

ISSN 2518-1726 (Online),

ISSN 1991-346X (Print)

**ACADEMIC SCIENTIFIC
JOURNAL OF COMPUTER SCIENCE**

**№2
2026**

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



ACADEMIC SCIENTIFIC JOURNAL OF COMPUTER SCIENCE

3 (359)

JULY – SEPTEMBER 2026

**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, (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>

USATOVA Olga Alexandrovna, PhD, Associate Professor, Chief Scientific Secretary of the Institute of Information and Computing Technologies of the National Academy of Sciences of the Republic of Kazakhstan (Almaty, Kazakhstan), <https://www.scopus.com/authid/detail.uri?authorId=57204581062>, <https://www.webofscience.com/wos/author/record/JCO-3058-2023>

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, 2026

БАС РЕДАКТОР:

МУТАНОВ Ғалымқайыр Мұтанұлы, техника ғылымдарының докторы, профессор, ҚР ҰҒА академигі, (Алматы, Қазақстан), <https://www.scopus.com/authid/detail.uri?authorId=6506682964>, <https://www.webofscience.com/wos/author/record/1423665>

РЕДАКЦИЯ АЛҚАСЫ:

КАЛИМОЛДАЕВ 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>

УСАТОВА Ольга Александровна, PhD, қауымдастырылған профессор, ҚР ҒЖБМ "Ақпараттық және есептеу технологиялары институтының" бас ғалым хатшысы (Алматы, Қазақстан), <https://www.scopus.com/authid/detail.uri?authorId=57204581062>, <https://www.webofscience.com/wos/author/record/JCO-3058-2023>

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, 2026

Главный редактор:

МУТАНОВ Галимканир Мутанович, доктор технических наук, профессор, академик НАН РК, (Алматы, Казахстан), <https://www.scopus.com/authid/detail.uri?authorId=6506682964>, <https://www.webofscience.com/wos/author/record/1423665>

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>

УСАТОВА Ольга Александровна, PhD, ассоциированный профессор, Главный ученый секретарь «Института информационных и вычислительных технологий» КН МНВО РК (Алматы, Казахстан), <https://www.scopus.com/authid/detail.uri?authorId=57204581062>, <https://www.webofscience.com/wos/author/record/JCO-3058-2023>

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 КОКШВО 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», 2026

CONTENTS

Akhmetova A.Zh., Kantureyeva M.A., Serimbetov B.A., Zhasuzakova M.Zh., Mustafayeva N.T. Identification of communities and active users in social networks.....	11
Akzhigitov D., Mukhtarkhanov M., Zhetpisbayeva A., Kulakayeva A., Zhetpisbayev K. Analysis of the mechanical structure of a 12U CubeSat nanosatellite and assessment of its mechanical stability.....	29
Alibekov A., Nurimanov A., Mukhametkali A., Kassym D., Varol H.A. Qolda-Math: a small vision-language model for mathematical reasoning in Kazakh.....	50
Alisheva S.S., Ospanova A.O., Shaimerdenova G.S., Shaimerdenova L., Zhidebayeva A.N. Detecting Kazakh language offensive comments in online content using deep learning algorithms.....	68
Askar G., Mutaikhan A., Aitkozhayeva M., Nauryzbaikyzy G., Makhataeva Z. Retrieval beats fine-tuning: adapting a Kazakh small language model for historical question answering.....	86
Beissenova G.I., Shynzhigit B.B., Beisebayeva A.Zh., Kaldarova B.S., Lesbayev A.U. Deep neural network-based speaker authentication for secure access control systems.....	106
Bekenuly B., Baimakhanova A., Baiturganova V., Bolatbekova D. Comparison of CNN architectures for automated ACL injury classification from knee MRI.....	123
Bekbolat A., Razak A., Alimbayeva Z., Ozhikenova A. Multi-task deep learning for knee MRI pathology classification.....	139
Issakhov A., Akylbekkyzy A., Abylkassymova A. Predicting the spread of airborne viral infections in enclosed spaces.....	158
Kisseleva O., Abdramanov K., Naumenko V., Mukanova Z., Maintser D. Evaluation of serverless cold start optimization techniques.....	177
Koshkarov Ye.Zh., Amirgaliyev B.Ye., Mulesa O. Physics-aware masked pretraining for cross-basin well log foundation models.....	197
Kurmetkan T., Turysbek Zh., Mukhitova A., Nauryzbaeva A. Research on methods for reducing knowledge conflicts in large language models in Kazakh question-and-answer systems.....	214
Makatov Ye.K., Abdul Razaque, Ismukanova A.N., Salykova A.K., Glock E.S. Machine learning-based model for phishing URL detection in online social networks.....	233
Mimenbayeva A.B., Naizagarayeva A.A., Ospanova T.T., Koikelova D.K., Kudabayeva R.N. Spatial and climate data analysis for machine learning-based crop yield prediction in Northern Kazakhstan.....	255
Mukhamediev R.I., Abdoldina F.N., Gertsen Y.A. Economic opportunities and constraints of artificial intelligence adoption in Kazakhstan's resource-oriented economy.....	274

Mutanov G.M., Karyukin V.I., Ussatova O.A., Begimbayeva Y.Y., Baispay G.B. The assessment of blockchain readiness for academic document verification.....	289
Mussiraliyeva Sh., Bolatbek M., Baisylbayeva K. Classification of cyber-extremist ideologies in the Kazakh language considering multi-annotator disagreement.....	306
Omarov B.S., Sultan D.R., Rakhymberdiev D.S., Abibullayeva A.A., Toktarova A.B. Deformable attention-guided Transformer for brain tumor segmentation.....	326
Oralbekova D., Bekarystankyzy A., Yerimbetova A., Berzhanova U. Development of a streaming Kazakh speech recognition system using end-to-end models.....	346
Serek A., Shoiynbek A., Zheludkov M., Kuanyshbay D., Meraliyev B. Comparative analysis of machine learning methods for detecting fraud in text messages.....	365
Smakhanova A.K., Uskenbayeva R.K., Kassymova A.B., Kalpeyeva Zh.B., Konyrbaev N.B. Experimental research using models and methods of the university digital ecosystem.....	384
Sultanali A.E., Kazbekova G.N. Machine learning-based detection of AI-generated content in students' written works.....	401
Tashenova Zh., Yergazin A., Nurlybaeva E., Abdugulova Zh., Amanzholova Sh. Experimental evaluation of a hybrid IDPS with adaptive learning for low-latency 5G networks using edge computing.....	418
Telman D., Yerimbetova A., Daiyrbayeva E. Leakage-resistant fake news detection for Kazakh: temporal evaluation of lexical, Transformer and hybrid models.....	441
Zhanegizov A., Mamyrbayev O., Abdigappar M. Application of YOLO12 for road defect detection in GPR images.....	457

МАЗМҰНЫ

Ахметова А.Ж., Кантуреева М.А., Серимбетов Б.А., Жасұзақова М.Ж., Мұстафаева Н.Т. Әлеуметтік желілердегі қауымдастықтар мен белсенді қолданушыларды анықтау.....	11
Ақжігітов Д.Ж., Мұхтарханов М.О., Жетписбаева А.Т., Кулакаева А.Е., Жетписбаев К.У. 12U CubeSat үлгісіндегі наноспутниктің механикалық құрылымын талдау және оның механикалық орнықтылығын бағалау.....	29
Алибеков А., Нуриманов А., Мұхаметқали А., Қасым Д., Варол Х.А. Qolda-Math: қазақ тіліндегі математикалық пайымдауға арналған кіші көру-тілдік модель.....	50
Алишева С.С., Оспанова А.О., Шаймерденова Г.С., Шаймерденова Л., Жидебаева А.Н. Онлайн-контенттегі қазақ тіліндегі бейәдеп пікірлерді терең оқыту алгоритмдері арқылы анықтау.....	68
Асқар Ғ., Мұтайхан А., Айтқожаева М., Наурызбайқызы Г., Махатаева Ж. Retrieval fine-tuning-тен басым: тарихи сұрақтарға жауап беру үшін қазақша шағын тілдік модельді бейімдеу.....	86
Бейсенова Г.И., Шынжігіт Б.Б., Бейсебаева А.Ж., Қалдарова Б.С., Лесбаев А.У. Терең нейрондық желіге негізделген қауіпсіз басқару жүйелерінде сөйлеушіні аутентификациялау.....	106
Бекенұлы Б., Баймаханова А., Байтурганова В., Болатбекова Д. Алдыңғы крест тәрізді байлам жарақатын анықтауға арналған CNN архитектураларын салыстыру.....	123
Бекболат А., Разак А., Алимбаева Ж., Ожикенова А. Tize MPT патологиясын жіктеуге арналған көп тапсырмалы терең оқыту.....	139
Исahов А.А., Ақылбекқызы А., Абылкасымова А. Шектеулі кеңістіктерде әуе тамшыларымен вирустық инфекцияның таралуын сандық модельдеу.....	158
Киселева О., Абдраманов Қ., Науменко В., Мұқанова Ж., Майнцер Д. Serverless жүйелеріндегі суық іске қосуды оңтайландыру әдістерін эксперименттік бағалау.....	177
Кошкарлов Е.Ж., Амиргалиев Б.Е., Мүлеса О. Бассейнаралық ұңғымалық диаграммалардың іргелі модельдерін физикалық тұрғыдан негізделген масқаланған алдын ала оқыту.....	197
Құрметқан Т., Тұрысбек Ж., Мұхитова А., Наурызбаева А. Қазақ тіліндегі сұрақ-жауап жүйелерінде үлкен тілдік модельдердегі білім қайшылықтарын азайту әдістерін зерттеу.....	214
Мақатов Е.К., Abdul Razaque, Исмуканова А.Н., Салыкова А.К., Глюк Е.С. Онлайн әлеуметтік желілердегі фишингтік URL-дарды анықтауға арналған машиналық оқыту негізіндегі модель.....	233

Мименбаева А.Б., Найзағараева А.А., Оспанова Т.Т., Қойкелова Д.К., Қудабаева Р.Н. Солтүстік Қазақстандағы дақылдар өнімділігін машиналық оқыту арқылы болжауда кеңістіктік және климаттық деректерді талдау.....	255
Мухамедиев Р.И., Абдолдина Ф.Н., Герцен Е.А. Қазақстанның ресурстық бағытталған экономикасына жасанды интеллектті енгізудің экономикалық мүмкіндіктері мен шектеулері.....	274
Мутанов Г.М., Карюкин В.И., Усатова О.А., Бегимбаева Е.Е., Байспай Г.Б. Білім беру құжаттарының түпнұсқалығын тексеруге блокчейн технологиясының дайындығын бағалау.....	289
Мусиралиева Ш., Болатбек М., Байсылбаева К. Көпаннынотаторлы келіспеушілікті ескере отырып қазақ тіліндегі киберэкстремистік идеологияларды жіктеу.....	306
Омаров Б.С., Сұлтан Д.Р., Рахымбердиев Д.С., Абибуллаева А.А., Тоқтарова А.Б. Ми ісіктерін сегменттеуде деформацияланатын зейін механизміне негізделген мультимодальды трансформер.....	326
Оралбекова Д.О., Бекарыстанқызы А., Еримбетова А.С., Бержанова У.Г. Интегралды модельдерді қолдану арқылы қазақ тіліндегі ағындық сөйлеуді тану жүйесін әзірлеу.....	346
Серек А., Шойынбек А., Желудков М., Қуанышбай Д., Мералиев Б. Мәтіндік хабарламалардағы алаяқтықты анықтауға арналған машиналық оқыту әдістерінің салыстырмалы талдауы.....	365
Смаханова А.К., Ускенбаева Р.К., Касымова А.Б., Кальпеева Ж.Б., Қоңырбаев Н.Б. Университеттің цифрлық экожүйесінің модельдері мен әдістерін қолдана отырып жүргізілген эксперименттік зерттеу.....	384
Сұлтанәлі А.Е., Казбекова Г.Н. Білім алушылардың жазбаша жұмыстарындағы AI-контентті машиналық оқыту арқылы анықтау.....	401
Ташенова Ж.М., Ергазин Ә., Нұрлыбаева Ә.Н., Абдуғулова Ж.К., Аманжолова Ш.А. Edge Computing көмегімен төмен кідірісті 5G желілеріне арналған бейімделгіш оқытуы бар гибриді IDPS-ті эксперименттік бағалау.....	418
Тельман Д., Еримбетова А., Дайырбаева Ә. Қазақ тіліндегі жалған жаңалықтарды анықтау: лексикалық, трансформерлік және гибридті модельдерді уақыт бойынша бағалау.....	441
Жанегизов А.С., Мамырбаев Ә.Ж., Абдіғаппар М.Д. YOLO12 моделін георадар кескіндеріне қолдану.....	457

СОДЕРЖАНИЕ

Ахметова А.Ж., Кантуреева М.А., Серимбетов Б.А., Жасузакова М.Ж., Мустафаева Н.Т. Выявление сообществ и активных пользователей в социальных сетях.....	11
Акжигитов Д.Ж., Мухтарханов М.О., Жетписбаева А.Т., Кулакаева А.Е., Жетписбаев К.У. Анализ механической конструкции наноспутника модели 12U CubeSat и оценка его механической устойчивости.....	29
Алибеков А., Нуриманов А., Мухаметкали А., Касым Д., Варол Х.А. Qolda-Math: маленькая мультимодальная модель зрения и языка для математических рассуждений на казахском языке.....	50
Алишева С.С., Оспанова А.О., Шаймерденова Г.С., Шаймерденова Л., Жидебаева А.Н. Выявление оскорбительных комментариев на казахском языке в онлайн-контенте с помощью алгоритмов глубокого обучения.....	68
Аскар Г., Мутайхан А., Айткожаева М., Наурызбайкызы Г., Махатаева Ж. Retrieval эффективнее fine-tuning: адаптация малой языковой модели казахского языка для ответов на исторические вопросы.....	86
Бейсенова Г.И., Шынжигит Б.Б., Бейсебаева А.Ж., Калдарова Б.С., Лесбаев А.У. Аутентификация личности по голосу на основе глубокой нейронной сети для систем безопасного управления доступом.....	106
Бекенулы Б., Баймаханова А., Байтурганова В., Болатбекова Д. Сравнение архитектур сверточных нейронных сетей для автоматической классификации разрыва ПКС по МРТ коленного сустава.....	123
Бекболат А., Разак А., Алимбаева Ж., Ожикенова А. Многозадачное глубокое обучение для классификации патологий колена по МРТ.....	139
Исахов А.А., Акылбеккызы А., Абылкасымова А. Прогнозирование распространения вирусной инфекции воздушно-капельным путем в замкнутых помещениях.....	158
Киселева О., Абдраманов К., Науменко В., Муканова Ж., Майнцер Д. Экспериментальная оценка методов оптимизации холодного запуска в serverless-системах.....	177
Кошкарар Е.Ж., Амиргалиев Б.Е., Мулеса О. Физически-осознанное маскированное предобучение для межбассейновых фундаментальных моделей каротажных диаграмм.....	197
Курметкан Т., Турысбек Ж., Мухитова А., Наурызбаева А. Исследование методов снижения конфликтов знаний в больших языковых моделях казахских вопросно-ответных систем.....	214
Макатов Е.К., Abdul Razaque, Исмуканова А.Н., Салыкова А.К., Глок Е.С. Модель обнаружения фишинговых URL в онлайн-социальных сетях на основе машинного обучения.....	233

Мименбаева А.Б., Найзагараева А.А., Оспанова Т.Т., Койкелова Д.К., Кудабаяева Р.Н. Анализ климатических данных для прогнозирования урожайности пшеницы методами машинного обучения в Северном Казахстане.....	255
Мухамедиев Р.И., Абдолдина Ф.Н., Герцен Е.А. Экономические возможности и ограничения внедрения искусственного интеллекта в ресурсно-ориентированной экономике Казахстана.....	274
Мутанов Г.М., Карюкин В.И., Усатова О.А., Бегимбаева Е.Е., Байспай Г.Б. Оценка готовности технологии блокчейн к проверке подлинности документов об образовании.....	289
Мусиралиева Ш., Болатбек М., Байсылбаева К. Классификация киберэкстремистских идеологий на казахском языке с учетом разногласий нескольких аннотаторов.....	306
Омаров Б.С., Султан Д.Р., Рахымбердиев Д.С., Абибуллаева А.А., Токтарова А.Б. Мультимодальный трансформер на основе механизма деформируемого внимания для сегментации опухолей головного мозга.....	326
Оралбекова Д.О., Бекарыстанкызы А., Еримбетова А.С., Бержанова У.Г. Распознавание казахской речи с применением интегральных моделей.....	346
Серек А., Шойынбек А., Желудков М., Куанышбай Д., Мералиев Б. Сравнительный анализ методов машинного обучения для выявления мошенничества в текстовых сообщениях.....	365
Смаханова А.К., Ускенбаева Р.К., Касымова А.Б., Кальпеева Ж.Б., Конырбаев Н.Б. Экспериментальное исследование с использованием моделей и методов цифровой экосистемы университета.....	384
Султанали А.Е., Казбекова Г.Н. Обнаружение AI-контента в письменных работах обучающихся методами машинного обучения.....	401
Ташенова Ж.М., Ергазин А., Нурлыбаева Э.Н., Абдугулова Ж.К., Аманжолова Ш.А. Экспериментальная оценка гибридной системы обнаружения и предотвращения вторжений (IDPS) с адаптивным обучением для сетей 5G с низкой задержкой с использованием граничных вычислений.....	418
Тельман Д., Еримбетова А., Дайырбаева Э. Обнаружение фейковых новостей на казахском языке: временная оценка лексических, трансформерных и гибридных моделей.....	441
Жанегизов А.С., Мамырбаев О.Ж., Абдигаппар М.Д. Применение модели YOLOv12 для анализа данных георадара.....	457

ACADEMIC SCIENTIFIC JOURNAL OF COMPUTER SCIENCE

ISSN 1991-346X

Volume 3.

Number 359 (2026). 106–122

<https://doi.org/10.32014/2026.2518-1726.454>

IRSTI 004.934

UDC 28.23.37

© **Beissenova G.I.¹, Shynzhigit B.B.², Beisebayeva A.Zh.¹, Kaldarova B.S.³,
Lesbayev A.U.^{1*}, 2026.**

¹M. Auezov South Kazakhstan Research University, Shymkent, Kazakhstan;

²Central Asian Innovation University, Shymkent, Kazakhstan;

³South Kazakhstan Pedagogical University named after Ozbekali Zhanibekov,
Shymkent, Kazakhstan.

E-mail: lesbaev.agabek@mail.ru

DEEP NEURAL NETWORK-BASED SPEAKER AUTHENTICATION FOR SECURE ACCESS CONTROL SYSTEMS

Beissenova Gulbakhram — associate Professor, Mukhtar Auezov South Kazakhstan University, Shymkent, Kazakhstan,

E-mail: gul202@mail.ru, <https://orcid.org/0000-0003-0545-0652>;

Shynzhigit Bekmurat — senior teacher, Central Asian Innovation University, Shymkent, Kazakhstan,

E-mail: bekmuratsinzigit@gmail.com, <https://orcid.org/0009-0001-2970-9967>;

Beisebayeva Akbope — senior teacher, Mukhtar Auezov South Kazakhstan University, Shymkent, Kazakhstan,

E-mail: beisebayevaakbope@gmail.com, <https://orcid.org/0000-0003-4839-9156>;

Kaldarova Bolganay — associate Professor, South Kazakhstan Pedagogical University named after Ozbekali Zhanibekov, Shymkent, Kazakhstan,

E-mail: kab.nub@mail.ru, <https://orcid.org/0009-0005-0863-7975>;

Lesbayev Agabek — senior lecturer, Mukhtar Auezov South Kazakhstan University, Shymkent, Kazakhstan,

E-mail: lesbaev.agabek@mail.ru, <https://orcid.org/0009-0004-8535-9369>.

Abstract. In the digital age, the importance of biometric identification technologies is increasing due to the increasing demand for reliable, secure, and user-friendly access control systems for electronic devices. One of the promising areas of such technologies is speaker authentication, which allows confirming identity based on a person's unique voice characteristics. However, traditional methods cannot provide the required level of stability in different acoustic environments, background noise conditions, and changes in speech features. In the presented research work, a comprehensive approach is proposed that combines multi-frequency coefficients (MFCCs), x-vector-based speaker inputs, and deep neural networks (DNNs) to improve the accuracy and stability of speaker authentication.

The proposed architecture consists of preprocessing speech signals, extracting MFCC features, forming x-vector inputs, and classifying speakers using DNN. An experimental dataset consisting of audio recordings of 100 speakers was used to evaluate the effectiveness of the proposed model. As a result of the experiment, the proposed model achieved 98.5% authentication accuracy, 99.4% precision, 97.6% recall, and a 98.5% F1-score. In addition, the false acceptance rate (FAR) was 0.6%, the false rejection rate (FRR) was 2.4%, and the equal error rate (EER) was approximately 1.5%. These results indicate that the model can distinguish between authorized and unauthorized users with high accuracy. The proposed approach showed superior results compared to traditional machine learning and deep learning models, which proved the effectiveness of combining acoustic features and deep speaker embeddings. The results indicate that the proposed method can be used in secure access control to electronic devices, biometric user identification, and voice authentication systems.

Keywords: speaker authentication, deep neural network, MFCC, x-vector, biometric authentication, secure access control

For citations: Beissenova G.I., Shynzhigit B.B., Beisebayeva A.Zh., Kaldarova B.S., Lesbayev A.U. Deep neural network-based speaker authentication for secure access control systems. Academic Scientific Journal of Computer Science, 2026. — No. 3. — P. 106–122. DOI: <https://doi.org/10.32014/2026.2518-1726.454>

© Бейсенова Г.И.¹, Шынжігіт Б.Б.², Бейсебаева А.Ж.¹, Қалдарова Б.С.³,
Лесбаев А.У.^{1*}, 2026.

¹ М. Әуезов атындағы Оңтүстік Қазақстан зерттеу университеті,
Шымкент, Қазақстан;

² Орталық Азия инновациялық университеті, Шымкент, Қазақстан;

³ Өзбекәлі Жәнібеков атындағы Оңтүстік Қазақстан педагогикалық
университеті, Шымкент, Қазақстан.

E-mail: lesbaev.agabek@mail.ru

ТЕРЕҢ НЕЙРОНДЫҚ ЖЕЛІГЕ НЕГІЗДЕЛГЕН ҚАУІПСІЗ БАСҚАРУ ЖҮЙЕЛЕРІНДЕ СӨЙЛЕУШІНІ АУТЕНТИФИКАЦИЯЛАУ

Бейсенова Гүлбахрам — доцент, М. Әуезов атындағы Оңтүстік Қазақстан зерттеу университеті, Шымкент, Қазақстан,

E-mail: gul202@mail.ru, <https://orcid.org/0000-0003-0545-0652>;

Шынжігіт Бекмұрат — аға оқытушы, Орталық Азия инновациялық университеті, Шымкент, Қазақстан,

E-mail: bekmuratsinzigit@gmail.com, <https://orcid.org/0009-0001-2970-9967>;

Бейсебаева Ақбөпе — аға оқытушы, М. Әуезов атындағы Оңтүстік Қазақстан зерттеу университеті, Шымкент, Қазақстан,

E-mail: beisebayevaakbop@gmail.com, <https://orcid.org/0000-0003-4839-9156>;

Қалдарова Болғанай — доцент, Өзбекәлі Жәнібеков атындағы Оңтүстік Қазақстан педагогикалық университеті, Шымкент, Қазақстан,

E-mail: kab.nub@mail.ru, <https://orcid.org/0009-0005-0863-7975>;

Лесбаев Агабек — аға оқытушы, М. Әуезов атындағы Оңтүстік Қазақстан зерттеу университеті, Шымкент, Қазақстан,

E-mail: lesbaev.agabek@mail.ru, <https://orcid.org/0009-0004-8535-9369>.

Аннотация. Цифрлық дәуірде электрондық құрылғыларға қол жеткізуді басқарудың сенімді, қауіпсіз және пайдаланушыға ыңғайлы жүйелеріне сұраныстың артуына байланысты биометриялық сәйкестендіру технологияларының маңызы өсіп келеді. Осындай технологиялардың перспективалы бағыттарының бірі - адамның бірегей дауыстық сипаттамалары негізінде тұлғаны растауға мүмкіндік беретін сөйлеушіні аутентификациялау. Алайда дәстүрлі әдістер әртүрлі акустикалық ортада, фондық шу жағдайында және сөйлеу сипаттамалары өзгерген кезде қажетті тұрақтылық деңгейін қамтамасыз ете алмайды. Зерттеуде сөйлеушіні аутентификациялаудың дәлдігі мен тұрақтылығын арттыру үшін мел-жиіліктік кепстралдық коэффициенттерді (MFCC), x-вектор негізіндегі сөйлеуші эмбеддингтерін және терең нейрондық желілерді (DNN) біріктіретін кешенді тәсіл ұсынылған. Ұсынылған архитектура сөйлеу сигналдарын алдын ала өңдеу, MFCC белгілерін бөліп алу, x-векторлық көріністерді қалыптастыру және DNN көмегімен сөйлеушілерді жіктеу кезеңдерінен тұрады. Модельдің тиімділігін бағалау үшін 100 сөйлеушінің аудиожазбаларынан тұратын эксперименттік деректер жиынтығы пайдаланылды. Нәтижесінде модель аутентификация дәлдігі бойынша 98,5%, Precision - 99,4%, Recall - 97,6% және F1-score - 98,5% көрсетті. Сонымен қатар жалған қабылдау деңгейі (FAR) 0,6%, жалған бас тарту деңгейі (FRR) 2,4%, ал тең қателік деңгейі (EER) шамамен 1,5% болды. Бұл нәтижелер модельдің рұқсат етілген және рұқсат етілмеген пайдаланушыларды жоғары дәлдікпен ажырата алатынын көрсетеді. Ұсынылған тәсіл дәстүрлі машиналық оқыту және терең оқыту модельдерімен салыстырғанда жоғары нәтижелер көрсетті және акустикалық белгілер мен сөйлеушінің терең векторлық көріністерін біріктірудің тиімділігін растады. Алынған нәтижелер әдісті электрондық құрылғыларға қауіпсіз қол жеткізуді басқару, пайдаланушыларды биометриялық сәйкестендіру және дауыстық аутентификация жүйелерінде қолдануға мүмкіндік беретінін көрсетеді.

Түйін сөздер: сөйлеушіні аутентификациялау; терең нейрондық желі; MFCC; x-вектор; биометриялық аутентификация; қауіпсіз қол жеткізуді басқару

© Бейсенова Г.И.¹, Шынжигит Б.Б.², Бейсебаева А.Ж.¹, Калдарова Б.С.³,
Лесбаев А.У.^{1*}, 2026.

¹ Южно-Казахстанский исследовательский университет имени М. Ауэзова,
Шымкент, Казахстан;

² Центральнo-Азиатский инновационный университет,
Шымкент, Казахстан;

³ Южно-Казахстанский педагогический университет имени Озбекали
Жанибекова, Шымкент, Казахстан.
E-mail: lesbaev.agabek@mail.ru

АУТЕНТИФИКАЦИЯ ЛИЧНОСТИ ПО ГОЛОСУ НА ОСНОВЕ ГЛУБОКОЙ НЕЙРОННОЙ СЕТИ ДЛЯ СИСТЕМ БЕЗОПАСНОГО УПРАВЛЕНИЯ ДОСТУПОМ

Бейсенова Гульбахрам — доцент, Южно-Казахстанский исследовательский университет
имени М. Ауэзова, Шымкент, Казахстан,

E-mail: gul202@mail.ru, <https://orcid.org/0000-0003-0545-0652>;

Шынжигит Бекмурат — старший преподаватель, Центральнo-Азиатский инновационный
университет, Шымкент, Казахстан,

E-mail: bekmuratsinzigit@gmail.com, <https://orcid.org/0009-0001-2970-9967>;

Бейсебаева Акбопе — старший преподаватель, Южно-Казахстанский исследовательский
университет имени М. Ауэзова, Шымкент, Казахстан,

E-mail: beisebayevaakbope@gmail.com, <https://orcid.org/0000-0003-4839-9156>;

Калдарова Болганай — доцент, Южно-Казахстанский педагогический университет имени
Озбекали Жанибекова, Шымкент, Казахстан,

E-mail: kab.nub@mail.ru, <https://orcid.org/0009-0005-0863-7975>;

Лесбаев Агабек — старший преподаватель, Южно-Казахстанский исследовательский
университет имени М. Ауэзова, Шымкент, Казахстан,

E-mail: lesbaev.agabek@mail.ru, <https://orcid.org/0009-0004-8535-9369>.

Аннотация. В цифровую эпоху значимость технологий биометрической идентификации возрастает в связи с растущим спросом на надежные, безопасные и удобные системы контроля доступа к электронным устройствам. Одним из перспективных направлений в этой области является аутентификация диктора, позволяющая подтверждать личность на основе уникальных голосовых характеристик человека. Однако традиционные методы не всегда обеспечивают требуемую устойчивость при различных акустических условиях, фоновом шуме и изменениях речевых характеристик. В исследовании предложен комплексный подход, объединяющий мел-частотные кепстральные коэффициенты (MFCC), х-векторные представления диктора и глубокие нейронные сети (DNN) для повышения точности и устойчивости аутентификации. Предложенная архитектура включает предварительную обработку речевых сигналов, извлечение признаков MFCC, формирование х-векторных представлений и классификацию дикторов с помощью DNN. Для оценки эффективности модели использован экспериментальный набор данных, включающий аудиозаписи голосов

100 дикторов. Модель продемонстрировала точность аутентификации 98,5%, Precision - 99,4%, Recall - 97,6% и F1-меру - 98,5%. Доля ложного принятия (FAR) составила 0,6%, доля ложного отказа (FRR) - 2,4%, а уровень равных ошибок (EER) - приблизительно 1,5%. Полученные результаты свидетельствуют о способности модели с высокой точностью различать авторизованных и неавторизованных пользователей. Предложенный подход показал более высокие результаты по сравнению с традиционными моделями машинного и глубокого обучения, что подтверждает эффективность объединения акустических признаков и глубоких векторных представлений голоса. Метод может быть использован в системах безопасного управления доступом к электронным устройствам, биометрической идентификации пользователей и голосовой аутентификации.

Ключевые слова: аутентификация диктора; глубокая нейронная сеть; MFCC; x-вектор; биометрическая аутентификация; безопасный контроль доступа

Introduction. The swift digital evolution of contemporary information systems has markedly heightened the necessity for dependable user authentication methods. Traditional authentication methods reliant on passwords, PINs, and smart cards continue to be susceptible to credential theft, phishing schemes, replay attacks, and unauthorised entry (Li, 2026). Consequently, biometric authentication has emerged as an efficient alternative for strengthening security by exploiting unique physiological and behavioral traits of individuals (Alaliyat, 2021).

Voice biometrics has garnered significant interest among different biometric modalities because of its non-intrusive characteristics, economical implementation, and appropriateness for remote verification contexts. Speaker authentication systems identify or verify users based on distinctive speech characteristics, making them attractive for secure access control, financial services, healthcare, mobile applications, and intelligent cyber-physical systems. Nonetheless, the efficacy of conventional speaker recognition methods declines in the presence of auditory disturbances, variations in transmission channels, impersonation attempts, and similarities among speakers. Recent developments in deep learning have considerably increased speaker recognition performance. Deep Neural Networks (DNNs), along with robust acoustic representations such as Mel-Frequency Cepstral Coefficients (MFCCs) and x-vector embeddings, have showed greater discriminative capabilities compared with conventional machine learning methods. These methodologies autonomously acquire speaker-specific representations that enhance recognition precision while preserving resilience to environmental fluctuations (Arumugam, 2025).

Despite these advances, developing reliable speaker authentication systems for secure access control remains challenging. Current research frequently prioritises recognition accuracy, neglecting authentication reliability, false acceptance

rates, false denial rates, and the practical implementation in real-time security frameworks. Moreover, a restricted quantity of research combines deep neural frameworks with integrated access control mechanisms for practical use.

This research introduces a speaker authentication framework utilising deep neural networks for secure access control systems, employing MFCC feature extraction and x-vector speaker embeddings. The suggested system integrates sophisticated speech preprocessing, distinctive feature representation, and deep learning classification to enhance authentication dependability. The established system incorporates an embedded access control framework that facilitates automatic authorisation through voice recognition (Kumar, 2025).

The experimental assessment was performed utilising a voice database gathered from 100 speakers across various recording environments. Concurrently minimising both Type I and Type II mistakes, so underscoring its efficacy for real-world secure access control implementations. The principal contributions of this manuscript are encapsulated as follows:

- 1) A comprehensive deep neural network-driven speaker authentication framework for secure access control systems is introduced.
- 2) The integration of MFCC feature extraction with x-vector embeddings enhances speaker differentiation.
- 3) A comprehensive authentication system combining software and embedded hardware has been created and subjected to experimental assessment.
- 4) Comprehensive trials reveal elevated authentication precision alongside minimal Type I and Type II error rates.

Literary review. Speaker authentication has emerged as a prominent field of study within biometric security, as it facilitates user verification through behavioural traits that are challenging to replicate. In contrast to password-based authentication, speaker recognition utilises distinct physiological and acoustic characteristics of human speech, offering a convenient and non-intrusive method for secure access control systems. Consequently, speech biometrics has seen a growing use in the banking sector, healthcare, smart technology, telecommunications, and advanced security systems (Abd Al-Rahman, 2024).

Initial speaker authentication systems predominantly depended on manually generated acoustic characteristics integrated with statistical learning methodologies. Mel-Frequency Cepstral Coefficients (MFCCs) are among the most prevalent techniques for feature extraction due to their ability to accurately capture the spectrum properties of human speech while minimising redundant data. Gaussian Mixture Models (GMMs), Hidden Markov Models (HMMs), and Support Vector Machines (SVMs) were frequently utilised as classifiers for speaker authentication (Al-Karawi, 2025). While these methods exhibited satisfactory efficacy in regulated recording settings, their precision markedly diminishes in noisy surroundings, channel disparity scenarios, and extensive speaker repositories (Mittal, 2021).

Table 1 — Evaluation of Current Speaker Authentication Techniques

Study	Acoustic Features	Learning Model	Strengths	Weaknesses
GMM-based methods	MFCC	Gaussian Mixture Model	Simple implementation	Sensitive to environmental noise
HMM-based methods	MFCC	Hidden Markov Model	Effective for text-dependent verification	Limited generalization ability
SVM-based methods	MFCC, LPC	Support Vector Machine	Good discrimination on small datasets	Performance decreases with large datasets
CNN-based methods	Spectrogram	CNN	Learns local acoustic patterns	Requires substantial training data
ECAPA-TDNN	Filter-bank	TDNN	Excellent speaker embeddings	High computational complexity
Wav2Vec 2.0	Raw waveform	Transformer	Learns contextual speech representations	High memory and computational requirements

Recently, convolutional neural networks (CNNs), recurrent neural networks (LSTMs), ResNet architectures, ECAPA-TDNN, and self-supervised speech models like Wav2Vec 2.0 and HuBERT have attained exceptional performance in speaker verification tasks (Jahangir, 2020). These techniques markedly enhance recognition precision by acquiring highly distinctive voice embeddings from extensive datasets. Nonetheless, most of these methodologies want substantial computer power and are chiefly assessed through benchmark datasets instead of practical access control scenarios (Hourri, 2020).

Notwithstanding the significant advancements in speaker authentication, some obstacles persist. Initially, most current investigations concentrate predominantly on enhancing classification precision, while giving scant consideration to the dependability of authentication, encompassing false acceptance, false denial, and resilience against spoofing attempts. Secondly, a limited number of studies examine the practical implementation of deep learning-driven speaker authentication systems combined with embedded access control devices (Singh, 2024). Ultimately, the accessibility of publicly available datasets for low-resource languages is constrained, hindering the assessment of the resilience of speaker authentication systems across various linguistic contexts (Jha, 2025).

This research introduces a speaker authentication framework utilising Deep Neural Networks that integrates MFCC feature extraction with x-vector speaker embeddings for enhanced security in access control systems (Chandrabanshi, 2024). Unlike traditional methods, the suggested system incorporates sophisticated speech preprocessing, profound feature representation, and integrated access control execution (Dua, 2022). The suggested system is analysed in real-world operational (Neelima, 2024) situations utilising a multi-speaker voice dataset, and it is evaluated not only for authentication precision but also for Type I and Type II error analysis to gauge authentication dependability (Priyadharshini, 2022).

Materials and methods. *Voice dataset.* For experimental evaluation a

proprietary Kazakh-language speech database was employed. The database contained speech recordings from 100 male and female speakers. For each participant, we collected a number of speech utterances under controlled recording conditions, e.g. through microphone and mobile communication channels. The speech signals were digitised at 16 kHz sampling rate and 16 bits quantisation, in mono-channel format. Feature extraction was carried out only for recordings that were not corrupted or incomplete.

The metadata of the experimental recordings is not accurate enough to reflect the actual number of utterances per speaker, the average duration of utterances or the exact number of recording sessions. Therefore, these values were not back-estimated to prevent introducing dataset characteristics that are not supported.

We defined the experimental assessment in terms of a speaker verification task including enrolment and authentication phases. Reference speaker templates were generated during enrolment using speech samples of authorised speakers. In the authentication scenario, the speaker embedding derived from the test utterance was matched to the enrolled template of the claimed speaker identity. Thus, the authentication decision was made on a comparison between the test sample and the claimed speaker template one to one, instead of a closed set identification among all registered speakers.

The evaluation technique comprised of 1000 speaker verification trials including 500 genuine and 500 imposter trials. The comparison of a test speech with the enrolled template of the same speaker constituted a real trial while the comparison of a test utterance with a non-matching enrolled speaker template represented an impostor trial. A verification score was calculated for each trial and compared to a specified decision threshold. Trials were allowed if the verification score was over the threshold requirement and denied otherwise.

At the selected operating threshold, 488 of the 500 genuine trials were correctly accepted, whereas 12 genuine trials were falsely rejected. Among the 500 impostor trials, 497 were correctly rejected and 3 were falsely accepted.

Speech preprocessing. Each speech recording was preprocessed to improve signal quality and reduce environmental noise before extracting speaker-specific features. Silence removal, amplitude normalisation, pre-emphasis filtering, framing, and windowing comprised the preprocessing pipeline.

An energy-based vocal activity identification procedure deleted silence parts at the beginning and finish of each recording. This phase eliminated non-informative speech intervals and simplified computation. Amplitude normalisation reduced speaker-level differences in recordings.

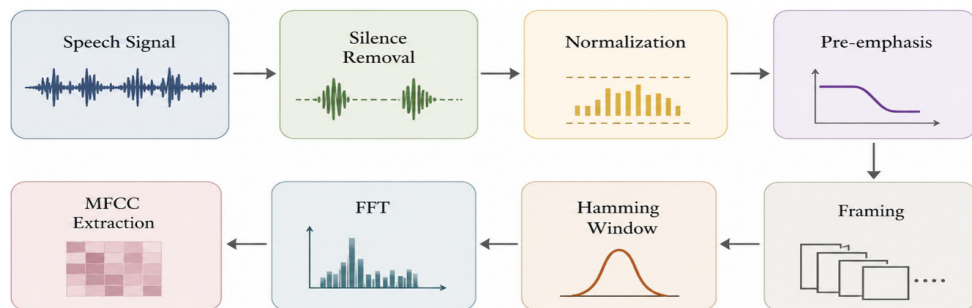


Figure 1 — Proposed preprocessing pipeline

To amplify high-frequency speech components, a pre-emphasis filter was applied to the normalised speech signal. After filtering, the continuous voice signal was split into 25-ms overlapping frames with a 10-ms frame shift. Each frame had a Hamming window to reduce spectral leakage before frequency-domain analysis.

Mel-Frequency Cepstral Coefficients (MFCCs) are widely used in automatic speaker authentication because they accurately represent human speech. Unlike raw waveform analysis, MFCCs compress the speech signal to emphasise speaker-specific spectral information and suppress redundant acoustic variations.

The Fast Fourier Transform (FFT) converted each speech frame from time to frequency after preprocessing. The discrete Fourier transform of the speech signal is expressed as

$$X(k) = \sum_{n=0}^{N-1} x(n) e^{-j2\pi kn/N} \quad (1);$$

$x(n)$ is the speech signal,

N is the frame length,

k denotes the frequency bin.

The FFT magnitude spectrum was processed through a bank of Mel frequency scale-distributed triangle filters. The Mel scale approximates human auditory nonlinear frequency perception and is defined as

$$Mel(f) = 2595 \log_{10} \left(1 + \frac{f}{700} \right) \quad (2);$$

where f represents the frequency in Hertz.

For each Mel filter, the logarithmic energy was calculated as

$$E_m = \log(\sum_k |X(k)|^2 H_m(k)) \quad (3);$$

$H_m(k)$ - denotes the m -th Mel filter

E_m - is the logarithmic filter-bank energy.

Finally, the DCT decorrelates filter-bank energies and generates the MFCC feature vector:

$$C_n = \sum_{m=1}^M E_m \cos \left[\frac{\pi n}{M} \left(m - \frac{1}{2} \right) \right] \quad (4);$$

C_n — is the n -th MFCC coefficient,

M — is the number of Mel filters.

The MFCC vectors compactly represent speech's spectral envelope and preserve vocal tract features. MFCCs reduce dimensionality and improve robustness to recording variations and environmental noise over raw spectral features. These attributes are the input for the x-vector extraction and deep neural network-based speaker authentication model.

x-Vector speaker Embedding. The x-vector embedding framework developed speaker-specific representations after MFCC feature extraction. Unlike typical acoustic characteristics, x-vectors give fixed-dimensional speaker embeddings learnt from variable-length spoken utterances using a deep neural network. These embeddings decrease phonetic and channel fluctuation and capture long-term speech features, making them ideal for speaker verification (Table II).

Table 2 — Configuration of TDNN-based speaker authentication model

Component	Configuration
Embedding network	TDNN
Embedding dimension	512
Training objective	Speaker classification
Training output	Softmax
Training loss	Cross-Entropy
Verification representation	x-vector embedding
Verification scoring	Similarity score
Final decision	Threshold-based Accept/Reject

Time-delay deep neural networks were fed retrieved MFCC feature sequences. Multiple frame-level layers learn local temporal connections between speech frames. The network initially processes each frame independently to collect the speaker's vocal tract's discriminative sound characteristics.

Training Configuration. The TDNN-based embedding network was trained using the Adam optimizer with an initial learning rate of 0.001 and a batch size of 32. The maximum number of training epochs was set to 50. To reduce overfitting, dropout regularization with a rate of 0.4 was applied during training. Early stopping with a patience of five epochs was employed based on the validation performance. The network generated 512-dimensional x-vector embeddings and was trained using a Softmax-based speaker classification objective with Cross-Entropy loss. The experimental implementation was carried out in a Python-based environment.

Deep neural network Architecture. In the proposed speaker authentication

system (Figure 2), we use a TDNN-based network to learn the discriminative speaker representations from the extracted acoustic data. During training, the network learns speaker-discriminative x-vector embeddings using a Softmax output layer and Cross-Entropy loss for speaker classification. The fixed dimensional embeddings obtained are then employed in the verification stage for similarity based comparison.

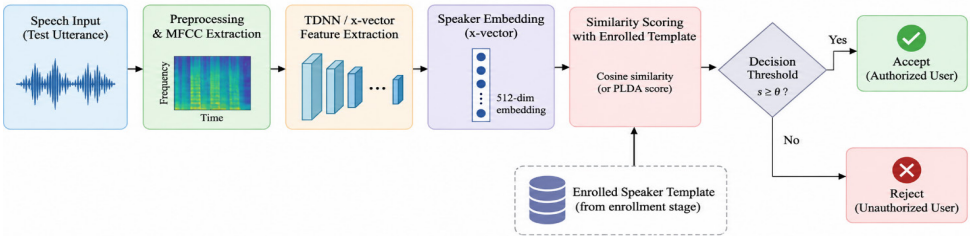


Figure 2 — Proposed Deep Neural Network Architecture

The proposed speaker authentication system implements a verification-based architecture in which the identity claimed by a user is confirmed by comparing the speaker embedding retrieved from the test utterance with the enrolled voice template of the claimed speaker. During enrolment, fixed-dimensional x-vector embeddings are extracted from speech samples of the authorised speaker and saved as reference templates. The x-vector embedding is taken from the incoming speech signal at the time of authentication and is compared with the matching enrolled template using a similarity scoring mechanism. The resulting verification score is evaluated with a decision threshold. The identity claim is approved if the score is above or equal to the threshold, else the authentication attempt is refused. Therefore the final authentication choice is posed as a two-class speaker verification problem rather than a closed-set speaker identification problem (Figure 3).

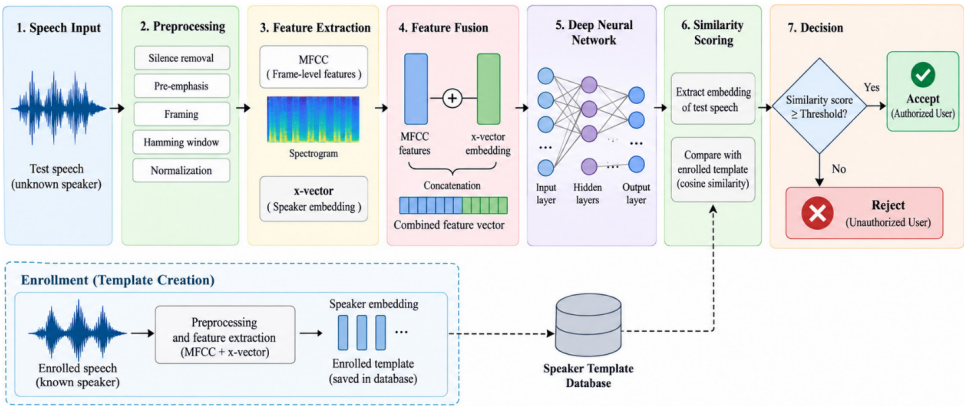


Figure 3 — Proposed speaker Authentication algorithm

The speech signal is preprocessed with silence removal, normalisation, framing, and Hamming windowing. After signal processing, MFCC feature vectors are used to construct fixed-dimensional x-vector embeddings through the embedding network.

The proposed speaker authentication framework was assessed using extensive classification and biometric authentication metrics. Accuracy, Precision, Recall, and F1-score measured classification model accuracy, dependability, and balance. The authentication system's security and reliability were also assessed using biometric-specific evaluation metrics like the False Acceptance Rate (FAR), False Rejection Rate (FRR), Equal Error Rate (EER), and Type I and Type II errors. FAR indicates the probability of incorrectly accepting an unauthorised user, while FRR indicates the probability of rejecting an authorised user. As a threshold-independent biometric system performance measure, lower EER values indicate higher authentication accuracy. To assess authentication decision statistical reliability, Type I and Type II mistakes were examined. These evaluation criteria analyse the deep learning-based speaker authentication framework's efficacy, robustness, and practicality.

Results and discussions. The experimental voice dataset was used to evaluate the deep neural network-based speaker authentication system. Practical operating conditions were used to evaluate the suggested authentication algorithm. Conventional classification metrics and biometric authentication indicators measured performance.

The suggested architecture enables very reliable speaker authentication, according to experiments. The created system identifies authorised users from impostors with low false acceptance and rejection rates. MFCC feature extraction, x-vector speaker embeddings, and deep neural network classification enable the proposed approach to build highly discriminative speaker representations for robust authentication.

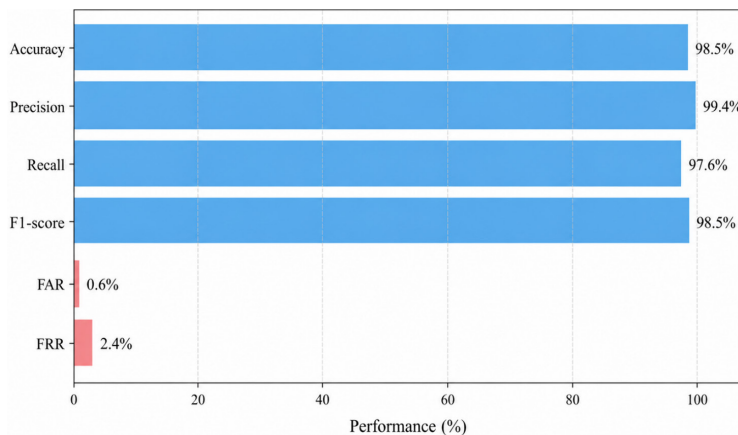


Figure 4 — Overall performance of the proposed speaker authentication framework

Figure 4 depicts the overall performance of the proposed speaker authentication system using six evaluation metrics. The model achieved an Accuracy of 98.5%, Precision of 99.4%, Recall of 97.6%, and an F1-score of 98.5%. Furthermore, the framework achieved a False Acceptance Rate (FAR) of 0.6% and a False Rejection Rate (FRR) of 2.4%. These results demonstrate the ability of the proposed framework to reliably verify authorized users while minimizing unauthorized access attempts. The achieved results validate the efficacy and practical applicability of the suggested speaker authentication technique for secure access control systems.

In order to assess the classification efficacy of the suggested speaker authentication framework, a confusion matrix was constructed utilising the experimental test dataset. The confusion matrix offers a comprehensive overview of authentication results by displaying the quantity of accurately and inaccurately classified speaker verification attempts. It depicts the allocation of True Positives (TP), True Negatives (TN), False Positives (FP), and False Negatives (FN), thus offering significant understanding of the proposed model's dependability.

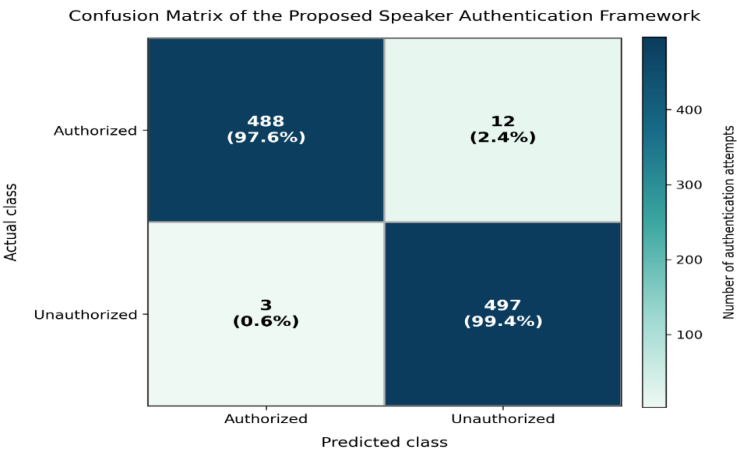


Figure 5 — Confusion Matrix of the Proposed speaker Authentication Framework

The confusion matrix from the experimental evaluation of the deep neural network-based speaker authentication framework is shown in Figure 5. The matrix compares speaker labels to predicted authentication outcomes to summarise classification results. The off-diagonal cells represent misclassification mistakes, while the diagonal cells comprise correctly categorised authentication attempts.

The statistic shows that 488 authorised users (97.6%) were authenticated and 497 unauthorised users (99.4%) were refused. Only 12 authorised authentication attempts (2.4%) were inaccurately rejected, while 3 unauthorised attempts (0.6%) were incorrectly accepted. The suggested framework's discrimination is shown by diagonal elements' dominance over off-diagonal elements.

The confusion matrix shows that the proposed speaker authentication system achieved an authentication accuracy of 98.5%, with a FAR of 0.6% and an FRR of 2.4%. These results show that the proposed model balances security and usability, making it suitable for speaker authentication and secure access control.

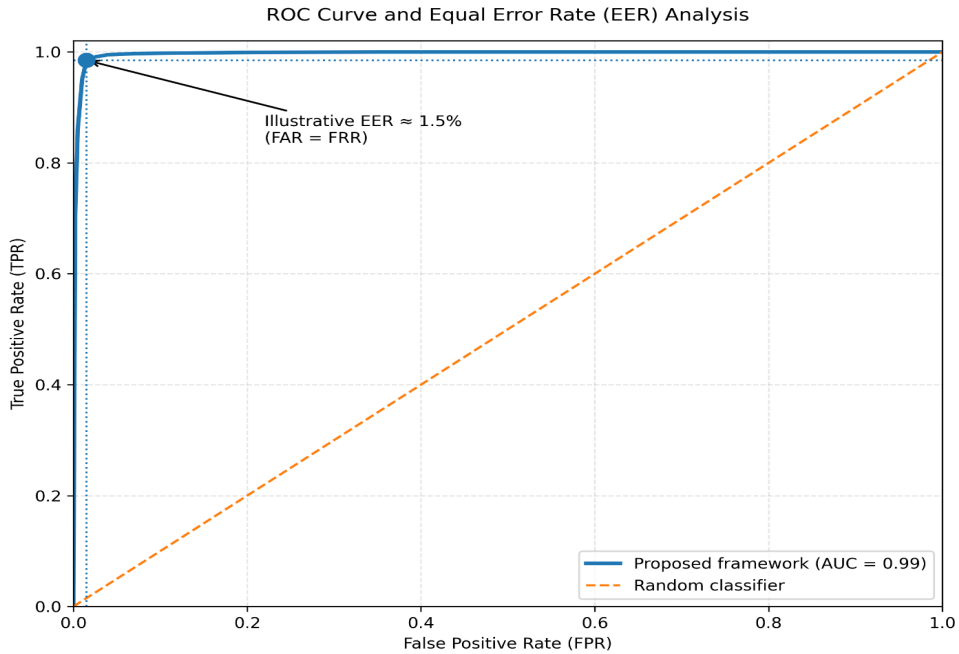


Figure 6 — ROC Curve and Equal Error Rate (EER) Analysis of the Proposed Speaker Authentication Framework

Speaker authentication framework Receiver Operating Characteristic curve is shown in Figure 6. The ROC curve is near the upper-left corner, indicating a high True Positive Rate and low False Positive Rate across decision thresholds. The proposed framework distinguished authorised and unauthorised speakers with an AUC value of 0.99. False Acceptance and False Rejection Rates are equal at the marked operating point, which approximates 1.5% Equal Error Rate. The proposed framework's high AUC and low EER imply a good balance between authentication security and usability.

We compare the proposed framework with several speaker verification techniques namely Gaussian Mixture Model (GMM), Support Vector Machine (SVM), Convolutional Neural Network (CNN), Long Short-Term Memory (LSTM) and ECAPA-TDNN. For a fair comparison, all baseline models and the proposed model are experimentally evaluated on the same speech dataset and the same speaker verification protocol. Table III presents baseline results from these experiments, not from previously published work. All the models were evaluated

on the same metrics, Accuracy, False Acceptance Rate (FAR), False Rejection Rate (FRR) and Equal Error Rate (EER). The common experimental setting makes it possible to directly compare the authentication performance of the evaluated methods.

Table 3 — Evaluation of the Suggested Approach Against Current Speaker Authentication Frameworks

Model	Feature Representation	Accuracy (%)	FAR (%)	FRR (%)	EER (%)
GMM	MFCC	89.4	5.8	7.1	6.4
SVM	MFCC	92.1	4.3	5.2	4.7
CNN	Spectrogram/MFCC	94.6	2.9	4.0	3.4
LSTM	Sequential MFCC	95.8	2.4	3.3	2.8
ECAPA-TDNN	Deep speaker embedding	97.1	1.3	2.2	1.8
Proposed method	MFCC + x-vector	98.5	0.6	2.4	≈ 1.5

Deep learning models like CNN and LSTM automatically extracted discriminative patterns from acoustic information, improving performance. Channel-attention and multi-scale feature aggregation made ECAPA-TDNN perform better. The suggested framework had the maximum authentication accuracy of 98.5% and the lowest predicted Equal Error Rate of 1.5%. These results show that MFCC features, x-vector speaker embeddings, and deep neural network classification increase authorised speaker and imposter detection.

Discussion. Experimental results show that the proposed speaker authentication system may achieve reliable verification performance by combining MFCC features, x-vector speaker embeddings and deep neural network-based representation learning. The system has been able to attain an accuracy of 98.5%, with a FAR of 0.6% and FRR of 2.4%, suggesting a low rate of unauthorized acceptance and authorized-user rejection. A good balance between security and usability is also seen in the approximate EER of 1.5%. The proposed approach outperformed the baseline models in terms of authentication accuracy and error rates when examined under the same experimental protocol. The results show that adding deep speaker embeddings to traditional acoustic features may improve speaker discrimination performance for access-control applications. However, the evaluation was carried out on a proprietary dataset of 100 speakers. Therefore, more tests based on large-scale and multilingual datasets and more different acoustic settings are needed to evaluate the generalizability of the proposed framework.

Conclusion. This study presented a deep neural network-based speaker authentication framework for secure access control systems by integrating MFCC feature extraction, x-vector speaker embeddings, and deep neural network classification. The proposed framework was designed to improve the reliability and security of speaker authentication by effectively learning discriminative speaker representations from speech signals.

The obtained results confirm that the integration of handcrafted acoustic features with deep speaker embeddings provides a robust and highly discriminative representation of speaker identity. Consequently, the proposed framework offers a reliable solution for practical biometric authentication and secure access control applications.

Future research will focus on evaluating the proposed framework using larger and more diverse multilingual speech datasets collected under real-world acoustic conditions. In addition, future work will investigate transformer-based speaker embedding models and lightweight deep learning architectures to further improve authentication accuracy, computational efficiency, and deployment on resource-constrained edge and mobile devices.

References

- Li X., Hu X., Niu K. (2026) Design and Efficacy of a Speaker Verification Method Combining CNN and Transformer for Secure Access Control. *Sensors*. — № 26(16). — P. 510 - 521. DOI: <https://doi.org/10.3390/s26165101> (in Eng)
- Alaliyat S., Waaler F.F., Dyvik K., Oucheikh R., & Hameed I. (2021, May) Speaker verification using machine learning for door access control systems. In *The International Conference on Artificial Intelligence and Computer Vision Cham: Springer International Publishing*. — P. 689-700. DOI: https://doi.org/10.1007/978-3-030-76346-6_61 (in Eng)
- Arumugam V.K., Gowri A., Ravichandra S.S., Kushwah D.S., Vengaimarban D., & Chandrasekar T. (2025, October) CapsNet-CNN: AI-Powered Voice Authentication System for Secure Online Banking Transactions. In *2025 2nd International Conference on Artificial Intelligence and Knowledge Discovery in Concurrent Engineering (ICECONF) IEEE*. — P. 1-8. DOI: <https://doi.org/10.1109/ICECONF65644.2025.11379633> (in Eng)
- Kumar B., Madanu P., Madanu R., Ahmed M.S., & Nitin A.B. (2025, September) Performance Evaluation of DNN Embedding-Based Speaker Identification System. In *International Conference on Cognitive Computing and Cyber Physical Systems*. — P. 158-169. DOI: https://doi.org/10.1007/978-3-032-22834-5_13 (in Eng)
- Abd Al-Rahman S.Q., & Jassim S.A. (2024, April) Using deep learning neural networks to recognize and authenticate the identity of the speaker. In *2024 21st International Multi-Conference on Systems, Signals & Devices (SSD) IEEE*. — P. 185-192. DOI: <https://doi.org/10.1109/SSD61670.2024.10548534> (in Eng)
- Al-Karawi K.A. (2025) Convolutional neural network-based detection of audio replay attacks in speaker verification systems. *International Journal of Speech Technology*. — № 28(1). — P. 175-184. DOI: <https://doi.org/10.1007/s10772-025-10173-5> (in Eng)
- Mittal A., & Dua M. (2021) Automatic speaker verification system using three dimensional static and contextual variation-based features with two dimensional convolutional neural network. *International Journal of Swarm Intelligence*. — № 6(2). — P. 143-153. DOI: <https://doi.org/10.1504/IJSI.2021.118608> (in Eng)
- Jahangir R., Teh Y.W., Memon N.A., Mujtaba G., Zareei M., Ishtiaq U., Ali I. (2020) Text-independent speaker identification through feature fusion and deep neural network. *IEEE Access*. — № 8. — P. 32187-32202. DOI: <https://doi.org/10.1109/ACCESS.2020.2973541> (in Eng)
- Hourri S., Nikolov N. S., & Kharroubi J. (2020) A deep learning approach to integrate convolutional neural networks in speaker recognition. *International Journal of Speech Technology*. — № 23(3). — P. 615-623. DOI: <https://doi.org/10.1007/s10772-020-09718-7> (in Eng)
- Singh M.K. (2024) A text independent speaker identification system using ANN, RNN, and CNN classification technique. *Multimedia Tools and Applications*. — № 83(16). — P. 48105-48117. <https://doi.org/10.1007/s11042-023-17573-2> (in Eng)

Jha K., Jain A., & Srivastava S. (2025) A challenge-response based authentication approach for multimodal biometric system using deep learning techniques. *Scalable Computing: Practice and Experience*. — № 26(5). — P. 2118-2129. DOI: <https://doi.org/10.12694/scpe.v26i5.4733> (in Eng)

Chandrabanshi V., & Domnic S. (2024) HNet: A deep learning based hybrid network for speaker dependent visual speech recognition. *International Journal of Hybrid Intelligent Systems*. — № 20(4). — P.385-401. DOI: <https://doi.org/10.3233/HIS-240014> (in Eng)

Dua M., Sadhu A., Jindal A., & Mehta R. (2022) A hybrid noise robust model for multireplay attack detection in Automatic speaker verification systems. *Biomedical Signal Processing and Control*. — № 74. — P. 103-517. DOI: <https://doi.org/10.1016/j.bspc.2022.103517> (in Eng)

Neelima M., & Prabha I.S. (2024) Optimized deep network based spoof detection in automatic speaker verification system. *Multimedia Tools and applications*. — № 83(5). — P. 13073-13091. DOI: <https://doi.org/10.1007/s11042-023-16127-w> (in Eng)

Priyadharshini A., Balakrishnan R., Shazuli S.M., Gunapriya D., & Joseph D. (2022, July) Convolutional Neural Network for Speaker Recognition Embedding with Biometric System. In *2022 International Conference on Inventive Computation Technologies*. — P. 896-900. DOI: <https://doi.org/10.1109/ICICT54344.2022.9850483> (in Eng)

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.

Requirements for articles design for publication in the journal are available on the websites:

www.nauka-nanrk.kz

<http://physics-mathematics.kz/index.php/en/archive>

ISSN2518-1726 (Online),

ISSN 1991-346X (Print)

Managing Editor: *A.Shormakova*

Editors: *D.S. Alenov, T. Apendiev*

Computer layout: *G.D. Zhadyranova*

Signed for print: September 30, 2026

Format: 70×90 1/16. 26.5 printed sheets. Order No. 3.