



ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТІРЛІГІ
Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТИ

MINISTRY OF EDUCATION AND SCIENCE OF
THE REPUBLIC OF KAZAKHSTAN
L.N. GUMILYOV EURASIAN NATIONAL UNIVERSITY

*«Eurasian Mathematical Journal» журналының
шығарыла бастағанына 10 жыл толуына арналған*

**«АНАЛИЗДІҢ, ДИФФЕРЕНЦИАЛДЫҚ ТЕҢДЕУЛЕРДІҢ
ЖӘНЕ АЛГЕБРАНЫҢ ӨЗЕКТІ МӘСЕЛЕЛЕРІ» (EMJ-2019)**

атты халықаралық конференция

ТЕЗИСТЕР ЖИНАҒЫ

International Conference

**INTERNATIONAL CONFERENCE
«ACTUAL PROBLEMS OF ANALYSIS,
DIFFERENTIAL EQUATIONS AND ALGEBRA» (EMJ-2019)**

dedicated to the 10th anniversary of the Eurasian Mathematical Journal

THE ABSTRACT BOOK

**16-19 қазан 2019
Нұр-Сұлтан, Қазақстан**



ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТІРЛІГІ
Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ

MINISTRY OF EDUCATION AND SCIENCE OF
THE REPUBLIC OF KAZAKHSTAN
L.N. GUMILYOV EURASIAN NATIONAL UNIVERSITY

«Eurasian Mathematical Journal» журналының
шығарыла бастағанына 10 жыл толуына арналған

«АНАЛИЗДІҢ, ДИФФЕРЕНЦИАЛДЫҚ ТЕНДЕУЛЕРДІҢ ЖӘНЕ
АЛГЕБРАНЫҢ ӨЗЕКТІ МӘСЕЛЕЛЕРІ » (EMJ-2019)
атты халықаралық конференция

ТЕЗИСТЕР ЖИНАҒЫ

International Conference
«ACTUAL PROBLEMS OF ANALYSIS, DIFFERENTIAL EQUATIONS
AND ALGEBRA» (EMJ-2019)
dedicated to the 10th anniversary of the Eurasian Mathematical Journal

THE ABSTRACT BOOK

16-19 қазан 2019
Нұр-Сұлтан, Қазақстан

ӘОЖ 51
КБЖ 22.1
А 56

«Анализдің, дифференциалдық теңдеулердің және алгебраның өзекті мәселелері» (EMJ-2019): «Eurasian Mathematical Journal» журналының шығарыла бастағанына 10 жыл толуына арналған халықаралық конференцияның тезистер жинағы.-Нұр-Сұлтан: Л.Н. Гумилев атындағы Еуразия ұлттық университеті, 2019. -183 б.

«Актуальные проблемы анализа, дифференциальных уравнений и алгебры»(EMJ-2019): Сборник тезисов международной конференции, посвященной 10-летию выпуска журнала «Eurasian Mathematical Journal».-Нур-Слтан: Евразийский национальный университет имени Л.Н. Гумилева, 2019. -183 с.

International Conference «Actual problems of analysis, differential equations and algebra» (EMJ-2019) dedicated to the 10th anniversary of the Eurasian Mathematical Journal. –Nur-Sultan: L.N. Gumilyov Eurasian National University, 2019. -183 p.

ISBN 978-601-7590-58-1

ӘОЖ 51
КБЖ 22.1
© Л.Н. Гумилев атындағы ЕҰУ, 2019

Мазмұны/Contents/Содержание

| | |
|---|-----------|
| Функциялар теориясы және функционалдық талдау | 12 |
| А.М. Абылаева Двухвесовая оценка интегрального оператора с логарифмической особенностью | 13 |
| А.Н. Адилханов, Ж.М. Онербек О достаточных условиях ограниченности потенциала Рисса в глобальных пространствах типа Морри с переменным показателем | 14 |
| А.Ж. Адиева, А.О. Байарыстанов Об одном переопределенном весовом неравенстве типа Харди в дифференциальной форме | 15 |
| А.Ж. Адиева, Р. Ойнаров, Я.Т. Султанаев Весовое неравенство и дискретность спектра полярного оператора высокого порядка | 17 |
| Г. Акишев Оценки наилучших приближений функций класса Никольского - Бесова в пространстве Лоренца | 18 |
| A.R. Aliev, Sh.Sh. Rajabov Essential self-adjointness of the magnetic helmholtz operator | 18 |
| Д.Б. Базарханов Оптимальное восстановление псевдодифференциальных операторов на классах гладких периодических функций многих переменных | 19 |
| К.А. Бекмаганбетов, Е. Толеугазы Об оценке наилучших приближений смешанных дробных производных в анизотропной метрике | 19 |
| А.Т. Бесжанова, А.М. Темирханова Ограниченность и компактность одного класса матричных операторов с переменными пределами суммирования | 22 |
| Н.А. Бокаев, А.А. Хайркулова Об оценке нормы в дискретных пространстве Орлича - Морри | 23 |
| Н.К. Блиев Многомерные сингулярные интегралы и интегральные уравнения в дробных пространствах | 25 |
| N.A. Bokayev, E.S. Smailov, A.T. Syzdykova Embedding theorems for Besov type generalized spaces with respect to multiplicative systems | 26 |
| P.D. Lamberti, V. Vespri Generalised Campanato spaces and Hardy spaces | 28 |
| P.D. Lamberti, V. Vespri Remarks on Sobolev- Morrey-Campanato spaces defined on $c^{0,\gamma}$ domains | 28 |
| М.Г. Гадоев, Ф.С. Исхоков О разделимости одного класса вырождающихся дифференциальных операторов | 29 |
| R. J. Heydarov Constructive method for solving an impedance boundary value problem for Helmholtz equation | 29 |
| Н.С. Даирбеков, О.М. Пенкин, Л.О. Сарыбекова Обобщенное неравенство соболева на стратифицированном множестве | 31 |
| D. Dautbek, J. Huang and F. Sukochev Extreme points of the set of elements majorised by an integrable function | 32 |
| А.А. Джумабаева, А.Е. Жетписбаева Неравенство наилучшего приближение со ступенчатым крестом | 33 |
| Г.Ж. Каршыгина Опоточечном эквивалентности конусов функций с условиями монотонности | 35 |
| Ж.А. Кеулимжаева Эквивалентные нормы пространства с мультивесовыми производными | 37 |
| A.N. Kopezhanova Some new inequalities for the Fourier transform | 39 |
| Л.К. Кусаинова, А.С. Касым Коэрцитивные оценки для одного дифференциального оператора на оси в пространствах мультипликаторов. | 40 |
| A.S. Kabdulova Analysis of p-q-sub - Laplacians on Stratified Lie groups | 42 |

| | |
|---|-----------|
| A.A. Kalybay, R. Oinarov Boundedness of Riemann - Liouville operator from weighted Sobolev space to weighted Lebesgue space | 44 |
| A. Kassymov Hardy - Littlewood - Sobolev and Stein - Weiss inequalities on homogeneous Lie groups | 45 |
| Л.К. Кусаинова, А.А. Шкалик, Г. Мурат О мультипликаторах в весовых пространствах потенциалов. приложения. | 46 |
| К.Т. Мунбаев, С.В. Martins Filho Inversion theorems for Fourier transforms | 47 |
| А.Б. Муқанов Преобразование Фурье и классы Липшица | 48 |
| Zh. Mukeyeva, E.D. Nursultanov On the interpolation properties of the integral operator in anisotropic spaces | 50 |
| G.K. Mussabayeva, N.T. Tleukhanova, K. Sadykova Hardy - Littlewood theorem for anisotropic Lorentz spaces | 51 |
| Y.D. Nursultanov The Marcinkiewicz - Calderon type interpolation theorems | 52 |
| Е.Д. Нурсултанов, А.Н. Баширова Теорема Харди - Литтлвуда для кратных рядов Фурье - Хаара | 52 |
| В.К. Omarbayeva Weighted estimate of a class of quasilinear discrete operators | 53 |
| M. Raikhan, A.E. Uatayeva Stein - Weiss type interpolation theorem of Haagerup noncommutative Hardy spaces associated with subdiagonal algebra | 55 |
| M.A. Ragusa Actual problems related to some minimizers of functionals | 56 |
| B. Sabitbek, D. Suragan Geometric hardy inequalities on starshaped sets | 57 |
| Б.Н. Сейлбеков компактность оператора дробного интегрирования с переменным верхним пределом | 58 |
| A. Senouci Hardy type inequality with sharp constant for $0 < p < 1$ | 59 |
| D. Suragan Recent progress in the theory of subelliptic Hardy type inequalities | 60 |
| F. Sukochev, K. Tulenov, D. Zanin The boundedness of the Hilbert transform in Lorentz spaces and its applications | 60 |
| D.B. Shilibekova Uncertainty type principles | 61 |
| M.U. Yakhshiboev On a class of non-convolution operators | 62 |
| Дифференциальные уравнения и уравнения математической физики | 64 |
| Т.М. Алдибеков, М.М. Алдажарова Об асимптотической устойчивости нулевого решения нелинейной системы дифференциальных уравнений | 65 |
| М. Алдай, К.Р. Мырзатаева, Д.С. Каратаева Условие осцилляторности и неосцилляторности полулинейного дифференциального уравнения второго порядка | 66 |
| С.Е. Айтжанов, Г.Р. Ашурова Поведение решения обратной задачи для псевдопараболического уравнения с p -Лапласианом | 67 |
| С.Е. Айтжанов, Г.О. Жумагул Разрешимость псевдопараболического уравнения с нелинейными краевыми условиями | 68 |
| С.Е. Айтжанов, Д.Т. Жанузакова Разрушение решений обратной задачи для параболического уравнения со степенной нелинейностью | 69 |
| Н. Аканбай, Э.И. Сулейменова, С.К. Тапеева Об эволюции магнитного поля в марковской модели Хаббла | 70 |
| А. Айжан, М.Б. Жасыбаева, К.Р. Есмаханова представление лакса бездисперсионного $(2+1)$ -мерного уравнения фокаса-ленэллса | 72 |
| К.С. Алыбаев, Т.К. Нарымбетов Аналитические функции комплексного аргумента с параметром | 74 |
| К. Алымкулов, К.Г. Кожобеков Новый подход к построению асимптотики решения уравнения Бесселя для больших значений комплексного аргумента | 75 |

| | |
|---|-----|
| А.Т. Асанова, Н.Т. Орумбаева, А.Б. Кельдибекова Об одном приближенном решении периодической раевой задачи для дифференциального уравнения третьего порядка | 77 |
| M.U. Akhmet, M. Feçkan, M.O. Fen, A. Kashkynbayev Perturbed li-yorke homoclinic chaos | 79 |
| А.Т. Assanova, Z.S. Tokmurzin Parameter identification in an initial-boundary value problem for hyperbolic equation of the fourth order | 80 |
| А.С. Бердышев, Н. Адил О непустоте спектра задачи с условиями Бицадзе - Самарского для смешанного парабола-гиперболического уравнения | 81 |
| Е.А. Bakirova, А.Т. Assanova Control problem for parabolic integro-differential equation with parameter | 82 |
| B. N. Biyarov, D. A. Svistunov, G. K. Abdrasheva Correct singular perturbations of the Laplace operator | 84 |
| М.В. Borikhanov Local existence and global non-existence for the integro-differential diffusion equation | 85 |
| А.Т. Bountis Stable and chaotic dynamics in hamiltonian systems applications to one - dimensional lattices | 86 |
| Н. Begehr, S. Burgumbayeva, A. Dauletkulova, Н. Lin, B. Shupeyeva Polyanalytic Schwarz problem and the Almaty apple | 87 |
| М.Т. Дженалиев, М.И. Рамазанов, А.О. Танин Крещению псевдо - Вольтеррового интегрального уравнения задачи Солонникова - Фазано | 89 |
| D.S. Dzhumabaev, S.T. Mynbayeva New general solution to a nonlinear Fredholm integro-differential equation | 90 |
| М.Т. Jenaliyev, М.И. Ramazanov, M.G. Yergaliyev On the coefficient inverse problems of heat conduction in a degenerating domains | 92 |
| Ж.Б. Ескабылова, К.Н. Оспанов, Т.Н. Бекжан О существовании и гладкости решения квазилинейного дифференциального уравнения третьего порядка с доминирующим промежуточным членом | 94 |
| A. Yesbayev Correct solvability of second-order differential equations with unbounded coefficients | 95 |
| S.S. Zhumatov On a stability of a program manifold of control systems with variable coefficients with stationary nonlinearity | 97 |
| A.Kh. Zhumagazyev, Zh.A. Sartabanov, G.A. Abdikalikova Multiperiodic solution of one hyperbolic system | 99 |
| Н.С. Иманбаев К спектральному вопросу оператора Коши-Римана | 102 |
| Т. Ш. Кальменов, А.К. Лес Определение плотности эллиптического потенциала | 103 |
| С.А. Кассабек, А.А. Кавокин, Ю.Р. Шпади, Д.С. Кулахметова Асимптотическое представление решения двухфазной задачи Стефана с областью, вырождающейся в начальный момент времени | 103 |
| М.Т. Космакова, Ж.М. Тулеутаева, Л.Ж. Касымова Об одном неоднородном интегральном уравнении | 105 |
| М.Д. Кошанова, М.А. Муратбекова, Б.Х. Турметов Об одной краевой задаче для нелокального уравнения Пуассона | 107 |
| Б.Д. Кошанов, Ж.Б. Султангазиева, А.Н. Емир Кадыоглы О собственных числах краевой задачи для квазигиперболического уравнения высокого порядка | 110 |
| Л.К. Кусаинова, Б.С. Кошкарова О некоторых качественных характеристиках одномерных операторов с комплексными переменными коэффициентами | 111 |
| А.А. Калыбай, Д.С. Каратаева Сопряженные и несопряженные свойства полупериодического уравнения второго порядка | 113 |

| | |
|---|-----|
| A.A. Kulzhumiyeva, Zh.A. Sartabanov Multiperiodic solutions of a semi-linear D_c -equation | 115 |
| М. Рамазанов, А. Сейтмуратов, Н. Медеубаев, Г. Мукеева Определения частот собственных колебаний методом декомпозиции | 117 |
| Ж.Р. Мырзакулова Калибровочная эквивалентность между Γ -спиновой системой и нелинейным уравнением Шредингера | 119 |
| М.Б. Муратбеков, Е.Н. Баяндиев Существование и максимальная регулярность решений | 120 |
| М.В. Muratbekov, М.М. Muratbekov Maximal regularity and two-sided estimates for the approximation numbers of solutions of the nonlinear Sturm-Liouville equation with rapidly oscillating coefficients in $L_2(r)$ | 122 |
| А.Р. Мырзақұл, Г.Н. Нугманова Об эквивалентности системы манакова и обобщенного уравнения Ландау - Лифшица | 124 |
| К.Н. Оспанов, Р.Д. Ахметкалиева Об эллиптической системе второго порядка с неограниченными промежуточными коэффициентами | 125 |
| М.Н. Оспанов О свойствах решения псевдопараболического уравнения третьего порядка в бесконечной области | 127 |
| М. Отелбаев, Б.Д. Кошанов Задачи управления точечным источником тепла . | 128 |
| G. Oralsyn Trace formula for the poisson potential for the time-fractional heat equation | 131 |
| Zh.A. Sartabanov, G.M. Aitenova, G.A. Abdikalikova Multiperiodic solutions of quasilinear systems of integro-differential equations with D_c operator and ϵ -hereditary period | 133 |
| Zh.A. Sartabanov, B.Zh. Omarova Research of multiperiodic solutions of perturbed nonlinear autonomous systems with differentiation operator on the vector field . . | 135 |
| A.A. Сарсенби Базисность системы собственных функций дифференциального оператора второго порядка с инволюцией | 137 |
| А.М. Сарсенби, М. Утелбаева Разрешимость смешанной задачи для возмущенного волнового уравнения с инволюцией | 139 |
| М.А. Sadybekov, N. Kakharman Riesz basis of root functions of periodic Sturm - Liouville problem with symmetric potential | 140 |
| М.А. Sadybekov, А.А. Dukenbayeva Laplace operator with nonlocal Samarskii - Ionkin type boundary conditions in a disk | 141 |
| Y.T. Sultanaev, N.F. Valeev E.A. Nairova, Spectral properties of differential operators with oscillating coefficients | 143 |
| К.Б. Тампагаров Погранслойные линии в теории сингулярно возмущенных уравнений второго порядка с аналитическими функциями | 145 |
| Д.А. Турсунов, М.О. Орозов Асимптотика решения задачи Дирихле для кольца с негладким коэффициентом | 147 |
| Zh.N. Tasmambetov, Zh.K. Ubayeva Design of heterogeneous systems solution of differential equation in partial derivative of third order hypergeometric type | 149 |
| Zh.N. Tasmambetov, А.А. Issenova Properties of related systems solutions with whittaker type system | 151 |
| А.В. Tleulessova On the solvability of a nonlinear periodic boundary value problem for an ode system with impulse actions | 153 |
| Б.Х. Турметов, К.И. Усманов Об одном обобщении задачи Робена для уравнения Лапласа | 155 |
| Д.А. Турсунов, З.М. Сулайманов Асимптотика решения одной сингулярно возмущенной задачи с внутренним слоем | 156 |

| | |
|---|------------|
| M.I. Tleubergenov, G.I. Ibraeva On the closure of stochastic differential equations of motion | 159 |
| Ye.M. Khairullin, G.A. Tulesheva, A.S. Azhibekova A multidimensional boundary value problem of heat and mass transfer, when the boundary conditions contain higher-order derivatives | 161 |
| S.N. Kharin Mathematical models of variuos forms of erosion in opening electrical contacts | 162 |
| S. Shaimardan, N.S. Tokmagambetov The Bessel equation in h-discrete calculus . | 164 |
| Т.Ж. Шугаева, И.Ф. Спивак-Лавров, Т.С. Калиматов Решение задачи Дирихле для уравнения Лапласа для трансаксиальных и осесимметричных систем | 166 |
| Алгебра және модельдер теориясы | 167 |
| A.V. Altayeva, B.Sh. Kulpeshov On almost omega-categoricity for quite o-minimal theories | 168 |
| Е.Р. Байсалов, У. Дауыл О линейно минимальных квадратичных йордановых алгебрах | 170 |
| Е.Р. Байсалов, У. Дауыл О линейных трехэтапных протоколах | 171 |
| T.P. Gou On recurrent formulas for third-order horadam numbers | 172 |
| А.Р.Ешкеев, М.Т. Омарова, Г.А. Уркен Подобия центральных типов наследственных теорий | 174 |
| А.Р. Ешкеев Г.Е. Жумабекова, Н.М. Мусина Свойства категоричности и стабильности гибридов для наследственных теорий | 175 |
| А.Р. Ешкеев, А.К. Исаева, Н.М. Мусина Свойства атомности модели для гибрида замыканий атомных множеств | 176 |
| A.S. Iskakova The remark about modified chi-square estimation for polynomial distribution | 177 |
| М.Т. Kassymetova Totally categorical universal classes of the robinson spectrum . . | 179 |
| М. Manat Ocomputable numberings in the Ershov hierarchy | 180 |
| А.Т. Нуртазин Экзистенциально замкнутые Абелевы группы | 180 |
| О.И. Ульбрихт Йонсоновская совершенность j -категоричного модуля | 182 |

О ЛИНЕЙНЫХ ТРЕХЭТАПНЫХ ПРОТОКОЛАХ

Е.Р. Байсалов, У. Дауыл

ЕНУ им. Л.Н. Гумилева, Нур-Султан, Казахстан

E-mail: baisalov_yer@mail.enu.kz

Криптографические протоколы, основанные на линейных функциях, не обладают достаточной стойкостью к атакам. В [1] приведен обширный список таких протоколов, взлом которых возможен методом линейного разложения, подробно описанного впервые В.А. Романьковым.

В своем докладе мы хотим рассказать об аналогичной слабости трехэтапных протоколов [2], основанных на линейных преобразованиях. Сначала напомним упрощенное определение трехэтапного протокола. Платформой для такого протокола может послужить некоторое множество M , в группе перестановок S_M которого выбираются два коммутирующих множества A и B . Возможные сообщения, которые Алиса хочет отправить Бобу, закодированы с помощью элементов M , поэтому, для простоты изложения, M можно рассматривать как множество возможных сообщений. Допустим, Алиса хочет отправить Бобу сообщение $x \in M$. Тогда для этого поочередно осуществляются три следующих шага протокола:

1. Алиса выбирает случайно $a \in A$, вычисляет $a(x) = y$ и отправляет y Бобу.
2. Боб выбирает случайно $b \in B$, вычисляет $b(y) = z$ и возвращает z Алисе.
3. Алиса вычисляет $a^{-1}(z) = w$ и возвращает w Бобу.

Поскольку A и B коммутируют, нетрудно видеть, что $w = a^{-1}ba(x) = a^{-1}ab(x) = b(x)$. Поэтому, применив к w перестановку b^{-1} , Боб получит желанное сообщение x .

Задача криптоаналитика состоит в восстановлении x по данным $a(x)$, $ba(x)$ и $b(x)$. Она может стать вполне разрешимой, если M — подмножество конечномерного векторного пространства, а A и B — множества обратимых линейных преобразований. Достаточно найти (любое) решение уравнения $f(y) = z$ в B : действительно, если f — решение этого уравнения, то $f^{-1}(w) = x$.

Пример 1 Пусть M — множество всех $n \times n$ -матриц над некоторым вычислимым полем, A (B) состоит из линейных преобразований пространства M , полученных с помощью умножения слева (справа) на невырожденную $n \times n$ -матрицу. Известно, что в этом случае невырожденное решение уравнения $f(y) = z$ находится за полиномиальное время с помощью метода Гаусса.

Список литературы

- [1] В.А. Романьков, *Алгебраическая криптография*. Издательство ОГУ им. Ф.М. Достоевского, Омск (2013).
- [2] Сайт: https://ru.wikipedia.org/wiki/Трёхэтапный_протокол.