Нечаев — авторы широко используемого «метода сечений» в теории линейных рекуррентных последовательностей над кольцами и модулями. Полученные А. А. Нечаевым и А. С. Кузьминым в начале 1980-х годов результаты лишь в середине 2000-х годов были повторены и частично усилены в работах зарубежных математиков.

Алексей Сергеевич разработал оригинальный математический аппарат, позволивший найти точные формулы для частот знаков на цикле старшей разрядной последовательности линейной рекуррентной максимальной длины над кольцом Галуа характеристики 4.

Его работы по свойствам гипербент-функций стали базой для дальнейших исследований его учеников, в том числе для ряда кандидатских диссертаций. Алексей Сергеевич щедро делился научными идеями с учениками и коллегами. Под его руководством защищено 7 кандидатских диссертаций; еще 3 диссертации были подготовлены к защите.

А. С. Кузьмин — один из авторов фундаментального учебного пособия «Основы криптографии», выдержавшего несколько изданий и рекомендованного Министерством образования и науки Российской Федерации для студентов вузов. Алексей Сергеевич Кузьмин был одним из главных организаторов Федерального учебно-методического объединения вузов Российской Федерации по информационной безопасности, бессменным членом президиума объединения и его деятельным участником. Внес огромный вклад в разработку и утверждение на государственном уровне системы федеральных государственных стандартов по специальностям в области информационной безопасности. За создание комплекта учебных пособий по криптографическим, программно-аппаратным, техническим методам и средствам защиты информации, обеспечивающего подготовку специалистов в области информационной безопасности, Алексей Сергеевич вместе с соавторами награжден Премией Правительства Российской Федерации в области образования. С 2011 года А. С. Кузьмин руководил деятельностью Технического комитета по стандартизации ТК 26, задачей которого является организация разработки национальных стандартов и методических рекомендаций в области защиты информации. Алексей Сергеевич являлся руководителем и организатором международного симпозиума «Современные тенденции в криптографии (СТCrypt)». Материалы этого симпозиума регулярно публикуются на страницах журнала «Математические вопросы криптографии». Алексей Сергеевич был активным членом редакционной коллегии нашего журнала.

Признанием роли и заслуг А. С. Кузьмина в области защиты информации стало избрание его действительным членом Академии криптографии Российской Федерации.

За плодотворную деятельность на научном поприще, большой личный вклад в решение научно-прикладных и теоретических проблем в области информационной безопасности Алексей Сергеевич награжден орденом Почета и орденом «За военные заслуги».

Светлая память об Алексее Сергеевиче Кузьмине навсегда сохранится в наших сердцах.

Главный редактор журнала
«Математические вопросы криптографии» В. Н. Сачков,
редакционная коллегия журнала