Заключение диссертационного совета МГУ.012.3
по диссертации на соискание ученой степени кандидата наук

Решение диссертационного совета от «12» ноября 2025 г. № 23 о присуждении Давыдову Степану Андреевичу, гражданину Российской Федерации, ученой степени кандидата физико-математических наук.

Диссертация «Анализ и синтез некоторых классов линейных и нелинейных преобразований для использования в XSL-схемах» по специальности 2.3.6 Методы и системы защиты информации, информационная безопасность принята к защите диссертационным советом «24» сентября 2025 г., протокол № 19.

Соискатель **Давыдов Степан Андреевич** в 2017 году окончил специалитет ФГКОУВО Академии ФСБ России, факультет прикладной математики института криптографии, связи и информатики по специальности 10.05.06 Криптография.

В настоящее время Давыдов С.А. является аспирантом очной аспирантуры факультета вычислительной математики и кибернетики МГУ имени М.В. Ломоносова по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность. Сданы государственные экзамены (соответствующие документы прилагаются).

Соискатель работает в АО «НПК «Криптонит» в должности старшего специалиста-исследователя лаборатории криптографии.

Диссертация выполнена на кафедре информационной безопасности факультета вычислительной математики и кибернетики МГУ имени М.В.Ломоносова.

Научный руководитель - Чижов Иван Владимирович, кандидат физико-математических наук, доцент кафедры информационной безопасности факультета вычислительной математики и кибернетики МГУ имени М.В.Ломоносова.

Официальные оппоненты:

- **Фомичев Владимир Михайлович**, доктор физико-математических наук, профессор, профессор кафедры теории вероятностей и кибербезопасности Российского университета дружбы народов имени Патриса Лумумбы;
- **Камловский Олег Витальевич**, доктор физико-математических наук, доцент, профессор кафедры 252 Института искусственного интеллекта МИРЭА-Российского технологического университета;
- **Таранников Юрий Валерьевич**, доктор физико-математических

наук, профессор кафедры дискретной математики механико-математического факультета Московского государственного университета имени М.В. Ломоносова;

дали положительные отзывы на диссертацию.

Выбор официальных оппонентов обосновывался тем, что оппоненты являются известными специалистами в области синтеза и анализа криптографических алгоритмов и имеют работы, близкие к теме диссертационного исследования, в центральных математических журналах.

Соискатель имеет 7 опубликованных работ, в том числе по теме диссертации 4 работы, из них 3 работы опубликованы в рецензируемых научных изданиях, рекомендованных для защиты в диссертационном совете МГУ по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность (физико-математические науки). Результаты диссертационной работы опубликованы в открытой печати.

Основные публикации по теме диссертации:

1. С. А. Давыдов, И. А. Круглов. Метод синтеза дифференциально 4-равномерных подстановок пространства Vm для четных m // Дискрет. матем. — 2019. — Т. 31, № 2. — С. 69—76. — (0.5 п.л., ВАК, RSCI, Двухлетний импакт-фактор РИНЦ без самоцитирования – 0.385) // Соавтору принадлежит постановка задачи. Основные результаты получены Давыдовым С.А. – 95%, 0.465 п.л., EDN: ZJDZIL.
2. С. А. Давыдов, Ю. Д. Шкуратов. Использование матриц-циркулянтов над F2 при построении эффективных линейных преобразований с высокими показателями рассеивания // Матем. вопр. криптогр. — 2024. — Т. 15, № 2. — С. 29—46. — (1.125 п.л., ВАК, RSCI, Двухлетний импакт-фактор РИНЦ без самоцитирования – 0.232) // Соавтору принадлежат лемма 1 и теорема 2. Остальные результаты получены Давыдовым С.А. – 86%, 0.9675 п.л., EDN: WYZJQK.
3. С. А. Давыдов. Об инвариантных подпространствах матриц-циркулянтов и рекурсивных матриц // Дискрет. матем. — 2024. — Т. 36, № 4. — С. 44—63. — (1.25 п.л., ВАК, RSCI, Двухлетний импакт-фактор РИНЦ без самоцитирования – 0.385) – 100%, EDN: YWWKFP.

Дополнительно поступило 2 отзыва на автореферат диссертации, все положительные.

Диссертационный совет отмечает, что представленная диссертация на соискание ученой степени кандидата физико-математических наук является

научно-квалификационной работой, в которой содержатся следующие результаты: предложена конструкция, позволяющая строить дифференциально 4-равномерные подстановки; найдены все степенны́е подстановки, к которым применима конструкция; доказана теорема о построении дифференциально 4-равномерных подстановок размерности $s=2k$ при произвольном k, обладающих максимально известной нелинейностью; для эффективной программной реализации матриц предложено их разложение в сумму произведений диагональных матриц и двоичных матриц-циркулянтов, получены оценки на число слагаемых в указанном разложении; для сопровождающей матрицы найдены все решения уравнения подобия матрицы и транспонированной матрицы; получены разложения рекурсивных матриц в произведения двух матриц, имеющих эффективную программную реализацию; полностью описаны инвариантные подпространства максимально рассеивающих матриц-циркулянтов размерности 2^k; показано отсутствие инвариантных подпространств определенного вида у рекурсивных матриц.

Диссертация представляет собой самостоятельное законченное исследование, обладающее внутренним единством. Положения, выносимые на защиту, содержат новые научные результаты и свидетельствуют о личном вкладе автора в науку:

- Конструкция, позволяющая строить дифференциально 4-равномерные подстановки произвольной чётной размерности, обладающие максимально известной нелинейностью.
- Теорема о минимальном числе слагаемых в разложении произвольной матрицы в сумму произведений диагональных матриц и двоичных циркулянтных матриц.
- Описание всех решений уравнения подобия для сопровождающей и её транспонированной матриц. Теорема о разложении произвольной рекурсивной матрицы в произведение двух матриц, имеющих эффективную программную реализацию.
- Теорема о подобии циркулянтной матрицы размера 2^k верхнетреугольной матрице Тёплица. Полное описание инвариантных подпространств максимально рассеивающих матриц-циркулянтов размера 2^k. Теорема об отсутствии инвариантных подпространств определенного вида у рекурсивных матриц.

В диссертации применяются математические методы из алгебры, теории булевых функций.

Результаты диссертации имеют законченный характер и снабжены строгими математическими доказательствами, являются новыми, прошли апробацию на международных конференциях и научных семинарах. Основные результаты диссертационной работы изложены в 4 работах, 3 из которых опубликованы в научных изданиях, индексируемых в базах данных WoS, Scopus, RSCI и рекомендованных для защиты в диссертационном совете МГУ по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

На заседании 12.11.2025 диссертационный совет принял решение присудить Давыдову С.А. ученую степень кандидата физико-математических наук.

При проведении тайного голосования диссертационный совет в количестве 19 человек, из них 4 доктора наук по специальности рассматриваемой диссертации, участвовавших в заседании, из 26 человек, входящих в состав совета, проголосовали: за 19, против 0, недействительных бюллетеней нет.

Заместитель председателя
диссертационного совета,
д.ф.-м.н., профессор **Васенин В.А.**

Ученый секретарь
диссертационного совета,
к.ф.-м.н. **Галатенко А.В.**

12.11.2025