ISSN: 2224-5227 (Print)
ISSN: 2518-1483 (Online)

ACADEMIC SCIENTIFIC JOURNAL OF COMPUTER SCIENCE

№4
2025

ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

CENTRAL ASIAN ACADEMIC
RESEARCH CENTER

ACADEMIC SCIENTIFIC JOURNAL OF COMPUTER SCIENCE

4 (356)

OCTOBER – DECEMBER 2025

PUBLISHED SINCE JANUARY 1963
PUBLISHED 4 TIMES A YEAR

ALMATY, NAS RK

CHIEF EDITOR:

MUTANOV Galimkair Mutanovich, doctor of technical sciences, professor, academician of NAS RK, acting General Director of the Institute of Information and Computing Technologies CS MES RK (Almaty, Kazakhstan), https://www.scopus.com/authid/detail.uri?authorId=6506682964, https://www.webofscience.com/wos/author/record/1423665

EDITORIAL BOARD:

KALIMOLDAYEV Maksat Nuradilovich, (Deputy Editor-in-Chief), Doctor of Physical and Mathematical Sciences, Professor, Academician of NAS RK, Advisor to the General Director of the Institute of Information and Computing Technologies of the CS MES RK, Head of the Laboratory (Almaty, Kazakhstan), https://www.scopus.com/authid/detail.uri?authorId=56153126500, https://www.webofscience.com/wos/author/record/2428551

MAMYRBAEV Orken Zhumazhanovich, (Academic Secretary), PhD in Information Systems, Deputy Director for Science of the Institute of Information and Computing Technologies CS MES RK (Almaty, Kazakhstan), https://www.scopus.com/authid/detail.uri?authorId=55967630400, https://www.webofscience.com/wos/author/record/1774027

BAIGUNCHEKOV Zhumadil Zhanabaevich, Doctor of Technical Sciences, Professor, Academician of NAS RK, Institute of Cybernetics and Information Technologies, Department of Applied Mechanics and Engineering Graphics, Satbayev University (Almaty, Kazakhstan), https://www.scopus.com/authid/detail.uri?authorId=6506823633, https://www.webofscience.com/wos/author/record/1923423

WOICIK Waldemar, Doctor of Technical Sciences (Phys.-Math.), Professor of the Lublin University of Technology (Lublin, Poland), https://www.scopus.com/authid/detail.uri?authorId=7005121594, https://www.webofscience.com/wos/author/record/678586

SMOLARJ Andrej, Associate Professor Faculty of Electronics, Lublin polytechnic university (Lublin, Poland), https://www.scopus.com/authid/detail.uri?authorId=56249263000, https://www.webofscience.com/wos/author/record/1268523

KEILAN Alimkhan, Doctor of Technical Sciences, Professor (Doctor of science (Japan)), chief researcher of Institute of Information and Computational Technologies CS MES RK (Almaty, Kazakhstan), https://www.scopus.com/authid/detail.uri?authorId=8701101900, https://www.webofscience.com/wos/author/record/1436451

KHAIROVA Nina, Doctor of Technical Sciences, Professor, Chief Researcher of the Institute of Information and Computational Technologies CS MES RK (Almaty, Kazakhstan), https://www.scopus.com/authid/detail.uri?authorId=37461441200, https://www.webofscience.com/wos/author/record/1768515

OTMAN Mohamed, PhD, Professor of Computer Science Department of Communication Technology and Networks, Putra University Malaysia (Selangor, Malaysia), https://www.scopus.com/authid/detail.uri?authorId=56036884700, https://www.webofscience.com/wos/author/record/747649

NYSANBAYEVA Saule Yerkebulanovna, Doctor of Technical Sciences, Associate Professor, Senior Researcher of the Institute of Information and Computing Technologies CS MES RK (Almaty, Kazakhstan), https://www.scopus.com/authid/detail.uri?authorId=55453992600, https://www.webofscience.com/wos/author/record/3802041

BIYASHEV Rustam Gakashevich, doctor of technical sciences, professor, Deputy Director of the Institute for Informatics and Management Problems, Head of the Information Security Laboratory (Kazakhstan), https://www.scopus.com/authid/detail.uri?authorId=6603642864, https://www.webofscience.com/wos/author/record/3802016

KAPALOVA Nursulu Aldazharovna, Candidate of Technical Sciences, Head of the Laboratory cybersecurity, Institute of Information and Computing Technologies CS MES RK (Almaty, Kazakhstan), https://www.scopus.com/authid/detail.uri?authorId=57191242124,

KOVALYOV Alexander Mikhailovich, Doctor of Physical and Mathematical Sciences, Academician of the National Academy of Sciences of Ukraine, Institute of Applied Mathematics and Mechanics (Donetsk, Ukraine), https://www.scopus.com/authid/detail.uri?authorId=7202799321, https://www.webofscience.com/wos/author/record/38481396

MIKHALEVICH Alexander Alexandrovich, Doctor of Technical Sciences, Professor, Academician of the National Academy of Sciences of Belarus (Minsk, Belarus), https://www.scopus.com/authid/detail.uri?authorId=7004159952, https://www.webofscience.com/wos/author/record/46249977

TIGHINEANU Ion Mihailovich, Doctor of Physical and Mathematical Sciences, Academician, President of the Academy of Sciences of Moldova, Technical University of Moldova (Chisinau, Moldova), https://www.scopus.com/authid/detail.uri?authorId=7006315935, https://www.webofscience.com/wos/author/record/524462

Academic Scientific Journal of Computer Science
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

Owner: «Central Asian Academic Research Center» LLP (Almaty).

Certificate **№ KZ77VPY00121154** on the re-registration of the periodical printed and online publication of the information agency, issued on **05.06.2025** by the Republican State Institution «Information Committee» of the Ministry of Culture and Information of the Republic of Kazakhstan

Subject area*: information and communication technologies.*

Currently: *included in the list of journals recommended by the CCSES MSHE RK in the direction of «Information and communication technologies».*

Periodicity: *4 times a year.*

http://www.physico-mathematical.kz/index.php/en/

© «Central Asian Academic Research Center» LLP, 2025

БАС РЕДАКТОР:

МҰТАНОВ Ғалымқайыр Мұтанұлы, техника ғылымдарының докторы, профессор, ҚР ҰҒА академигі, ҚР ҒЖБМ ҒК «Ақпараттық және есептеу технологиялары институты» бас директорының м.а. (Алматы, Қазақстан), https://www.scopus.com/authid/detail.uri?authorId=6506682964, https://www.webofscience.com/wos/author/record/1423665

РЕДАКЦИЯ АЛҚАСЫ:

ҚАЛИМОЛДАЕВ Мақсат Нұрәділұлы, (бас редактордың орынбасары), физика-математика ғылымдарының докторы, профессор, ҚР ҰҒА академигі, ҚР ҒЖБМ ҒК «Ақпараттық және есептеу технологиялары институты» бас директорының кеңесшісі, зертхана меңгерушісі (Алматы, Қазақстан), https://www.scopus.com/authid/detail.uri?authorId=56153126500, https://www.webofscience.com/wos/author/record/2428551

МАМЫРБАЕВ Өркен Жұмажанұлы (ғалым хатшы), Ақпараттық жүйелер саласындағы техника ғылымдарының (PhD) докторы, ҚР ҒЖБМ ҒК «Ақпараттық және есептеу технологиялары институты» директорының ғылым жөніндегі орынбасары (Алматы, Қазақстан), https://www.scopus.com/authid/detail.uri?authorId=55967630400, https://www.webofscience.com/wos/author/record/1774027

БАЙГУНЧЕКОВ Жұмаділ Жаңабайұлы, техника ғылымдарының докторы, профессор, ҚР ҰҒА академигі, Кибернетика және ақпараттық технологиялар институты, Қолданбалы механика және инженерлік графика кафедрасы, Сәтбаев университеті (Алматы, Қазақстан), https://www.scopus.com/authid/detail.uri?authorId=6506823633, https://www.webofscience.com/wos/author/record/1923423

ВОЙЧИК Вальдемар, техника ғылымдарының докторы (физ-мат), Люблин технологиялық университетінің профессоры (Люблин, Польша), https://www.scopus.com/authid/detail.uri?authorId=7005121594, https://www.webofscience.com/wos/author/record/678586

СМОЛАРЖ Анджей, Люблин политехникалық университетінің электроника факультетінің доценті (Люблин, Польша), https://www.scopus.com/authid/detail.uri?authorId=56249263000, https://www.webofscience.com/wos/author/record/1268523

КЕЙЛАН Әлімхан, техника ғылымдарының докторы, профессор (ғылым докторы (Жапония)), ҚР ҒЖБМ ҒК «Ақпараттық және есептеу технологиялары институтының» бас ғылыми қызметкері (Алматы, Қазақстан), https://www.scopus.com/authid/detail.uri?authorId=8701101900, https://www.webofscience.com/wos/author/record/1436451

ХАЙРОВА Нина, техника ғылымдарының докторы, профессор, ҚР ҒЖБМ ҒК «Ақпараттық және есептеу технологиялары институтының» бас ғылыми қызметкері (Алматы, Қазақстан), https://www.scopus.com/authid/detail.uri?authorId=37461441200, https://www.webofscience.com/wos/author/record/1768515

ОТМАН Мохаммед, PhD, Информатика, Коммуникациялық технологиялар және желілер кафедрасының профессоры, Путра университеті Малайзия (Селангор, Малайзия), https://www.scopus.com/authid/detail.uri?authorId=56036884700, https://www.webofscience.com/wos/author/record/747649

НЫСАНБАЕВА Сауле Еркебұланқызы, техника ғылымдарының докторы, доцент, ҚР ҒЖБМ ҒК «Ақпараттық және есептеу технологиялары институтының» аға ғылыми қызметкері (Алматы, Қазақстан), https://www.scopus.com/authid/detail.uri?authorId=55453992600, https://www.webofscience.com/wos/author/record/3802041

БИЯШЕВ Рустам Гакашевич, техника ғылымдарының докторы, профессор, Информатика және басқару мәселелері институты директорының орынбасары, Ақпараттық қауіпсіздік зертханасының меңгерушісі (Қазақстан), https://www.scopus.com/authid/detail.uri?authorId=6603642864, https://www.webofscience.com/wos/author/record/3802016

КАПАЛОВА Нұрсұлу Алдажарқызы, техника ғылымдарының кандидаты, ҚР ҒЖБМ ҒК «Ақпараттық және есептеу технологиялары институты», Киберқауіпсіздік зертханасының меңгерушісі (Алматы, Қазақстан), https://www.scopus.com/authid/detail.uri?authorId=57191242124,

КОВАЛЕВ Александр Михайлович, физика-математика ғылымдарының докторы, Украина Ұлттық Ғылым академиясының академигі, Қолданбалы математика және механика институты (Донецк, Украина), https://www.scopus.com/authid/detail.uri?authorId=7202799321, https://www.webofscience.com/wos/author/record/38481396

МИХАЛЕВИЧ Александр Александрович, техника ғылымдарының докторы, профессор, Беларусь Ұлттық Ғылым академиясының академигі (Минск, Беларусь), https://www.scopus.com/authid/detail.uri?authorId=7004159952, https://www.webofscience.com/wos/author/record/46249977

ТИГИНЯНУ Ион Михайлович, физика-математика ғылымдарының докторы, академик, Молдова Ғылым Академиясының президенті, Молдова техникалық университеті (Кишинев, Молдова), https://www.scopus.com/authid/detail.uri?authorId=7006315935, https://www.webofscience.com/wos/author/record/524462

Academic Scientific Journal of Computer Science
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

Меншіктеуші: «Орталық Азия академиялық ғылыми орталығы» ЖШС (Алматы).

Ақпарат агенттігінің мерзімді баспасөз басылымын, ақпарат агенттігін және желілік басылымды қайта есепке қою туралы ҚР Мәдениет және Ақпарат министрлігі «Ақпарат комитеті» Республикалық мемлекеттік мекемесі **05.06.2025** ж. берген **№ KZ77VPY00121154** Куәлік.

Тақырыптық бағыты: *ақпараттық-коммуникациялық технологиялар*

Қазіргі уақытта: *«ақпараттық-коммуникациялық технологиялар» бағыты бойынша ҚР БҒМ БҒСБК ұсынған журналдар тізіміне енді.*

Мерзімділігі: *жылына 4 рет.*

http://www.physico-mathematical.kz/index.php/en/

© «Орталық Азия академиялық ғылыми орталығы» ЖШС, 2025

ГЛАВНЫЙ РЕДАКТОР:

МУТАНОВ Галимкаир Мутанович, доктор технических наук, профессор, академик НАН РК, и.о. генерального директора «Института информационных и вычислительных технологий» КН МНВО РК (Алматы, Казахстан), https://www.scopus.com/authid/detail.uri?authorId=6506682964, https://www.webofscience.com/wos/author/record/142 3665

Редакционная коллегия:

КАЛИМОЛДАЕВ Максат Нурадилович, (заместитель главного редактора), доктор физико-математических наук, профессор, академик НАН РК, советник генерального директора «Института информационных и вычислительных технологий» КН МНВО РК, заведующий лабораторией (Алматы, Казахстан), https://www.scopus.com/authid/detail.uri?authorId=56153126500, https://www.webofscience.com/wos/author/record/2428551

МАМЫРБАЕВ Оркен Жумажанович, (ученый секретарь), доктор философии (PhD) по специальности «Информационные системы», заместитель директора по науке РГП «Институт информационных и вычислительных технологий» Комитета науки МНВО РК (Алматы, Казахстан), https://www.scopus.com/authid/detail.uri?authorId=55967630400, https://www.webofscience.com/wos/author/record/1774027

БАЙГУНЧЕКОВ Жумадил Жанабаевич, доктор технических наук, профессор, академик НАН РК, Институт кибернетики и информационных технологий, кафедра прикладной механики и инженерной графики, Университет Сатпаева (Алматы, Казахстан), https://www.scopus.com/authid/detail.uri?authorId=6506823633, https://www.webofscience.com/wos/author/record/1923423

ВОЙЧИК Вальдемар, доктор технических наук (физ.-мат.), профессор Люблинского технологического университета (Люблин, Польша), https://www.scopus.com/authid/detail.uri?authorId=7005121594, https://www.webofscience.com/wos/author/record/678586

СМОЛАРЖ Анджей, доцент факультета электроники Люблинского политехнического университета (Люблин, Польша), https://www.scopus.com/authid/detail.uri?authorId=56249263000, https://www.webofscience.com/wos/author/record/1268523

КЕЙЛАН Алимхан, доктор технических наук, профессор (Doctor of science (Japan)), главный научный сотрудник РГП «Института информационных и вычислительных технологий» КН МНВО РК (Алматы, Казахстан), https://www.scopus.com/authid/detail.uri?authorId=8701101900, https://www.webofscience.com/wos/author/record/1436451

ХАЙРОВА Нина, доктор технических наук, профессор, главный научный сотрудник РГП «Института информационных и вычислительных технологий» КН МНВО РК (Алматы, Казахстан), https://www.scopus.com/authid/detail.uri?authorId=37461441200, https://www.webofscience.com/wos/author/record/1768515

ОТМАН Мохамед, доктор философии, профессор компьютерных наук, Департамент коммуникационных технологий и сетей, Университет Путра Малайзия (Селангор, Малайзия), https://www.scopus.com/authid/detail.uri?authorId=56036884700, https://www.webofscience.com/wos/author/record/747649

НЫСАНБАЕВА Сауле Еркебулановна, доктор технических наук, доцент, старший научный сотрудник РГП «Института информационных и вычислительных технологий» КН МНВО РК (Алматы, Казахстан), https://www.scopus.com/authid/detail.uri?authorId=55453992600, https://www.webofscience.com/wos/author/record/3802041

БИЯШЕВ Рустам Гакашевич, доктор технических наук, профессор, заместитель директора Института проблем информатики и управления, заведующий лабораторией информационной безопасности (Казахстан), https://www.scopus.com/authid/detail.uri?authorId=6603642864,https://www.webofscience.com/wos/author/record/3802016

КАПАЛОВА Нурсулу Алдажаровна, кандидат технических наук, заведующий лабораторией кибербезопасности РГП «Института информационных и вычислительных технологий» КН МНВО РК (Алматы, Казахстан), https://www.scopus.com/authid/detail.uri?authorId=57191242124,

КОВАЛЕВ Александр Михайлович, доктор физико-математических наук, академик НАН Украины, Институт прикладной математики и механики (Донецк, Украина), https://www.scopus.com/authid/detail.uri?authorId=7202799321, https://www.webofscience.com/wos/author/record/38481396

МИХАЛЕВИЧ Александр Александрович, доктор технических наук, профессор, академик НАН Беларуси (Минск, Беларусь), https://www.scopus.com/authid/detail.uri?authorId=7004159952, https://www.webofscience.com/wos/author/record/46249977

ТИГИНЯНУ Ион Михайлович, доктор физико-математических наук, академик, президент Академии наук Молдовы, Технический университет Молдовы (Кишинев, Молдова), https://www.scopus.com/authid/detail.uri?authorId=7006315935, https://www.webofscience.com/wos/author/record/524462

Academic Scientific Journal of Computer Science
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

Собственник: *ТОО «Центрально-азиатский академический научный центр» (г. Алматы).*

Свидетельство о постановке на переучет периодического печатного издания, информационного агентства и сетевого издания **№ KZ77VPY00121154.** Дата выдачи **05.06.2025**

Тематическая направленность: *информационно-коммуникационные технологии.*

В настоящее время: *вошел в список журналов, рекомендованных КОКСНВО МНВО РК по направлению «информационно-коммуникационные технологии».*

Периодичность: *4 раза в год.*

http://www.physico-mathematical.kz/index.php/en/

© ТОО «Центрально-азиатский академический научный центр», 2025

CONTENTS

B. Assanova, Zh. Moldasheva, A.T. Kishubaeva
Decision support system structure and blocks for selecting efficient delayed coking modes.....11

Zh.T. Abildayeva, R.K. Uskenbayeva, G.S. Beketova, N.B. Konyrbaev, S.B. Seydazimov
Multi-criterion optimization of advertising budget allocation in the agro-industrial complex based on NSGA-III algorithm.....26

A.O. Aliyeva, B.S. Omarov, R.B. Abdrakhmanov, D.R. Sultan, A.B. Toktarova
Neural network model for automatic detection of Kazakh-language hate speech.....40

O. Auyelbekov, E. Bostanov, S. Sapakova, L. Tukenova, A. Kozhagul
Modeling and analysis of a generator with permanent and variable magnets.....55

G. Autova, G. Nurtayeva, E. Zulbukharova, G. Yeleussizova, R. Zhumabekova
Theoretical foundations of interdisciplinary integration of physics and computer science.....73

A.Zh. Akhmetova, M.A. Kantureyeva, A.A. Abisheva, A. Aubakirova, A.A. Shekerbek
Analysis of the social network user's enviroment.....89

A.Sh. Barakova, K.S. Shadinova, A.S. Orynbaeva, G. Sugurzhanova
Design of a model for protecting a website's authentication data and content based on blockchain technology.....102

A.N. Zhidebayeva, G.U. Madaliyeva, B.O. Tastanbekova, S.S. Karzhaubekova, G.S. Shaimerdenova
Deep neural network Conv-LSTM for ECG-based cardiac disorder identification.....122

N.M. Zhunissov, A.B. Aben, A.B. Amanzholova
The fraud detection model in text messages.....138

A. Issakhov, A. Alzhanov, A. Akhmedov, A. Amanzholov, T. Murat
Numerical simulation of thermohydrodynamics during heated water discharge into Lake Balkhash.....152

Z. Kaderkeyeva, B. Razakhova, G. Bekmanova, A. Nazyrova, M. Zhasuzakova
Q-Bilim: an intelligent system for assessing learning outcomes based on competencies.....171

N. Karymsakova, A. Boltaboyeva, D. Turmakhanbet, M. Maulenbekov, T. Abdirova
Unsupervised learning for the identification of critical conditions in renewable energy production.....184

A.Kulakayeva, E.Daineko, B. Medetov, A. Nurlankyzy
Evaluation of the effectiveness of modern neural network architectures for VAD under low snr ratio conditions.....203

B. Orazbayev, A. Zhumadillayeva, K. Orazbayeva, R. Yessirkessinov, Zh. Tuleuov
Development of models of sulfur production processes based on artificial neural networks and simulation.....216

L. Rzayeva, A. Ryzhova, M. Zhaparkhanova, A. Myrzatay, Zh. Kozhakhmet
A new LSTM-based web application for automated password strength evaluation.....234

D. Sagidoldin, A. Zhetpisbayeva, B. Zhumazhanov, B. Zhumazhanov
Increasing the reliability of data transmission from small spacecraft using SDR equipment.....259

A.N. Seraly, A.D. Mekhtiyev, G.Z. Ziyatbekova, K.B. Begalieva, R.A. Mekhtiyev
Development of hardware for monitoring optical parameters.....274

A.A. Taurbekova, M.V. Markosyan
Development and implementation of a computational model of magmatic processes in the bowls of the Earth and on its surface.....288

K. Chezhimbayeva, A. Mukhamejanova, Y. Garmashova
Fuzzy-logic-based expert system for predicting QoS in 5G networks.....306

МАЗМҰНЫ

Б.У. Асанова, Ж.Ж. Молдашева, А. Кишубаева
Баяу кокстеу қондырғысы үшін тиімді жұмыс режимдерін таңдауға шешім қолдау жүйесі құрылымы.....11

Ж.Т. Әбілдаева, Р.К. Ускенбаева, Г.С. Бекетова, Н.Б. Қоңырбаев, С.Б. Сейдазимов
NSGA-III алгоритмі негізінде агроөнеркәсіптік кешендегі жарнамалық бюджетті бөлуді көп критериалды оңтайландыру.....26

А.О. Әлиева, Б.С. Омаров, Р.Б. Абдрахманов, Д.Р. Султан, А.Б. Тоқтарова
Қазақ тіліндегі дискриминацияны автоматты анықтауға арналған нейрондық желілік моделі.....40

О. Әуелбеков, Е. Бостанов, С. Сапақова, Л. Түкенова, А. Қожағұл
Тұрақты және айнымалы магниттері бар генераторды модельдеу және талдау.....55

Г.М. Аутова, Г.К. Нуртаева, Э.М. Зульбухарова, Г.С. Елеусизова, Р.Р. Жұмабекова
Физика мен информатика пәндерінің пәнаралық интеграциясының теориялық негіздері.....73

А.Ж. Ахметова, М.А. Кантуреева, А.А. Абишева, А. Аубакирова, А.А. Шекербек
Әлеуметтік желі қолданушыларының ортасын талдау.....89

А.Ш. Баракова, К.С. Шадинова, А.С. Орынбаева, Г. Сугуржанова
Блокчейн технологиясы негізінде веб сайттың аутентификациялық деректері мен өнімін қорғау моделін құрастыру.....102

А.Н. Жидебаева, Г.У. Мадалиева, Б.О. Тастанбекова, С.С. Қаржаубекова, Г.С. Шаймерденова
Жүрек ауруларын анықтауда Conv-LSTM архитектурасына негізделген терең нейрондық желі.....122

Н.М. Жунисов, А.Б. Абен, Ә.Б. Аманжолова
Мәтіндік хабарламалардағы алаяқтықты анықтау моделі.....138

А.А. Исахов, А. Альжанов, А. Ахмедов, А. Аманжолов, Т. Мурат
Балқаш көліне жылы су ағызу кезіндегі термогидродинамиканы сандық модельдеу.....152

З.К. Кадеркеева, Б.Ш. Разахова, Г.Т. Бекманова, А.Е. Назырова, М.Ж. Жасұзақова
Q-Bilim: құзыреттерге негізделген оқу нәтижелерін бағалауға арналған интеллектуалды жүйе.....171

Н. Карымсакова, А. Болтабоева, Д. Тұрмаханбет, М. Мауленбеков, Т. Абдирова
Жаңартылатын энергия өндірісіндегі критикалық режимдерді анықтауға арналған мұғалімсіз оқыту.....184

А. Кулакаева, Е. Дайнеко, Б. Медетов, А. Нурланкызы
Сигнал/шуыл қатынасы төмен жағдайларда заманауи нейрондық желілік VAD архитектураларының тиімділігін бағалау.....203

Б. Оразбаев, А. Жумадиллаева, К. Оразбаева, Р. Есиркесинов, Ж. Тулеуов
Күкірт өндіру процесстерінің модельдерін жасанды нейрондық желілер негізінде әзірлеу және модельдеу.....216

Л. Рзаева, А. Рыжова, М. Жапарханова, А. Мырзатай, Ж. Кожахмет,
Құпиясөздің беріктігін автоматты бағалауға арналған LSTM негізіндегі жаңа веб-қосымша.....234

Д.Т. Сагидолдин, А.Т. Жетписбаева, Б.Р. Жумажанов, Б.С. Жумажанов
SDR жабдықтарын пайдалану арқылы, шағын ғарыш аппараттарынан деректерді берудің сенімділігін арттыру.....259

А.Н. Сералы, А.Д. Мехтиев, Г.З. Зиятбекова, К.Б. Бегалиева, Р.А. Мехтиев
Оптикалық параметрлерді бақылауға арналған аппараттық құрылғыны әзірлеу.....274

А.А. Таурбекова, М.В. Маркосян
Жер көзіндегі және оның бетіндегі магматтық процестердің есептік моделін әзірлеу және енгізу.....288

К.С. Чежимбаева, А. Мухамеджанова, Ю. Гармашова
Айқын емес логика негізінде 5G желілеріндегі QoS болжау эксперттік жүйесі.....306

СОДЕРЖАНИЕ

Б.У. Асанова, Ж.Ж. Молдашева, А. Кишубаева
Структура и функциональные блоки системы поддержки решений для выбора режимов замедленного коксования.....11

Ж.Т. Абилдаева, Р.К. Ускенбаева, Г.С. Бекетова, Н.Б. Конырбаев, С.Б. Сейдазимов
Многокритериальная оптимизация распределения рекламного бюджета в апк на основе алгоритма NSGA-III.....26

А.О. Алиева, Б.С. Омаров, Р.Б. Абдрахманов, Д.Р. Султан, А.Б. Токтарова
Нейросетевая модель для автоматического обнаружения дискриминации в казахском языке.....40

О. Ауельбеков, Е. Бостанов, С. Сапакова, Л. Тукенова, А. Кожагул
Моделирование и анализ генератора с постоянными и переменными магнитами.....55

Г.М. Аутова, Г.К. Нуртаева, Э.М. Зульбухарова, Г.С. Елеусизова, Р.Р. Жумабекова
Теоретические основы междисциплинарной интеграции физики и информатики.....73

А.Ж. Ахметова, М.А. Кантуреева, А.А. Абишева, А. Аубакирова, А.А. Шекербек
Анализ окружения ползователей социальной сети.....89

А.Ш. Баракова, К.С. Шадинова, А.С. Орынбаева, Г. Сугуржанова
Разработка модели защиты аутентификационных данных и контента веб-сайта на основе технологии блокчейн.....102

А.Н. Жидебаева, Г.У. Мадалиева, Б.О. Тастанбекова, С.С. Каржаубекова, Г.С. Шаймерденова
Глубокая нейронная сеть на основе архитектуры Conv-LSTM для выявления сердечных заболеваний.....122

Н.М. Жунисов, А.Б. Абен, А.Б. Аманжолова
Модель обнаружения мошенничества в текстовых сообщениях.....138

А.А. Исахов, А. Альжанов, А. Ахмедов, А. Аманжолов, Т. Мурат
Численное моделирование термогидродинамики при сбросе подогретых вод в озеро Балхаш.....152

З.К. Кадеркеева, Б.Ш. Разахова, Г.Т. Бекманова, А.Е. Назырова, М.Ж. Жасузакова
Q-Bilim: интеллектуальная система оценки результатов обучения на основе компетенций.....171

Н. Карымсакова, А. Болтабоева, Д. Тұрмаханбет, М. Мауленбеков, Т. Абдирова
Обучение без учителя для выявления критических режимов в производстве возобновляемой энергии.....184

А. Кулакаева, Е. Дайнеко, Б. Медетов, А. Нурланкызы
Оценка эффективности современных нейросетевых архитектур VAD при низком отношении сигнал/шум.....203

Б. Оразбаев, А. Жумадиллаева, К. Оразбаева, Р. Есиркесинов, Ж. Тулеуов
Разработка моделей процессов производства серы на основе искусственных нейронных сетей и моделирование.....216

Л. Рзаева, А. Рыжова, М. Жапарханова, А. Мырзатай, Ж. Кожахмет
Новое веб-приложение на основе LSTM для автоматизированной оценки надежности паролей.....234

Д.Т. Сагидолдин, А.Т. Жетписбаева, Б.Р. Жумажанов, Б.С. Жумажанов
Повышение надёжности передачи данных с малых космических аппаратов с применением SDR оборудования.....259

А.Н. Сералы, А.Д. Мехтиев, Г.З. Зиятбекова, К.Б. Бегалиева, Р.А. Мехтиев
Разработка аппаратного средства для контроля оптических параметров.....274

А.А. Таурбекова, М.В. Маркосян, Н.Т. Карымсакова
Разработка и реализация вычислительной модели магматических процессов в недрах земли и на её поверхности.....288

К.С. Чежимбаева, А. Мухамеджанова, Ю. Гармашова
Экспертная система прогнозирования QoS в 5G-сетях на основе нечеткой логики.....306

ACADEMIC SCIENTIFIC JOURNAL OF COMPUTER SCIENCE
ISSN 1991-346X
Volume 4. Namber 356 (2025). 138–151

https://doi.org/10.32014/2025.2518-1726.388

ҒТМР 05.13.17
ӘОЖ 004.912:004.056

© N.M. Zhunissov*, A.B. Aben, A.B. Amanzholova, 2025.
Khoja Akhmet Yassawi International Kazakh-Turkish University,
Turkistan, Kazakhstan.
E-mail: nurseit.zhunissov@ayu.edu.kz

THE FRAUD DETECTION MODEL IN TEXT MESSAGES

Zhunissov Nurseit — PhD, Khoja Akhmet Yassawi International Kazakh-Turkish University, Turkestan, Kazakhstan,
E-mail: nurseit.zhunissov@ayu.edu.kz, https://orcid.org/0000-0001-6531-9408;
Aben Arypzhan — Master, Khoja Akhmet Yassawi International Kazakh-Turkish University, Turkestan, Kazakhstan,
E-mail: arypzhan.aben@ayu.edu.kz, https://orcid.org/0000-0001-8534-3288;
Amanzholova Alina — PhD, senior lecturer, Khoja Akhmet Yassawi International Kazakh-Turkish University, Turkestan, Kazakhstan,
E-mail: alina.amanzholova@ayu.edu.kz, https://orcid.org/0000-0003-0370-7645.

Abstract. This article presents a new model for protecting text messages sent via instant messengers from Internet fraud. The increase in the types and volume of fraudulent actions in the modern digital environment makes the issue of ensuring the security of instant messengers, especially in the Republic of Kazakhstan, relevant. During the study, tokenization was performed based on the QazNLTK library and comparative text analysis methods were used. These methods were aimed at testing the ability to identify messages with a risk of fraud. The proposed model is based on an algorithm that identifies dangerous signs in incoming messages. The results of experimental testing showed that the similarity between messages of the same type reached about 75%. For example, sample texts such as "Your message concerns suspicious actions" demonstrate the effectiveness of the model. The values of accuracy (accuracy), recall (recall) and F1-score (F1-score) obtained as a result of the Confusion Matrix clearly demonstrate the ability of the model to work in real conditions. In addition, the analysis of the channels and mechanisms of distribution of fake messages revealed the importance of increasing the digital literacy of citizens. The results of the study showed the need to use expanded datasets, implement machine learning methods, and test in real time to further improve the model. The conclusions and results presented in the article are considered one of the first steps that will serve as the basis for increasing the security of messengers

and creating new defense mechanisms against Internet fraud. Further research in this direction will allow us to deeply understand the dynamics of the creation of fraudulent texts and analyze the evolution of text templates. Also, the development of universal models that include multilingual data will significantly increase the efficiency of the system in the future and expand its scope.

Keywords: messenger, text messages, QazNLTK, machine learning, Internet security

© Н.М. Жунисов*, А.Б. Абен, Ә.Б. Аманжолова, 2025.
Қожа Ахмет Ясауи атындағы Халықаралық қазақ-түрік университеті,
Түркістан, Қазақстан.
*E-mail: nurseit.zhunissov@ayu.edu.kz

МӘТІНДІК ХАБАРЛАМАЛАРДАҒЫ АЛАЯҚТЫҚТЫ АНЫҚТАУ МОДЕЛІ

Жунисов Нурсейт — PhD, аға оқытушы, Қожа Ахмет Ясауи атындағы Халықаралық қазақ-түрік университеті, Түркістан, Қазақстан,
E-mail: nurseit.zhunissov@ayu.edu.kz, https://orcid.org/0000-0001-6531-9408;
Абен Арыпжан — магистр, Қожа Ахмет Ясауи атындағы Халықаралық қазақ-түрік университеті, Түркістан, Қазақстан,
E-mail: arypzhan.aben@ayu.edu.kz, https://orcid.org/0000-0001-8534-3288;
Аманжолова Әлина — PhD, аға оқытушы, Қожа Ахмет Ясауи атындағы Халықаралық қазақ-түрік университеті, Түркістан, Қазақстан,
E-mail: alina.amanzholova@ayu.edu.kz, https://orcid.org/0000-0003-0370-7645.

Аннотация. Бұл мақалада мессенджерлер арқылы таратылатын мәтіндік хабарламаларды интернет-алаяқтықтан қорғаудың жаңа үлгісі ұсынылады. Қазіргі цифрлық ортада алаяқтық әрекеттердің түрлері мен көлемінің артуы, әсіресе Қазақстан Республикасында мессенджерлер қауіпсіздігін қамтамасыз ету мәселесін өзекті етіп отыр. Зерттеу барысында QazNLTK кітапханасы негізінде токенизация жасалып, мәтіндерді салыстырмалы талдау әдістері қолданылды. Бұл тәсілдер алаяқтық қатері бар хабарламаларды анықтау мүмкіндігін тексеруге бағытталды. Ұсынылған үлгі кіріс хабарламалардағы қауіпті белгілерді айқындайтын алгоритмге сүйенеді. Эксперименттік сынақ нәтижелері бір типтегі хабарламалар арасындағы ұқсастық шамамен 75%-ға жеткенін көрсетті. Мысалы, «Сіздің хабарламаңыз күдікті әрекеттерге қатысты» сияқты үлгі мәтіндер модельдің тиімділігін айғақтайды. Confusion Matrix нәтижесінде алынған дұрыстық деңгейі (accuracy), қамту деңгейі (recall) және F1 көрсеткіші (F1-score) мәндері модельдің шынайы жағдайда жұмыс істеу қабілетін нақты көрсетеді. Сонымен қатар, жалған хабарламалардың таралу арналары мен механизмдерін талдау азаматтардың цифрлық сауаттылығын арттырудың маңыздылығын айқындады. Зерттеу нәтижелері модельді одан әрі жетілдіру үшін кеңейтілген деректер жиындарын

пайдалану, машиналық оқыту әдістерін енгізу және нақты уақыт режимінде тестілеу қажеттігін көрсетті. Мақалада баяндалған тұжырымдар мен нәтижелер мессенджерлер қауіпсіздігін арттыруға және интернет-алаяқтыққа қарсы жаңа қорғаныс тетіктерін қалыптастыруға негіз болатын алғашқы қадамдардың бірі ретінде қарастырылады. Бұл бағыттағы әрі қарайғы зерттеулер алаяқтық мәтіндердің жасалу динамикасын терең түсінуге және мәтіндік шаблондардың эволюциясын талдауға мүмкіндік береді. Сондай-ақ, көптілді деректерді қамтитын әмбебап модельдер әзірлеу болашақта жүйенің тиімділігін едәуір арттырып, қолдану аясын кеңейтеді.

Түйін сөздер: мессенджер, мәтіндік хабарламалар, QazNLTK, машиналық оқыту, интернет қауіпсіздігі

© Н.М. Жунисов*, А.Б. Абен, А.Б. Аманжолова, 2025.
Международный казахско-турецкий университет имени Ходжи Ахмеда Ясави, Туркестан, Казакстан.
*E-mail: nurseit.zhunissov@ayu.edu.kz

МОДЕЛЬ ОБНАРУЖЕНИЯ МОШЕННИЧЕСТВА В ТЕКСТОВЫХ СООБЩЕНИЯХ

Жунисов Нурсейт — PhD, старший преподаватель, Международный казахско-турецкий университет имени Ходжи Ахмеда Ясави, Туркестан, Казахстан,
E-mail: nurseit.zhunissov@ayu.edu.kz, https://orcid.org/0000-0001-6531-9408;
Абен Арыпжан — магистр, Международный казахско-турецкий университет имени Ходжи Ахмеда Ясави, Туркестан, Казахстан,
E-mail: arypzhan.aben@ayu.edu.kz, https://orcid.org/0000-0001-8534-3288;
Аманжолова Алина — PhD, старший преподаватель, Международный казахско-турецкий университет имени Ходжи Ахмеда Ясави, Туркестан, Казахстан,
E-mail: alina.amanzholova@ayu.edu.kz, https://orcid.org/0000-0003-0370-7645.

Аннотация. В данной статье представлена новая модель защиты текстовых сообщений, отправляемых через мессенджеры, от интернет-мошенничества. Рост видов и объёмов мошеннических действий в современной цифровой среде актуализирует вопрос обеспечения безопасности мессенджеров, особенно в Республике Казахстан. В ходе исследования проводилась токенизация на основе библиотеки QazNLTK и применялись методы сравнительного анализа текстов. Целью этих методов было тестирование способности выявлять сообщения, содержащие риск мошенничества. Предлагаемая модель основана на алгоритме, выявляющем опасные признаки во входящих сообщениях. Результаты экспериментальной апробации показали, что сходство между сообщениями одного типа достигает около 75%. Например, примеры текстов типа «Ваше сообщение касается подозрительных действий» демонстрируют эффективность модели. Значения точности, полноты и F1-оценки, полученные в результате применения матрицы спутывания, наглядно демонстрируют

работоспособность модели в реальных условиях. Кроме того, анализ каналов и механизмов распространения фейковых сообщений выявил важность повышения цифровой грамотности граждан. Результаты исследования показали необходимость использования расширенных наборов данных, внедрения методов машинного обучения и тестирования в режиме реального времени для дальнейшего совершенствования модели. Выводы и результаты, представленные в статье, рассматриваются как один из первых шагов, которые послужат основой для повышения безопасности мессенджеров и создания новых механизмов защиты от интернет-мошенничества. Дальнейшие исследования в этом направлении позволят глубже понять динамику создания мошеннических текстов и проанализировать эволюцию текстовых шаблонов. Кроме того, разработка универсальных моделей, включающих многоязычные данные, значительно повысит эффективность системы в будущем и расширит область ее применения.

Ключевые слова: мессенджер, текстовые сообщения, QazNLTK, машинное обучение, интернет-безопасность

Кіріспе. Қазіргі кезеңде мессенджерлер арқылы жүзеге асатын интернет-алаяқтық түрлері қарқынды дамып, қоғам үшін маңызды мәселеге айналып отыр. Алаяқтар пайдаланушылардың сеніміне еніп, материалдық немесе моральдық зиян келтіру мақсатында әртүрлі алдау тәсілдерін қолдануда. Соның ішінде WhatsApp платформасында дауыстық хабарламаларды пайдалану арқылы адамның дауысын көшіріп, оның туыстары мен жақындарын алдау жағдайлары жиілеп кеткен. Мұндай хабарламаларда көбіне «ауруханаға түстім» немесе «қаржылық қиындыққа тап болдым» деген мазмұнда қаржылай көмек сұрау жиі кездеседі. Бас прокуратураның деректеріне сәйкес, 2024 жылы Қазақстанда 21 мыңнан астам азамат интернет-алаяқтықтың құрбанына айналған (qazaqstan.tv, 2024).

Қазіргі кезеңдегі интернет-алаяқтық түрлері мен олардың таралу тетіктері қысқаша сипатталады. Авторлар азаматтардың мессенджерлер, жалған сілтемелер, әлеуметтік желілер және мемлекеттік органдар атын жамылған тұлғалар арқылы алдану қаупінің өсіп отырғанын атап өтеді. Сонымен қатар, портал пайдаланушыларға киберқауіпсіздік талаптарын сақтау бойынша нақты кеңестер береді: күмәнді хабарламаларды ашпау, жеке деректерді жарияламау, ақпаратты тек ресми ресурстар арқылы тексеру және алаяқтық белгілері байқалған жағдайда құқық қорғау органдарына жедел хабарлау ұсынылады (eGov.kz., 2024).

Эмоционалдық қозу деңгейі мен алдын алу мазмұнындағы хабарламалардың адамдардың алаяқтыққа алданып қалу ықтималдығына әсері қарастырылады. Авторлар эмоцияның күшеюі адамның шешім қабылдау қабілетін әлсіретіп, алаяқтыққа бейімділікті арттыратынын анықтайды. Сонымен бірге алдын ала ескерту және профилактикалық мазмұндағы хабарламалар адамдардың

сақтық деңгейін күшейтіп, алаяқтықтан қорғануға көмектесетіні көрсетілген. Зерттеу киберқауіпсіздік саласында мінез-құлықтық факторлардың маңызын айқындайды (Lu et al, 2020).

Спамға негізделген интернет-алаяқтықтың құрылымы, таратылу механизмдері және қауіптілігі жан-жақты талданады. Автор спам-хабарламалардың әлемдік киберқылмыстың маңызды бөлігіне айналғанын, олар арқылы фишинг, қаржылық алаяқтық және жалған ұсыныстардың кең таралатынын атап өтеді. Зерттеу халықаралық деңгейде спаммен күресу үшін құқықтық, техникалық және профилактикалық шараларды біріктіру қажеттігін көрсетеді (Kigerl, 2020).

Фишинг пен интернет алаяқтықтың архитектурасы өте күрделі болғандықтан, олардың Қазақстандағы әрекет ету механизмдерін талдау жан-жақты және терең зерттеуді талап етеді (Raximov et al, 2024). Қазақстан азаматтарына бағытталған ең кең таралған алаяқтық әдістерді сипаттап, жалған электрондық пошталар, хабарламалар және вирустық сілтемелер арқылы жүзеге асырылатын шабуылдардың қауіптілігін айқындайды. Олардың пайымдауынша, көптеген азаматтар жалған хабарламаларды шынайы байланыстан ажырата алмай, алаяқтықтың құрбанына айналады. Осы тұрғыда зерттеушілер интернеттегі қауіптердің алдын алуға арналған негізгі бағыттарды ұсынуда.

Киберқылмысқа қарсы әрекет етуде құқықтық және криминологиялық тұрғыдағы көзқарасты қарастырып, полиция жұмысының теориялық және практикалыққиындықтарынатоқталады.Авторларинтернеталаяқтықтарының Қазақстанның қоғамдық-саяси жағдайына бейімделген күрделі сипатын атап өтіп, мамандандырылған киберполиция құрылымдарының қажеттілігін көрсетеді (Lakbayev et al, 2020).

Психологиялық факторларға назар аударған фишингтік шабуылдардың сәттілігін түсіндіретін когнитивтік бұрмаланулар мен сандық сауаттылықтың төмендігін айқындайды (Sarno et al, 2024). Бұл құбылысты тереңірек зерттеп, импульсивтілік пен шамадан тыс өзіне сенімділік сияқты тұлғалық қасиеттердің адамдарды интернет алаяқтарының осал нысанасына айналдыратынын дәлелдейді (Hanoch et al, 2021).

Нигериядағы электрондық пошта алаяқтықтарында қолданылатын дискурсивті-манипулятивті стратегияларды талдай отырып, мұндай әдістерді Қазақстан жағдайымен салыстыруға болатындығын көрсетеді. Оның тілдік үлгілер мен психологиялық триггерлерге жасаған талдауы қазақ тіліндегі фишингтік хабарламаларды, әсіресе WhatsApp және Telegram платформаларындағы жалған ақпаратты зерттеуге құнды салыстыру ұсынады (Ajayi, 2022).

Технологиялық шешімдер тұрғысынан машиналық оқыту мен жасанды интеллектке негізделгенүшіншітарапжүйесінұсынып,күдіктіхабарламаларды пайдаланушыға жетпей анықтау және бұғаттау мүмкіндіктерін көрсетеді (Tran

et al, 2020). Әлеуметтік медиа платформалардағы пікір алаяқтықтарының күшеюіне назар аударып, фейк пікірлердің күрделі алаяқтықтарға жол ашатынын дәлелдейді (Li et al, 2024). «Ақша муле рекрутменті» феноменін қарастырып, интернет алаяқтықтарының психологиялық манипуляция аспектілерін ашып көрсетеді (Chethiyar et al, 2021).

Пайдаланушы тәжірибесін зерттеген) мобильді фишингтегі сендіруші хабарламалардың ықпалын талдаса (Ahmad et al, 2023), сарапшылар мен қарапайым қолданушылардың фишингтік алаяқтықтарды анықтау қабілеттеріндегі айырмашылықты айқындайды (Wash, 2020). Сонымен қатар, SMS арқылы жасалатын спам-фишинг шабуылдарын талдап, заңды және жалған хабарламаларды ажырату алгоритмдерінің тиімділігін қарастырады (Liu et al, 2021).

Жалпы алғанда, қарастырылған еңбектер фишинг пен интернет-алаяқтықтың көпқырлы табиғатын көрсетеді. Психологиялық бейімділіктер мен тілдік стратегиялардан бастап, құқықтық негіздер мен технологиялық интервенцияларға дейінгі факторлар алаяқтық әрекеттерді түсінуге кешенді көзқарасты қажет етеді. Бұл әдебиетке шолу киберқауіпсіздік мәселесін шешуде психология, құқық, технология және пайдаланушы тәжірибесін біріктіретін көпсалалы тәсілдің маңыздылығын айқындайды.

Материалдар мен әдістер. Мессенджер арқылы келетін хабарламаларды интернет-алаяқтыққа анықтау мақсатында жаңа модель ұсынылады. Бұл модель QazNLTK кітапханасының мүмкіндіктерін пайдалана отырып әзірленді және оның архитектурасы бірнеше кезеңнен тұрады: мәтінді токенизациялау, салыстырмалы талдау және алаяқтыққа болатын ықтимал қаупін бағалау. Ұсынылған жүйе әрбір кіріс хабарламадан қауіпті сигналдарды бөліп алып, ықтимал алаяқтыққа сәйкес балл немесе белгі қою арқылы шешім қабылдайды. Осы модельдің логикалық-схемасы және компоненттердің өзара байланысы Сурет 1-де көрсетілген.

Сурет 1. Модель құрылымы

Зерттеуде мессенджерлер арқылы келіп түсетін мәтіндік хабарламаларды интернет-алаяқтықтан қорғауға бағытталған жаңа модель ұсынылады. Модельдің құрылымы бірнеше кезеңнен тұрады:

1. **QazNLTK инициализациясы.** Зерттеу жұмысының бастапқы кезеңінде қазақ тіліндегі мәтіндерді өңдеуге арналған QazNLTK кітапханасы іске қосылады. Бұл кітапхана токенизациялау, морфологиялық талдау және мәтіндік деректермен жұмыс істеу үшін қажетті құралдарды қамтамасыз етеді.

2. **Сандарды мәтінге түрлендіру функциясы.** Мәтіндегі сандарды сөздік формаға түрлендіру арқылы («123» → «бір жүз жиырма үш») контекстің дұрыс түсінілуі қамтамасыз етіледі. Бұл процесс алаяқтық хабарламалардың семантикасын дәлірек тануға мүмкіндік береді.

3. **Алдын ала берілген сөйлемдерді белгілеу.** Базалық деңгейде белгілі бір үлгідегі хабарламалар токенизацияланып, сөздік массив құрылады. Бұл массив кейінгі салыстыру процесінде эталон ретінде қолданылады.

4. **Жаңа хабарламаларды таңбалау.** Мессенджерлерден алынған жаңа хабарламалар да QazNLTK арқылы токенизацияланады. Осылайша, олар алдын ала дайындалған базаға салыстыруға дайын күйге келтіріледі.

5. **Салыстыру және сәйкестендіру.** Токенизацияланған мәтіндер арасында ұқсастықты анықтау үшін Jaccard Similarity, Cosine Similarity сияқты алгоритмдер пайдаланылады. Бұл әдістер хабарламалар арасындағы семантикалық және лексикалық ұқсастықтарды бағалауға жол ашады.

6. **Ең жоғарға сәйкестікті анықтау.** Салыстыру қорытындыларына сәйкес, ұқсастық деңгейі ең үлкен хабарламалар іріктеп алынады. Осы кезеңде ықтимал қауіпті хабарламалар нақты белгіленеді.

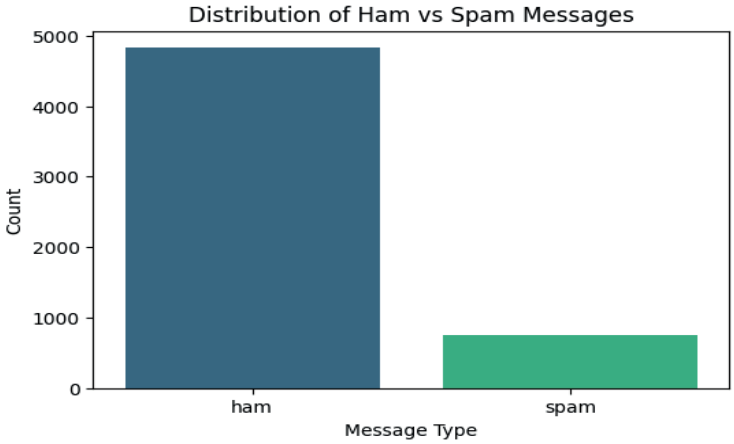
7. **Нәтижелерді шығару.** Модельдің жұмысының қорытындысы пайдаланушыға немесе жүйеге ұсынылады. Нәтижелер интерфейс жағдайына байланысты графикалық түрде, статистикалық кесте немесе мәтіндік файл түрінде берілуі мүмкін.

Ұсынылған модель қазақ тіліндегі мәтіндерді өңдеуге бағытталып, токенизация, салыстыру және ықтимал қауіптерді анықтау сияқты кезеңдерді қамтамасыз етеді. Әзірленген әдіс мессенджерлер арқылы таралатын жалған хабарламаларды ерте анықтауға және алдын алуға мүмкіндік береді.

Зерттеу барысында модельдің тиімділігі жан-жақты тексерілді. Алгоритмдер жұмысын талдау, статистикалық көрсеткіштерді бағалау арқылы оның алаяқтық хабарламаларды анықтаудағы нәтижелілігі дәлелденді.

Сонымен қатар, деректерді талдау үшін **SMS Spam Collection Dataset** пайдаланылды. Сурет 2-де осы деректер жиынындағы «Спам» және «Хам» хабарламаларының таралуы көрсетілген. Талдау нәтижесі бойынша «Хам» (заңды, шынайы) хабарламалардың үлесі көп болғанымен, «Спам» хабарламаларының үлесі де жоғары екені анықталды. Бұл қазіргі уақытта спамның көрсеткіші елеулі қауіп төндіруші фактор болып отырғанын

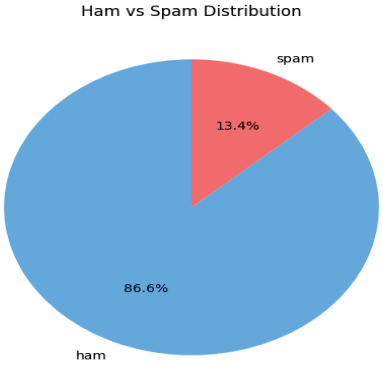
айғақтайды және алаяқтық хабарламаларды анықтау алгоритмдерін жетілдірудің өзектілігін күшейтеді.



Сурет 2. Спам және Хам хабарламаларының үлестірімі

Спам хабарламалардың кең таралуының негізгі себептерінің бірі – олардың таратылу құнының төмендігі мен жылдам орындалуы. Мұндай хабарламалар көбінесе жарнамалық немесе алдамшы мақсаттарда қолданылып, пайдаланушылардың қауіпсіздігіне елеулі қатер төндіреді.

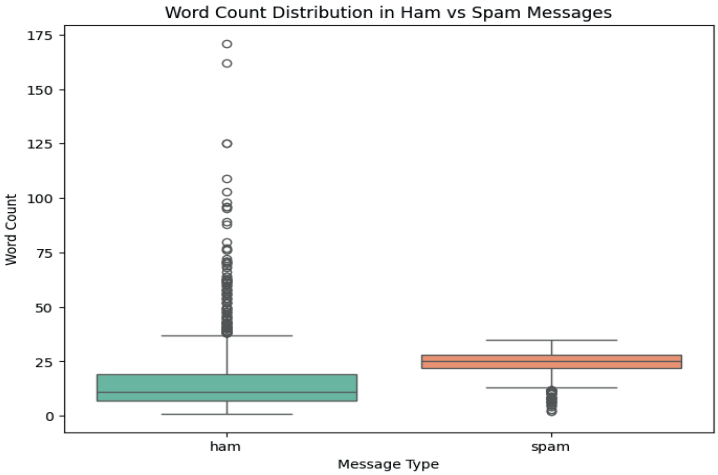
Сурет 3-те хабарламалардың ұзындығы сөздер саны бойынша талданған. Нәтижесінде, спам хабарламаларда әдетте сөздердің көбірек қолданылатыны байқалды, ал легитимді (хам) хабарламалар қысқа әрі нақты келеді. Диаграмма көрсеткендей, спам хабарламалар пайдаланушының назарын аударып, олардан белгілі бір әрекет жасауға итермелеу мақсатында ауқымды ақпаратты қамтиды. Керісінше, легитимді хабарламаларда қысқа мазмұн басым болып, тек қажетті ақпарат жеткізіледі.



Сурет 3. Хабарламалардағы сөз санының үлестірімі

Жүргізілген талдау қорытындыларына сәйкес, спам хабарламалар мәтініндегі сөздердің көп қолданылуы олардың мазмұнының ұзақ әрі көлемді болатынын дәлелдейді. Мұндай хабарламаларда көбінесе әртүрлі айла-шарғы тәсілдері, мысалы, ұсыныстар немесе сыйлық ұтып алу жайлы ақпарат беріледі.

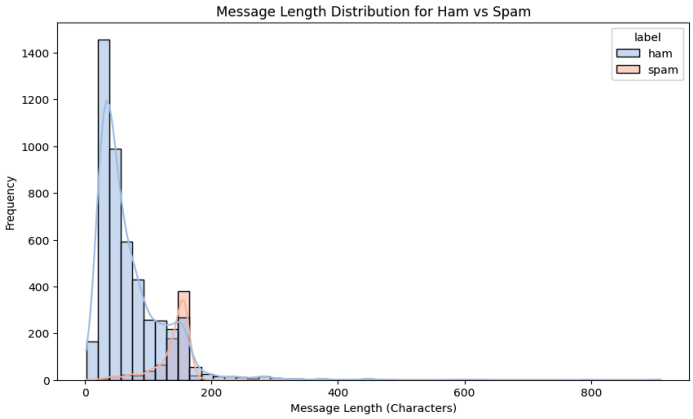
Сурет 4-те спам хабарламаларында ең көп қайталанатын сөздердің бұлты көрсетілген. Мұнда «ұтыс», «тегін», «сыйлық» сияқты сөздердің айрықша жиі қолданылатыны байқалады. Аталған сөздер спам хабарламаларының негізгі мазмұнын қалыптастыратын негізгі элементтер ретінде қарастырылады. Спамның негізгі мақсаты – пайдаланушының назарын аударып, оларды белгілі бір әрекеттерге, мысалы, ақша аударуға немесе жеке деректерін ұсынуға итермелеу болып табылады.



Сурет 4. Спам мәтіндеріндегі жиі қайталанатын сөздер

Спам хабарламаларында жиі қайталанатын сөздердің қолданылуы оларды автоматты түрде анықтау мен сүзгілеу үшін тиімді белгі ретінде қарастырылады. Осыған байланысты машиналық оқыту алгоритмдерін қолдану мақсатқа сай келеді. Жиі кездесетін сөздер негізінде құрылған классификаторлар хабарламаларды санаттарға бөліп, спамды автоматты түрде тануға мүмкіндік береді. Бұл тәсіл пайдаланушылардың ақпараттық қауіпсіздігін арттыруға елеулі үлес қоса алады.

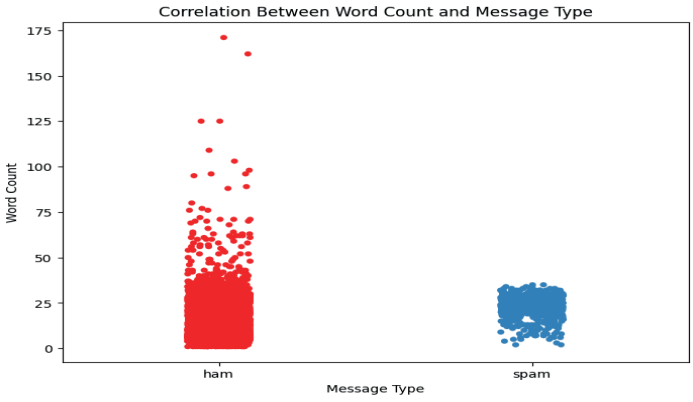
Сурет 5-те хабарлама мәтіндерінің ұзындығы бойынша жасалған талдау нәтижелері берілген. Мұнда хабарламалардың сөздер санына қарай спам мен хам түрлері арасындағы айырмашылық айқын көрсетілген. Нәтижелерге сәйкес, спам хабарламалар көбінесе ұзақ әрі көлемді болып келеді, себебі олар пайдаланушыны қызықтыру үшін артық ақпарат пен әртүрлі айла-тәсілдерді қамтиды. Ал хам хабарламалар қысқа әрі нақты болып, тек қажетті ақпаратты жеткізумен шектеледі.



Сурет 5. Хабарламалардың ұзындығы бойынша үлестірімі

Хабарламалардың ұзындығындағы вариациялар автоматтандырылған сүзгілеу жүйелері үшін маңызды ерекшелік болып табылады. Хабарламалардың ұзындығына талдау жасау арқылы жүйе спамды тиімді әрі жылдам анықтай алады. Бұл ерекшелік классификациялау алгоритмдері үшін қосымша өлшем ретінде қолданылады.

Сурет 6-да сөздер саны мен хабарлама типінің арасындағы байланысы көрсетілген. Мұнда әр хабарламаның ұзындығы (сөздер саны) және оның тиісті категориясы (спам немесе хам) арасындағы тәуелділік талданған. Нәтижелерге сәйкес, хам хабарламалар әдетте қысқа әрі нақты болып келеді, себебі олар тек қажетті ақпаратты қамтиды. Ал спам хабарламаларда сөздер саны көп болып, мазмұны артық ақпаратқа толы болады. Мұндай хабарламалардың негізгі мақсаты – пайдаланушының назарын аударып, оны белгілі бір әрекетке итермелеу. Осылайша, хабарлама ұзындығының талдауы мәтіндерді санаттарға бөлу процесінде маңызды факторлардың бірі ретінде қарастырылады.



Сурет 6. Хабарлама түрлеріне байланысты сөз санының таралуы

Зерттеуде қолданылатын модель бірнеше кезеңмен жүзеге асырылады:

1. Инициализация.

Алдымен QazNLTK кітапханасы іске қосылып, мәтінді токенизациялауға қажетті функциялар дайындалады:

```
From qaznltk import qaznltk as qtool
QazNLTK processor = qtool.QazNLTK()
```

2. Сандарды сөздерге ауыстыру.

Convert_numbers_to_words аталған функция мәтіндік деректер құрамындағы сандық мәндерді сөздік формаға түрлендіреді. Мысалы, *«3 мың теңге»* сандық түрде көрсетілген мән функция арқылы *«үш мың теңге»* сөздік формаға өзгереді. Бұл сөйлемдердің мәнмәтінін терең түсінуге мүмкіндік береді:

```
def numbers_to_text(message):
    tokens = message.split()
    updated_tokens = []
    for token in tokens:
        if token.isdigit():
            num_value = int(token)
            token = processor.num2word(num_value)
        updated_tokens.append(token)
    return ' '.join(updated_tokens)
```

3. Токенизация.

Жіберілген жабарлама түріне байланысты токендерге сыныптастырылады, яғни әрбір сөз жеке бөлік болып қарастырылады.

```
sentencesA = [
"Сіздің хабарламаңыз күдікті әрекеттерге байланысты.",
"Сіз ұтысқа ие болдыңыз! Алу үшін кішкене сома аударыңыз.",
"Сіздің достарыңыз көмек сұрауда. Оларға ақша керек.",
"Инвестиция салу бойынша ұсыныс бар."
]
```

4. Сәйкестікті тексеру

Жаңа хабарлама алдынала белгіленген күдікті мәтіндермен салыстырылады. Сәйкес сөздер саны мен сәйкестік пайызы есептеледі.

Тест нәтижелері.

Модель 100 мәтіндік хабарламада сыналды. Әр хабарлама 4 негізгі күдікті мәтінмен салыстырылды (Кесте 1).

Кесте 1. Хабарламалармен салыстыру нәтижелері

Хабарлама мәтіні	Ұқсастық деңгейі (%)	Ұқсас сөздер саны
Сіздің хабарламаңыз күдікті...	75.00	9
Сіз ұтысқа ие болдыңыз!...	50.00	6
Сіздің достарыңыз көмек сұрауда...	25.00	3
Инвестиция салу бойынша ұсыныс...	0.00	0

Талдау. Нәтижелер бойынша, модель «Сіздің хабарламаңыз күдікті әрекеттерге байланысты» мәтінімен 75% сәйкестік көрсетті, бұл оның күдікті хабарламаларды анықтауда тиімді екенін дәлелдейді.

Статистикалық бағалау. Confusion Matrix негізінде модельдің сапа көрсеткіштері есептелді (Кесте 2).

Кесте 2. Модельдің тиімділігін бағалау нәтижелері

Көрсеткіш	Мән
Дұрыстық деңгейі (Accuracy)	0.72
Қамту деңгейі (Recall)	0.70
Айқындығы (Precision)	0.65
F1 көрсеткіші (F1-Score)	0.67

Аталған көрсеткіштер модельдің хабарламаларды дұрыс жіктеуде және алаяқтық шабуылдарды болжауда әлеуеті бар екенін растайды.

Қорытынды. Зерттеу нәтижесінде мессенджерлер арқылы таратылатын мәтіндік хабарламаларды алаяқтықтан қорғауға арналған тиімді модель ұсынылды. QazNLTK негізіндегі жүйе мәтіндерді өңдеу, токенизациялау және салыстыру әдістерін қолданып, жақсы нәтижелер көрсетті.

Модельдің тиімділігі статистикалық көрсеткіштер негізінде дәлелденді. Жүйе «Сіздің хабарламаңыз күдікті әрекеттерге байланысты» хабарламасымен 75% сәйкестік көрсетті, бұл оның алаяқтықты анықтаудағы әлеуетін айқындайды. Confusion Matrix нәтижесінде алынған дұрыстық деңгейі (accuracy), қамту деңгейі (recall) және F1 көрсеткіші (F1-score) мәндері модельдің шынайы жағдайда жұмыс істеу қабілетін нақты көрсетті.

Алдағы уақытта модельді жетілдіру үшін бірнеше бағыт ұсынылады:

1. Деректер жиынтығын кеңейту: Алаяқтық хабарламалардың әртүрлі түрлері мен контекстін қамту арқылы модельдің үйрену мүмкіндігін күшейту.

2. Жасанды интеллект әдістерін енгізу: Машиналық оқыту мен терең оқыту (deep learning) алгоритмдерін қолдану модельдің тиімділігін арттыруға жол ашады.

3. Нақты уақыт режимінде сынақтан өткізу: Жүйені real-time форматында тестілеп, оның өнімділігін және жауап беру жылдамдығын бағалау.

Осы зерттеу мессенджерлердегі алаяқтық әрекеттерге қарсы қорғаныс жүйелерін дамытуға алғашқы негіз қалады. Алынған нәтижелер модельдің практикалық тұрғыда қолдануға жарамдылығын айқындап қана қоймай, болашақта оның тиімділігін жетілдіру үшін жаңа идеялар мен бағыттарға жол ашады. Алаяқтықпен күресте заманауи технологияларды пайдалану – өзекті әрі қажетті қадам, және бұл бағыттағы жұмыстардың алдағы уақытта зерттеулердің жалғасын табатынына сенім білдіріледі.

Әдебиеттер

qazaqstan.tv (2024) Интернет алаяқтық түрленіп барады. https://qazaqstan.tv/news/197676/7 (20 Қазан 2024 сілтеме алынды).

eGov.kz электрондық үкімет порталы (2024) Абайлаңыз, интернет-алаяқтар!. https://www.gov.kz/memleket/entities/sko-mamlyut-krasnoznamen/press/news/details/750707?lang=kk. (20 Қазан 2024 сілтеме алынды).

Lu H.Y., Chan S., Chai W., Lau S.M. & Khader M. (2020) Examining the influence of emotional arousal and scam preventive messaging on susceptibility to scams. Crime Prevention and Community Safety, 22(4). — P. 313-330. https://doi.org/10.1057/s41300-020-00098-3

Kigerl A. (2020) Spam-based scams. The Palgrave Handbook of International Cybercrime and Cyberdeviance. — P. 877-897. https://doi.org/10.1007/978-3-319-78440-3_42

Raximov Q., Mamatova Z. & Tazhikenova N. (2024). COMMON PHISHING ATTACKS IN KAZAKHSTAN AND WAYS TO PROTECT CITIZENS FROM INTERNET SCAMMERS. Farg'ona davlat universiteti, (3). — P. 130-130.

Lakbayev K.S., Rysmagambetova G.M., Umetov A.U. & Sysoyev A.K. (2020) The crimes in the field of high technology: Concept, problems and methods of counteraction in Kazakhstan. International Journal of Electronic Security and Digital Forensics, 12(4) . — P. 412-423.

Sarno D.M. & Black J. (2024) Who gets caught in the Web of lies?: Understanding susceptibility to phishing emails, fake news headlines, and scam text messages. Human Factors, 66(6) . — P. 1742-1753. https://doi.org/10.1177/00187208231173263

Hanoch Y. & Wood S. (2021). The scams among us: Who falls prey and why. Current Directions in Psychological Science, 30(3) . — P. 260-266. https://doi.org/10.1177/0963721421995489

Ajayi T.M. (2022) Discursive-manipulative strategies in scam emails and SMS: The Nigerian perspective. Lodz Papers in Pragmatics, 18(1) . — P. 175-195. DOI: 10.1515/lpp-2022-0008

Tran M.H., Hoai T.H. & Choo H. (2020) A third-party intelligent system for preventing call phishing and message scams. In Future Data and Security Engineering. Big Data, Security and Privacy, Smart City and Industry 4.0 Applications: 7th International Conference, FDSE 2020, Quy Nhon, Vietnam, November 25–27, 2020, Proceedings 7. — P. 486-492. Springer Singapore. https://doi.org/10.1007/978-981-96-0437-1

Li X., Rahmati A. & Nikiforakis N. (2024) Like, Comment, Get Scammed: Characterizing Comment Scams on Media Platforms. In Proceedings 2024 Network and Distributed System Security Symposium. https://dx.doi.org/10.14722/ndss.2024.24060

Chethiyar S.D.M., Vedamanikam M. & Sameem M.A. (2021) Losing The War Against Money Mule Recruitment: Persuasive Technique In Romance Scam. Ilkogretim Online, 20(3). — P. 2569-2585. DOI: 10.17051/ilkonline.2021.03.290

Ahmad R., Terzis S. & Renaud K. (2023) Content analysis of persuasion principles in mobile instant message phishing. In International Symposium on Human Aspects of Information Security and Assurance. — P. 324-336. Cham: Springer Nature Switzerland. DOI: 10.1007/978-3-031-38530-8_26

Wash R. (2020). How experts detect phishing scam emails. Proceedings of the ACM on Human-Computer Interaction, 4(CSCW2), 1-28. https://doi.org/10.1145/3415231

Liu M., Zhang Y., Liu B., Li Z., Duan H. & Sun D. (2021, December) Detecting and characterizing SMS spearphishing attacks. In Proceedings of the 37th Annual Computer Security Applications Conference. — P. 930-943. https://doi.org/10.1145/3485832.3488012

References

qazaqstan.tv (09 tamyz 2024). Internet alayaqtyq turlenip barady [Internet scams are transforming]. https://qazaqstan.tv/news/197676/7 (20 Qazan 2024 silteme alyndy) (in Kazakh)

eGov.kz elektrondyq ükimet portaly. (15 säuir 2024) Abaylañyz, internet-alayaqtar! [Caution, internet scammers!] https://www.gov.kz/memleket/entities/sko-mamlyut-krasnoznamen/press/news/details/750707?lang=kk (20 Qazan 2024 silteme alyndy) (in Kazakh)

Lu H.Y., Chan S., Chai W., Lau S.M. & Khader M. (2020) Examining the influence of emotional

arousal and scam preventive messaging on susceptibility to scams. Crime Prevention and Community Safety, 22(4). — P. 313-330 https://doi.org/10.1057/s41300-020-00098-3 (in English)

Kigerl A. (2020) Spam-based scams. The Palgrave Handbook of International Cybercrime and Cyberdeviance. — P. 877-897 https://doi.org/10.1007/978-3-319-78440-3_42 (in English)

Raximov Q., Mamatova Z. & Tazhikenova N. (2024) COMMON PHISHING ATTACKS IN KAZAKHSTAN AND WAYS TO PROTECT CITIZENS FROM INTERNET SCAMMERS. Farg'ona davlat universiteti, (3). — P. 130-130. (in English)

Lakbayev K.S., Rysmagambetova G.M., Umetov A.U. & Sysoyev A.K. (2020) The crimes in the field of high technology: Concept, problems and methods of counteraction in Kazakhstan. International Journal of Electronic Security and Digital Forensics, 12(4) . — P. 412-423. (in English)

Sarno D.M. & Black J. (2024) Who gets caught in the Web of lies?: Understanding susceptibility to phishing emails, fake news headlines, and scam text messages. Human Factors, 66(6). — P. 1742-1753 https://doi.org/10.1177/00187208231173263 (in English)

Hanoch Y. & Wood S. (2021) The scams among us: Who falls prey and why. Current Directions in Psychological Science, 30(3) . — P. 260-266. https://doi.org/10.1177/0963721421995489 (in English)

Ajayi T.M. (2022) Discursive-manipulative strategies in scam emails and SMS: The Nigerian perspective. Lodz Papers in Pragmatics, 18(1). — P. 175-195. DOI: 10.1515/lpp-2022-0008 (in English)

Tran M.H., Hoai T.H. & Choo H. (2020) A third-party intelligent system for preventing call phishing and message scams. In Future Data and Security Engineering. Big Data, Security and Privacy, Smart City and Industry 4.0 Applications: 7th International Conference, FDSE 2020, Quy Nhon, Vietnam, November 25–27, 2020, Proceedings 7. — P. 486-492. Springer Singapore. https://doi.org/10.1007/978-981-96-0437-1 (in English)

Li X., Rahmati A. & Nikiforakis N. (2024) Like, Comment, Get Scammed: Characterizing Comment Scams on Media Platforms. In Proceedings 2024 Network and Distributed System Security Symposium. https://dx.doi.org/10.14722/ndss.2024.24060 (in English)

Chethiyar S.D.M., Vedamanikam M. & Sameem M.A. (2021) Losing The War Against Money Mule Recruitment: Persuasive Technique In Romance Scam. Ilkogretim Online, 20(3). — P. 2569-2585. DOI: 10.17051/ilkonline.2021.03.290 (in English)

Ahmad R., Terzis S. & Renaud K. (2023) Content analysis of persuasion principles in mobile instant message phishing. In International Symposium on Human Aspects of Information Security and Assurance. — P. 324-336. Cham: Springer Nature Switzerland. DOI: 10.1007/978-3-031-38530-8_26 (in English)

Wash R. (2020). How experts detect phishing scam emails. Proceedings of the ACM on Human-Computer Interaction, 4(CSCW2), 1-28. https://doi.org/10.1145/3415231 (in English)

Liu M., Zhang Y., Liu B., Li Z., Duan H. & Sun D. (2021, December) Detecting and characterizing SMS spearphishing attacks. In Proceedings of the 37th Annual Computer Security Applications Conference. — P. 930-943. https://doi.org/10.1145/3485832.3488012 (in English)

Publication Ethics and Publication Malpractice in the journals of the Central Asian Academic Research Center LLP

For information on Ethics in publishing and Ethical guidelines for journal publication see http://www.elsevier.com/publishingethics and http://www.elsevier.com/journal-authors/ethics.

Submission of an article to the journals of the Central Asian Academic Research Center LLP implies that the described work has not been published previously (except in the form of an abstract or as part of a published lecture or academic thesis or as an electronic preprint, see http://www.elsevier.com/postingpolicy), that it is not under consideration for publication elsewhere, that its publication is approved by all authors and tacitly or explicitly by the responsible authorities where the work was carried out, and that, if accepted, it will not be published elsewhere in the same form, in English or in any other language, including electronically without the written consent of the copyright-holder. In particular, translations into English of papers already published in another language are not accepted.

No other forms of scientific misconduct are allowed, such as plagiarism, falsification, fraudulent data, incorrect interpretation of other works, incorrect citations, etc. The Central Asian Academic Research Center LLP follows the Code of Conduct of the Committee on Publication Ethics (COPE), and follows the COPE Flowcharts for Resolving Cases of Suspected Misconduct (http://publicationethics.org/files/u2/New_Code.pdf). To verify originality, your article may be checked by the Cross Check originality detection service http://www.elsevier.com/editors/plagdetect.

The authors are obliged to participate in peer review process and be ready to provide corrections, clarifications, retractions and apologies when needed. All authors of a paper should have significantly contributed to the research.

The reviewers should provide objective judgments and should point out relevant published works which are not yet cited. Reviewed articles should be treated confidentially. The reviewers will be chosen in such a way that there is no conflict of interests with respect to the research, the authors and/or the research funders.

The editors have complete responsibility and authority to reject or accept a paper, and they will only accept a paper when reasonably certain. They will preserve anonymity of reviewers and promote publication of corrections, clarifications, retractions and apologies when needed. The acceptance of a paper automatically implies the copyright transfer to the Central Asian Academic Research Center LLP.

The Editorial Board of the Central Asian Academic Research Center LLP will monitor and safeguard publishing ethics.

Правила оформления статьи для публикации в журнале смотреть на сайтах:
www:nauka-nanrk.kz
http://physics-mathematics.kz/index.php/en/archive
ISSN2518-1726 (Online),
ISSN 1991-346X (Print)

Ответственный редактор *А. Ботанқызы*
Редакторы: *Д.С. Аленов, Т. Апендиев*
Верстка на компьютере: *Г.Д. Жадырановой*

Подписано в печать 22.12.2025.
Формат 60x881/8. Бумага офсетная.
Печать –ризограф. 20,0 п.л. Заказ 4.

«Central Asian Academic Research Center» LLP
Алматы, Қонаев к-сі, 142