

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 Жұмаіл 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 Галимканр 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., Aitkozhasyeva 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
Исахов 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
Кошкарров 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., Құдабаева 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., Абдуғұлова 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., Кудабаева 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). 418–440

<https://doi.org/10.32014/2026.2518-1726.471>

IRSTI 27.47.19

UDC 512.647

© **Tashenova Zh.^{1*}, Yergazin A.¹, Nurlybaeva E.², Abdugulova Zh.¹,
Amanzholova Sh.³, 2026.**

¹L.N. Gumilyov Eurasian National University, Astana, Kazakhstan;

²Kazakh National Academy of Arts named after T. Zhurgenova,
Almaty, Kazakhstan;

³Kurmangazy Kazakh National Conservatory, Almaty, Kazakhstan.

E-mail: zhuldyz_tm@mail.ru

EXPERIMENTAL EVALUATION OF A HYBRID IDPS WITH ADAPTIVE LEARNING FOR LOW-LATENCY 5G NETWORKS USING EDGE COMPUTING

Tashenova Zhuldyz — PhD, associate professor L.N. Gumilyov Eurasian National University, Astana, Kazakhstan,

E-mail: zhuldyz_tm@mail.ru, <https://orcid.org/0000-0003-3051-1605>;

Yergazin Adil — Master, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan,

E-mail: anchorite.exe@gmail.com, <https://orcid.org/0009-0001-6284-7210>;

Nurlybaeva Elmira — PhD, The Kazakh National Academy of Arts named after T. Zhurgenova, Almaty, Kazakhstan,

E-mail: nuremek@mail.ru, <https://orcid.org/0000-0003-3051-1605>;

Abdugulova Zhanat — Associate professor, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan,

E-mail: janat_6767@mail.ru, <https://orcid.org/0000-0001-7462-4623>;

Amanzholova Shirin — PhD, Kurmangazy Kazakh National Conservatory, Almaty, Kazakhstan,

E-mail: sh.amanzholova@gmail.com; [https:// orcid.org/0000-0002-6674-2766](https://orcid.org/0000-0002-6674-2766).

Abstract. The rapid deployment of fifth-generation (5G) networks introduces novel security challenges due to ultra-low latency requirements, heterogeneous device environments, and distributed edge computing architectures. Traditional intrusion detection systems (IDS) are insufficient to address dynamic and evolving cyber threats in such environments. This study presents an experimental evaluation of a hybrid Intrusion Detection and Prevention System (IDPS) integrating signature-based detection with adaptive machine learning-based anomaly detection deployed in an edge computing framework. The system is evaluated across five 5G-oriented environments: 5G-enabled MANET, 5G mMTC (IoT), Heterogeneous 5G, 5G NSA (LTE-A), and SDN-enabled 5G. Isolation Forest is implemented as a lightweight unsupervised anomaly detection model. Experimental results

demonstrate improved detection accuracy, reduced false positive rate, scalable performance under increasing traffic load, and minimal response latency suitable for low-latency 5G applications. The proposed hybrid IDPS provides an effective and practical security mechanism for modern 5G infrastructures. The proposed system combines deterministic signature-based detection with an uncontrolled Isolation Forest anomaly detection model to eliminate known and previously unseen threats. The results of the study confirm that lightly uncontrolled anomaly detection models such as Isolation Forest can be effectively integrated into Edge architectures without excessive computational costs. By combining rule-based and anomaly-based mechanisms, hybrid IDPS detection provides a balanced compromise between coverage, response speed, and resource efficiency.

Keywords: 5G security; hybrid idps; anomaly detection; edge computing; intrusion detection; adaptive learning; isolation forest; low-latency networks

For citations: 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. Academic Scientific Journal of Computer Science, 2026. — No. 3. — P. 418–440. DOI: <https://doi.org/10.32014/2026.2518-1726.471>

© Ташенова Ж.М.^{1*}, Ерғазин Ә.¹, Нұрлыбаева Э.Н.², Абдугулова Ж.К.¹,
Аманжолова Ш.А.³, 2026.

¹ Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан;

² Т. Жүргенов атындағы Қазақ ұлттық өнер академиясы, Алматы, Қазақстан;

³ Құрманғазы атындағы Қазақ ұлттық консерваториясы, Алматы, Қазақстан.

E-mail: zhuldyz_tm@mail.ru

EDGE COMPUTING КӨМЕГІМЕН ТӨМЕН КІДІРІСТІ 5G ЖЕЛІЛЕРІНЕ АРНАЛҒАН БЕЙІМДЕЛГІШ ОҚЫТУЫ БАР ГИБРИДТІ IDPS-ТІ ЭКСПЕРИМЕНТТІК БАҒАЛАУ

Ташенова Жұлдыз — PhD, қауымдастырылған профессор, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан,

E-mail: zhuldyz_tm@mail.ru, ORCID: <https://orcid.org/0000-0003-3051-1605>;

Ерғазин Әділ — магистр, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан,

E-mail: anchorite.exe@gmail.com, <https://orcid.org/0009-0001-6284-7210>;

Нұрлыбаева Эльмира — PhD, Т. Жүргенов атындағы Қазақ ұлттық өнер академиясы, Алматы, Қазақстан,

E-mail: nuremek@mail.ru, <https://orcid.org/0000-0003-3051-1605>;

Абдугулова Жанат — қауымдастырылған профессор, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан,

E-mail: janat_6767@mail.ru, ORCID: <https://orcid.org/0000-0001-7462-4623>;

Аманжолова Ширин — PhD, Құрманғазы атындағы Қазақ ұлттық консерваториясы, Алматы, Қазақстан,

E-mail: sh.amanzholova@gmail.com, ORCID: <https://orcid.org/0000-0002-6674-2766>.

Аннотация. Бесінші буын (5G) желілерінің қарқынды енгізілуі аса төмен кідіріс талаптарына, гетерогенді құрылғылар ортасына және таратылған шеткі есептеу архитектураларына байланысты жаңа киберқауіпсіздік мәселелерін туындатады. Дәстүрлі енуді анықтау жүйелері (IDS) мұндай ортадағы динамикалық және үнемі өзгеріп отыратын киберқауіптерге қарсы әрекет ету үшін жеткіліксіз болуы мүмкін. Зерттеуде шеткі есептеу инфрақұрылымында сигнатураға негізделген анықтауды бейімделгіш машиналық оқытуға негізделген аномалияларды анықтау әдісімен біріктіретін гибриді енуді анықтау және алдын алу жүйесінің (IDPS) эксперименттік бағалауы ұсынылады. Жүйе 5G технологиясына бағдарланған бес ортада бағаланды: 5G қолдайтын MANET, 5G mMTC (IoT), гетерогенді 5G, 5G NSA (LTE-A) және SDN қолдайтын 5G. Isolation Forest жеңіл әрі мұғалімсіз оқытуға негізделген аномалияларды анықтау моделі ретінде қолданылды. Эксперименттік нәтижелер анықтау дәлдігінің жоғарылағанын, жалған оң нәтижелер үлесінің төмендегенін, трафик жүктемесі өскен кезде масштабталатын өнімділікті және кідірісі төмен 5G қолданбаларына сәйкес келетін қысқа жауап беру уақытын көрсетті. Ұсынылған гибриді IDPS белгілі және бұрын кездеспеген қауіптерді анықтау үшін детерминирленген сигнатуралық анықтауды Isolation Forest негізіндегі мұғалімсіз аномалияларды анықтаумен біріктіреді. Зерттеу нәтижелері Isolation Forest сияқты жеңіл аномалияларды анықтау модельдерін шамадан тыс есептеу шығындарынсыз шеткі есептеу архитектураларына тиімді енгізуге болатынын көрсетеді. Ережелерге негізделген және аномалияларға негізделген механизмдерді біріктіру арқылы ұсынылған гибриді IDPS анықтау қамтуы, жауап беру жылдамдығы және есептеу ресурстарын пайдалану тиімділігі арасында теңгерімді қамтамасыз етеді және заманауи 5G инфрақұрылымдары үшін практикалық қауіпсіздік тетігін қалыптастырады.

Түйін сөздер: 5G қауіпсіздігі; гибриді IDPS; аномалияларды анықтау; шеткі есептеулер; енуді анықтау; бейімделгіш оқыту; Isolation Forest; төмен кідірісті желілер

© Ташенова Ж.М.^{1*}, Ергазин А.¹, Нурлыбаева Э.Н.², Абдугулова Ж.К.¹,
Аманжолова Ш.А.³, 2026.

¹ Евразийский национальный университет имени Л.Н. Гумилёва,
Астана, Казахстан;

² Казахская национальная академия искусств имени Т. Жургенова,
Алматы, Казахстан;

³ Казахская национальная консерватория имени Курмангазы,
Алматы, Казахстан.

E-mail: zhuldyz_tm@mail.ru

ЭКСПЕРИМЕНТАЛЬНАЯ ОЦЕНКА ГИБРИДНОЙ СИСТЕМЫ ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ (IDPS) С АДАПТИВНЫМ ОБУЧЕНИЕМ ДЛЯ СЕТЕЙ 5G С НИЗКОЙ ЗАДЕРЖКОЙ С ИСПОЛЬЗОВАНИЕМ ГРАНИЧНЫХ ВЫЧИСЛЕНИЙ

Ташенова Жулдыз — PhD, ассоциированный профессор, Евразийский национальный университет имени Л.Н. Гумилёва, Астана, Казахстан,

E-mail: zhuldyz_tm@mail.ru, ORCID: <https://orcid.org/0000-0003-3051-1605>;

Ергазин Адил — магистр, Евразийский национальный университет имени Л.Н. Гумилёва, Астана, Казахстан,

E-mail: anchorite.exe@gmail.com, <https://orcid.org/0009-0001-6284-7210>;

Нурлыбаева Эльмира — PhD, Казахская национальная академия искусств имени Т. Жургенова, Алматы, Казахстан,

E-mail: nuremek@mail.ru, <https://orcid.org/0000-0003-3051-1605>;

Абдугулова Жанат — ассоциированный профессор, Евразийский национальный университет имени Л.Н. Гумилёва, Астана, Казахстан,

E-mail: janat_6767@mail.ru, ORCID: <https://orcid.org/0000-0001-7462-4623>;

Аманжолова Ширин — PhD, Казахская национальная консерватория имени Курмангазы, Алматы, Казахстан,

E-mail: sh.amanzholova@gmail.com, ORCID: <https://orcid.org/0000-0002-6674-2766>.

Аннотация. Быстрое развертывание сетей пятого поколения (5G) создает новые вызовы в области безопасности, обусловленные требованиями к сверхнизкой задержке, гетерогенной средой устройств и распределенными архитектурами граничных вычислений. Традиционные системы обнаружения вторжений (IDS) могут быть недостаточно эффективны для противодействия динамичным и постоянно развивающимся киберугрозам в подобных средах. В исследовании представлена экспериментальная оценка гибридной системы обнаружения и предотвращения вторжений (IDPS), объединяющей сигнатурное обнаружение с адаптивным машинным обучением для выявления аномалий в инфраструктуре граничных вычислений. Система оценивалась в пяти средах, ориентированных на 5G: MANET с поддержкой 5G, 5G mMTC (IoT), гетерогенной 5G-сети, 5G NSA (LTE-A) и 5G с поддержкой SDN. В качестве легковесной модели обнаружения аномалий без учителя применялся Isolation Forest. Экспериментальные результаты продемонстрировали повышение точности обнаружения, снижение частоты

ложноположительных срабатываний, масштабируемую производительность при увеличении трафиковой нагрузки и минимальную задержку ответа, соответствующую требованиям приложений 5G с низкой задержкой. Предложенная гибридная IDPS сочетает детерминированное сигнатурное обнаружение с основанным на Isolation Forest выявлением аномалий без учителя, что позволяет обнаруживать как известные, так и ранее не наблюдавшиеся угрозы. Результаты показывают, что легковесные модели обнаружения аномалий без учителя, такие как Isolation Forest, могут эффективно интегрироваться в архитектуры граничных вычислений без чрезмерных вычислительных затрат. Совмещение механизмов на основе правил и методов обнаружения аномалий обеспечивает сбалансированное соотношение между полнотой обнаружения, скоростью реагирования и эффективностью использования ресурсов, формируя практический механизм защиты современных 5G-инфраструктур.

Ключевые слова: безопасность 5G; гибридная IDPS; обнаружение аномалий; граничные вычисления; обнаружение вторжений; адаптивное обучение; Isolation Forest; сети с низкой задержкой

Кіріспе. 5G байланыс желілерінің эволюциясы өткізу қабілеттілігін, қосылу тығыздығын және аса сенімді төмен кідіріспен байланысты (URLLC) айтарлықтай жақсартады. Дегенмен, 5G-нің таратылған және гетерогенді архитектурасы күрделі киберқауіпсіздік мәселелерін тудырады (3GPP. Security Architecture and Procedures for 5G System (5GS) et al., 2023). Алдыңғы буындардан айырмашылығы, 5G желіні кесуді, мобильді жиек есептеулерін (MEC), бағдарламалық жасақтамамен анықталған желіні (SDN) және жаппай машиналық типтегі байланысты (mMTC) біріктіреді, бұл шабуыл беті мен жүйенің күрделілігін арттырады (National Institute of Standards and Technology (NIST) et al., 2026).

3GPP TS 33.501 стандартында анықталған 5G негізгі архитектурасы қауіпсіздік процедураларын белгілейді, бірақ таратылған қызмет көрсетуден бас тарту (DDoS), спуфинг, маршруттау шабуылдары және кесіндіге тән енулер сияқты динамикалық қауіптерді жоймайды (3GPP. Security Architecture and Procedures for 5G System (5GS) et al., 2023). Зерттеулер дәстүрлі орталықтандырылған енуді анықтау жүйелері 5G желілерінің кідіріс және масштабталу шектеулеріне сәйкес келе алмайтынын көрсетеді (European Telecommunications Standards Institute (ETSI) et al., 2022).

Жақында жүргізілген зерттеулер қолтаңбаға негізделген және аномалияға негізделген механизмдерді біріктіретін гибриді анықтау тәсілдерінің қажеттілігін атап көрсетеді (Rodriguez, C.A. et al., 2022). Сигнаттық жүйелер белгілі қауіптерді жылдам анықтауды қамтамасыз етеді, ал аномалияны анықтау нөлдік күндік және дамып келе жатқан шабуылдарды анықтауды қолдайды. Isolation Forest, автокодерлер және терең нейрондық желілер сияқты машиналық оқыту әдістері 5G шабуылын анықтау контексттерінде жоғары

өнімділік көрсетті (Imambayev, A. et al., 2022). Бақыланбайтын аномалияны анықтау әдістерінің ішінде Isolation Forest таңдалды, себебі ол белгіленген шабуыл деректерін қажет етпейді және кідіріске сезімтал орналастыруларда жоғары көлемді телеметрияны өңдеу үшін есептеу жағынан жеңіл болып қалады. Бұл таңдау жақында жүргізілген 5G шабуылын анықтау зерттеулеріне және операциялық желілерде тиімділік пен нақты уақыттағы қолданылуына баса назар аударатын ағынға негізделген мүмкіндіктерді алу құбырларына сәйкес келеді (Hussain, R. et al., 2021).

Негізгі назар төмен кідірістері 5G шеткі есептеу ортасында орналастырылған бейімделгіш оқытуы бар гибридті шабуылды анықтау және алдын алу жүйесінің (IDPS) өнімділігін, анықтау тиімділігін және нақты уақыттағы жауап беруін эксперименталды түрде бағалауға аударылды.

Бұл зерттеу төмен кідірістері 5G талаптарын қанағаттандыру үшін шеткі есептеу ортасында орналастырылған гибридті IDPS-ті эксперименталды түрде бағалайды. Негізгі үлестерге мыналар кіреді:

- Қолтаңба мен ML негізіндегі анықтауды біріктіретін гибридті IDPS әзірлеу;
- Таратылған жиекке негізделген архитектурада орналастыру;
- Бес өкілдік 5G желілік ортасында бағалау;
- Дәлдіктің, масштабталудың және жауап беру жылдамдығының сандық талдауы.

Әдебиеттерге шолу. 5G желілерінің қауіпсіздігі парадигманың орталықтандырылған ұялы байланыс архитектурасынан таратылған, виртуалдандырылған және бөліктерге негізделген инфрақұрылымдарға ауысуына байланысты зерттеудің маңызды бағытына айналды. 3GPP қауіпсіздік архитектурасы (3GPP. Security Architecture and Procedures for 5G System (5GS) et al., 2023) 5G ядросы мен радио интерфейстерінде аутентификация, кілттерді басқару және қорғау процедураларын орнатады. Алайда, ол жұмыс уақытында динамикалық киберқауіптерді анықтауға толық жауап бермейді. Сол сияқты, NIST 5G киберқауіпсіздік жүйесі (National Institute of Standards and Technology (NIST) et al., 2026) архитектуралық қауіпсіздік принциптеріне баса назар аударады, бірақ операциялық бақылау мәселелерін мойындайды.

ENISA-ның қауіп-қатер ландшафтын талдауы (European Union Agency for Cybersecurity (ENISA) et al., 2026) 5G орналастыруларына тән көптеген осалдықтарды, соның ішінде кесінділердің дұрыс конфигурацияланбауын, шеткі түйіндердің экспозициясын және сигналдық жазықтықты пайдалануды анықтайды. Бұл есептер қауіпсіздіктің негізгі стандарттары болғанымен, жедел қорғаныс үшін адаптивті анықтау механизмдері қажет екенін көрсетеді.

Edge computing қосымша шабуыл беттерін енгізеді. ETSI MEC қауіпсіздік нұсқаулары (European Telecommunications Standards Institute (ETSI) et al., 2022) маңызды қосымшаларды орналастыратын таратылған шеткі түйіндерден туындайтын тәуекелдерді сипаттаңыз. Шеткі түйіндер деректерді

пайдаланушы жазықтығының жанында өңдейтіндіктен, олар тартымды нысандарға айналады. Сондықтан интрузияны анықтау механизмдері айтарлықтай кідіріссіз деректер көздеріне жақын жұмыс істеуі керек.

Деректер жиынтығы жеке куәліктерді бағалауда орталық рөл атқарады. TON_IoT деректер жинағы (Moustafa et al., 2020) және Edge-IoTset (Ferrag, M.A. et al., 2022) адаптивті аномалияны анықтауды бағалауға жарамды Шынайы телеметрия және IoT шабуыл деректерін қамтамасыз етеді. CSE-CIC-IDS2018 деректер жиынтығы (Sharafaldin et al., 2018) 5G-ге тән болмаса да, анықтау дәлдігін салыстыру үшін кеңінен қолданылады. Жақында 5G-NIDD деректер жинағы (Sharafaldin et al., 2018) 5G сымсыз орталарында түсірілген трафикті ұсынады, бұл 5G-ге тән интрузия деректер жиынындағы алшақтықты жояды. 5GAD деректер жиынтығы (Idaho National Laboratory, 2026) қол жетімді 5G ену көрсеткіштерін одан әрі кеңейтеді.

Машиналық оқыту жеке куәліктерді әзірлеуде басты орынға ие болды. Бук және басқалар (Bouke et al., 2024) 5g интрузиясын анықтау үшін ML модельдеріне эмпирикалық бағалау жүргізіп, ансамбль негізінде аномалияны анықтау бір модельді жіктеуіштерден асып түсетіндігін көрсетті. Имамбаев және басқалар (Imambayev et al., 2022) ұсынылған ML әдістері 5G негізгі орталарына арнайы бейімделген, бұл анықтау өнімділігі мен есептеу құны арасындағы айырмашылықты көрсетеді.

Zeek негізіндегі мүмкіндіктерді алу әдістері ағын негізіндегі аномалияны анықтаудың перспективалы нәтижелерін көрсетті (Rodriguez et al., 2022). Мұндай тәсілдер нақты уақыт режимінде салыстырмалы түрде төмен есептеу үстеме шығындарымен жіктеуге мүмкіндік береді, бұл желінің кідірісі төмен талаптарын қолдайды.

Желіні кесу ортасындағы қауіпсіздік қосымша күрделілікті енгізеді (Gao et al., 2024). Оқшаулауды және анықтаудың түйіршіктілігін жақсарту үшін тілімге тән ML үлгілері ұсынылды. Зерттеулер көрсеткендей, қауіпсіздік саясаты қозғалыс сипаттамалары мен үлгілеріне динамикалық түрде бейімделуі керек.

Пайдаланушы жазықтығының функциясын (UPF) бақылау да назар аударды. P4 - бағдарламаланатын UPF интрузиясын анықтау жауаптың кідірісін азайта отырып, тікелей деректер жазықтығында анықтауға мүмкіндік береді. Бұл URLLC өнімділігін сақтау үшін қауіпсіздік тетіктері трафик ағындарына жақын жұмыс істеуі керек деген қағидаға сәйкес келеді (Hussain et al., 2021).

Құпиялылықты және таратылған орналастыру шектеулерін жою үшін федералды оқыту тәсілдері зерттелді. Перспективалы болғанымен, федеративті тәсілдер кідіріске сезімтал қосымшаларға әсер етуі мүмкін қосымша үстемей байланыс шығындарын енгізеді. Федеративті оқыту, деректер жазықтығында бағдарламаланатын анықтау және физикалық деңгейдегі қауіпсіздік механизмдері 5G-ді қорғаудың күшті әлеуетін көрсеткенімен, бұл зерттеу іске асырудың орындылығына, қайталануына және төмен кідіріспен

операциялық орналастыруға басымдық беру үшін бөлінген дайындықсыз немесе физикалық деңгей бақылауынсыз қол қою аномалиясы бар озық гибриді мәжбүрлі қоныс аударушыларға әдейі назар аударады.

Дегенмен, бірнеше зерттеулер масштабтылық пен жауап беру уақытын бір уақытта өлшей отырып, бірнеше 5G шабыттандырылған желілік сценарийлерде толық интеграцияланған гибриді мәжбүрлі қоныс аударушыларды эксперименталды түрде бағалайды. Бұл олқылық қазіргі жұмысты ынталандырады.

Материалдар мен әдістер. Материалдар мен әдістер бөлімінде осы зерттеуде қолданылған эксперименттік құрылым, гибриді анықтау архитектурасы, машиналық оқыту конфигурациясы және бағалау әдіснамасы сипатталған. Жүйе ашықтық пен қайталанымдылықты қамтамасыз ету үшін ашықбастапқыкодбартехнологияларменқайталанатынконфигурацияларды қолдану арқылы жүзеге асырылды. Барлық бағдарламалық жасақтама компоненттері Python тілінде әзірленді және платформадан тәуелсіз орындауды қамтамасыз ету үшін Docker көмегімен контейнерленген орталарда орналастырылды. Гибриді IDPS прототипінің толық бастапқы коды, соның ішінде мүмкіндіктерді алу сценарийлері, Isolation Forestn енгізу, бағалау процедуралары және конфигурация файлдары сұраныс бойынша қолжетімді және жарияланғанға дейін қоғамдық репозиторийге сақтауға болады. Эксперименттік трафик сценарийлері қоғамдық құжатталған 5G қауіпсіздік қауіп модельдерімен үйлестірілген бақыланатын модельдеу орталарын пайдалану арқылы жасалды (European Telecommunications Standards Institute (ETSI), 2022).

TON_IoT, Edge-IIoTset, CSE-CIC-IDS2018, 5G-NIDD және 5GAD сияқты қоғамдық енуді анықтау деректер жиынтығы IDS бенчмаркингіне және модельді валидациялауға қолайлы кешенді белгіленген трафикті қамтамасыз етеді (Moustafa, N. et al., 2026). Дегенмен, ауқымды деректер жиынтықтары кідіріске сезімтал 5G орталарында шеткі есептеу шектеулерімен әрқашан сәйкес келмейтін айтарлықтай есептеу шығындары мен жад талаптарын тудыруы мүмкін. Сондықтан, бұл зерттеуде бес 5G-дан шабыттанған ортада (5G-қосылған MANET, 5G mMTC/IoT, гетерогенді 5G, 5G NSA және SDN-қосылған 5G) қоршаған ортаға тән қауіпсіз базалық терезелер мен қайталанатын шабуыл сценарийлерін жасау үшін бақыланатын Scaru негізіндегі трафикті генерациялауды қолдана отырып, Isolation Forestn оқыту жүргізілді. Модельдеуге негізделген трафикті генерациялау ұсақ түйіршікті хаттаманы манипуляциялауға және қайталанатын эксперименттік жағдайларға мүмкіндік береді, бұл жаңа 5G қауіпсіздік архитектураларында бақыланатын өнімділікті бағалау үшін маңызды. Жоғарыда аталған жалпы деректер жиынтықтары ұсынылған қабылдау құрылымымен үйлесімді болып қала береді және кеңейтілген оқыту және деректер жиынтықтарын валидациялау бойынша болашақ жұмыстарға енгізілуі мүмкін. Ұсынылған гибриді IDPS таратылған телеметрияны өңдеу, ағын деңгейіндегі

агрегация және нақты уақыт режиміндегі аномалияларды бағалауды қоса алғанда, 5G желілік принциптерін көрсететін модельденген шеткі есептеу архитектурасында орналастырылды. Эксперименттер шеткі орналастырудың нақты шектеулерін көрсету үшін GPU үдеуінсіз стандартты есептеу ортасында жүргізілді. Өнімділік өлшемдері өңдеу өткізу қабілетін, процессорды пайдалануды, жадты тұтынуды және анықтау кідірісін бағалау үшін жүйелік деңгейдегі мониторинг құралдарын пайдалану арқылы жиналды.

Бұл зерттеуде адам қатысушылары немесе тікелей эфирдегі өндіріс желісінің деректері пайдаланылған жоқ. Барлық эксперименттер бақыланатын модельдеу орталарында жүргізілді; сондықтан этикалық мақұлдау қажет болмады.

Генеративті жасанды интеллектке (GenAI) қатысты, жасанды интеллектке негізделген құралдар тек техникалық жобалауды қолдау және қолжазба мәтінін құрылымдауға көмектесу үшін пайдаланылды. Эксперименттік деректерді, статистикалық нәтижелерді немесе сандарды жасау үшін жасанды интеллект құралдары пайдаланылған жоқ. Барлық модельді енгізу, деректер жиынтығын өңдеу, бағалау көрсеткіштері және эксперименттік нәтижелер автормен қолмен жобаланған, орындалған және тексерілген.

Келесі бөлімдерде жүйе архитектурасы, эксперименттік орталар, машиналық оқыту тұжырымдамасы және бағалау әдіснамасы егжей-тегжейлі сипатталған.

2.1. Гибридті IDPS архитектурасы

Ұсынылған гибридті басып кіруді анықтау және алдын алу жүйесі (IDPS) төмен кідіріспен 5G орталарына арналған көп қабатты таратылған архитектураны ұстанады. Жүйе төрт негізгі компоненттен тұрады:

- Қолтаңбаға негізделген анықтау механизмі
- Isolation Forestның аномалиясын анықтау модулі
- Жиекке негізделген трафикті қабылдау және мүмкіндіктерді алу
- Орталықтандырылған көрсеткіштерді агрегациялау және бағалау модулі

2.1.1. Жиекке негізделген орналастыру

IDPS Mobile Edge Computing (MEC) қағидаттарымен үйлесетін жиек есептеу жүйесінде жұмыс істейді. Трафик телеметриясы анықтау кідірісін азайту және орталықтандырылған кедергілердің алдын алу үшін пайдаланушы жазықтығына немесе желі жиегіне жақын жерде түсіріледі.

Әрбір жиек түйіні келесі әрекеттерді орындайды:

- Ағынды алу (NetFlow/Zeek тәрізді)
- Сырғымалы терезе агрегациясы
- Функция векторын құру
- Жергілікті аномалияны бағалау

Бұл архитектура анықтау шешімдері үшін екі жаққа бару уақытын қысқартады, 5G-дегі өте сенімді төмен кідіріс байланысы (URLLC) шектеулерін қанағаттандырады.

2.1.2. Қолтаңбаға негізделген ереже қозғалтқышы

Қолтаңба модулі алдын ала анықталған шабуыл үлгілеріне қарсы детерминирленген сәйкестендіруді орындайды.

Әрбір e оқиғасы үшін ережеге негізделген анықтау келесідей анықталады:

$$R(e) = \begin{cases} 1, & \text{if event matches known attack signature} \\ 0, & \text{otherwise} \end{cases}$$

Мұндағы:

- $R(e) = 1$ белгілі шабуылды анықтауды білдіреді
- $R(e) = 0$ қолтаңбаға сәйкес келмейтінін білдіреді

Бұл модуль бұрын анықталған қауіптерді кідіріссіз анықтауды қамтамасыз етеді.

2.1.3. Аномалияны анықтау модулі (Isolation Forest)

Isolation Forest (OO) бақылаусыз сипаты мен есептеу тиімділігіне байланысты таңдалды, бұл оны шеткі орналастыруға жарамды етеді.

Алгоритм қалыпты әрекеті тікелей профильдеудің орнына аномалияларды окшаулайды.

$X = \{x_1, x_2, \dots, x_n\}$ деректер жиынтығы берілгенде, Isolation Forest кездейсоқ ағаштарды құрастырады.

x деректер нүктесі үшін оның аномалия ұпайы орташа жол ұзындығына негізделіп есептеледі:

$$h(x) = \frac{1}{t} \sum_{i=1}^t h_i(x)$$

Мұндағы:

$h(x) = i$ ағашындағы x жолының ұзындығы

Аномалия ұпайы келесідей анықталады:

$$s(x, n) = 2^{-\frac{h(x)}{c(n)}}$$

Мұндағы:

$$c(n) = 2H(n-1) - \frac{2(n-1)}{n}$$

және $H(i)$ гармоникалық сан:

$$H(i) = \ln(i) + \gamma$$

$\gamma \approx 0.577$ (Эйлер-Машерони тұрақтысы).

Түсіндірме:

- Егер $s(x, n) \approx 1 \Rightarrow$ ықтимал аномалия болса
- Егер $s(x, n) < 0.5 \Rightarrow$ ықтимал қалыпты болса

2.1.4. Гибридті шешім біріктіруі

Соңғы анықтау шешімі қолтаңба мен аномалияны анықтауды біріктіреді:

$$D(e) = \alpha R(e) + \beta A(e)$$

Мұндағы:

- $R(e)$ = ережеге негізделген шығыс
- $A(e)$ = аномалияға негізделген шығыс
- α, β = салмақ параметрлері

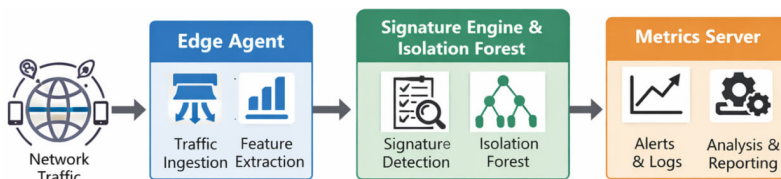
Бұл зерттеуде:

- $\alpha=0.5$
- $\beta=0.5$

Соңғы шешім:

Шабуыл егер $(e) > \tau$ болса

Мұндағы τ шешім шегі.



Сурет 1 — Гибридті IDPS архитектурасы.

1-сурет- шеткі есептеу ортасында орналастырылған ұсынылған гибридті IDPS архитектурасы. Трафиктік телеметрия шеткі түйіндерде қабылданады, қолтаңба және аномалияны анықтау модульдері арқылы өңделеді және бағалау және өнімділікті талдау үшін орталықтандырылған түрде жинақталады.

2.2. Эксперименттік орталар

Ұсынылған гибридті IDPS-тің беріктігі, масштабталуы және бейімделуін бағалау үшін бес өкілдік 5G желілік ортасы жасалды. Бұл орталар заманауи 5G орналастыруларына тән гетерогенді сәулеттік парадигмалар мен қауіп ландшафттарын көрсетеді. Әрбір орта соңғы әдебиеттерде құжатталған нақты трафик әрекетін, хаттама сипаттамаларын және шабуыл үлгілерін эмуляциялау үшін жасалған. Бағалау жүйесі зиянды оқиғалардың бақыланатын енгізілуін қамтамасыз етті, сонымен қатар оқыту және өнімділікті тексеру үшін базалық зиянсыз трафикті сақтады.

2.2.1. 5G қолдайтын MANET

5G қолдайтын мобильді Ad-hoc желісі (MANET) ортасы 5G жоғары байланысы бар виртуалдандырылған торлы маршруттау қабаты арқылы жұмыс істейтін орталықтандырылмаған, көп хопты маршруттау топологиясын модельдеді. Түйіндер орталықтандырылған инфрақұрылымға

сүйенбей трафикті динамикалық түрде бағыттады. Маршруттау әрекеті BATMAN тәрізді механизмдерге сәйкес келетін торлы хаттама абстракциясын пайдаланып жүзеге асырылды, бұл нақты көп хопты бағыттау динамикасын қамтамасыз етеді.

Бұл орта өзінің ішкі қауіпсіздік шектеулеріне байланысты таңдалды. Орталықтандырылған басқару механизмдерінің болмауы аутентификацияда, сенімді орнатуда және маршруттау тұтастығында қиындықтар туғызады. Әлсіз шифрлау конфигурациялары шектеулі құрылғы орталарын көрсету үшін әдейі эмуляцияланды. Сонымен қатар, орталықтандырылмаған басқару сәйкестікке негізделген және маршруттауға негізделген шабуылдарға сезімталдықты арттырады.

Келесі шабуыл санаттары модельденді:

- Sybil Attack-маршруттау шешімдерін манипуляциялау және сенім салмағын жасанды түрде арттыру үшін бірнеше жалған сәйкестіктер енгізілді;

- Қара тесік Шабуылы-Зиянды түйіндер маршруттаудың онтайлы жолдарын жарнамалады, бірақ ұсталған пакеттерді тастады;

- Жалған шабуыл-занды түйіндерді имитациялау және сенімді тексеруді айналып өту үшін Ір Және MAC Көздерін бұрмалау орындалды.

Бұл шабуылдар қолтаңбаға негізделген және аномалияға негізделген модульдер арқылы анықталатын аномальды маршруттау көрсеткіштерін, пакеттің түсу жылдамдығын және трафиктің асимметриясын тудырады.

2.2.2. 5g mMTC (заттар интернеті)

5g massive Machine-Type Communication (mMTC) ортасы Жоғары тығыздықтағы Интернет Заттарын орналастыру сценарийін ұсынды. Қозғалыс ағындары сенсорлық телеметрияны, жеңіл MQTT/CoAP байланысын және жарылысқа негізделген құрылғыны синхрондау әрекетін имитациялау үшін жасалды. Қоршаған орта ақылды қалалар мен Өнеркәсіптік Интернет Заттарына арналған Қосымшаларға тән шектеулі есептеу құрылғылары мен үзіліссіз байланыс үлгілеріне баса назар аударды.

Осалдықтың негізгі моделі мыналарға бағытталған:

- Әлсіз немесе статикалық аутентификация механизмдері;
- Ресурстардың шектеулілігіне байланысты шектеулі криптографиялық үстеме шығындар;

- Негізгі конфигурациядағы шифрланбаған телеметриялық арналар;

Келесі шабуылдар енгізілді:

- Таратылған қызмет көрсетуден бас тарту (DDoS) – агрегация шлюздеріне үлкен көлемдегі сұраныстарды су басу;

- Қайта ойнату шабуылдары-тексеру механизмдерін айналып өту үшін түсірілген аутентификация пакеттерін Қайта жіберу;

- Тыңдау-шифрланбаған телеметрия деректерін алу үшін пассивті трафикті түсіру.

Аномалияны анықтау компоненті бұл сценарийде трафиктің қалыптан

тыс жарылыстарына, энтропияның өзгеруіне және пакеттің уақытша таралуындағы ауытқуларға байланысты әсіресе тиімді болды.

2.2.3. Гетерогенді 5G

Гетерогенді 5G ортасы кеңейтілген мобильді кең жолақты (eMBB), ультра сенімді төмен кідіріс байланысын (URLLC) және mmTc сегменттерін қоса алғанда, бірнеше логикалық сегменттердегі аралас трафик ағындарын модельдеді. Трафиктің өзгергіштігі кідіріске сезімтал ағындарды, деректерді жаппай тасымалдауды және IoT тәрізді телеметрия ағындарын біріктіру арқылы енгізілді.

Гетерогенді 5G архитектуралық күрделілігі шабуыл бетін жоғарылатады:

- Көп қабатты протокол стектері
- Ресурстарды көлденең қималар бойынша бөлу
- Қызмет көрсету сапасының (QoS) әртүрлі параметрлері

Екі негізгі шабуыл сыныбы бағаланды:

– Ортадағы адам (MitM) – трафикті ұстап қалу және кесінділердің ауысуы кезінде пакеттің таңдамалы модификациясы.

– Деректерді өзгерту шабуылдары-тұтастықты анықтау мүмкіндігін тексеру үшін белсенді ағындар ішіндегі пайдалы жүктемені өзгерту.

Бұл шабуылдар ағын мөлшерінің үлестірілуіндегі статистикалық анықталатын ауытқуларға, уақыт үлгілеріне және бақылау сомасының сәйкессіздігіне әкелді.

2.2.4. 5G NSA (LTE-A)

5G Автономды емес ортасы (NSA) 5G пайдаланушы жазықтығының үдеуімен біріктірілген LTE-Advanced (LTE-A) басқару жазықтығының сигнализациясы негізінде модельденді. Бұл гибриді архитектура басқару сигнализациясы LTE инфрақұрылымында бекітілген күйінде қалатын өтпелі орналастыруларды көрсетеді.

Осы ортадағы негізгі осалдықтарға мыналар жатады:

- Бұрынғы LTE басқару-жазықтық шифрлауының әлсіз жақтары
- Тасымалдау кезінде сигнал беру протоколының экспозициясы
- EPS негізіндегі аутентификацияға тәуелділік

Шабуыл модельдеулеріне мыналар кірді:

– Тапсыру Шабуылдары-сеанстың үздіксіздігін бұзу үшін ұтқырлық туралы сигнал беретін хабарламаларды Манипуляциялау.

– Ұстау Шабуылдары-сәйкестендіру және сеанс ақпаратының ағып кетуін талдау үшін сигналдық пакеттерді Түсіру.

Бұл шабуыл үлгілері, ең алдымен, сигнал беру жиілігіне, күйдің ауысуына және аномалияны бағалау үлгісімен түсірілген пакеттік уақыт сипаттамаларына әсер етті.

2.2.5. SDN қосылған 5G

SDN қолдайтын 5g ортасы орталықтандырылған басқару архитектурасына еліктелді, мұнда бағыттау құрылғылары ережелерді тарату үшін логикалық орталықтандырылған SDN контроллеріне сүйенді. 5g негізгі желісінің шынайы әрекетін қайталау үшін ағын деңгейіндегі телеметрия бақыланды.

Бұл архитектура өзіне тән тәуекелдерді енгізеді:

- Орталықтандырылған шешім қабылдау
- Ашық басқару интерфейстері (Мысалы, OpenFlow тәрізді протоколдар)
- Контроллерге тәуелділік

Келесі шабуылдар жүзеге асырылды:

– Ағын Кестесімен Улану-трафикті қайта бағыттау үшін зиянды бағыттау ережелерін Енгізу.

– Контроллерге Қызмет көрсетуден бас тарту (DoS) – SDN контроллеріне бағытталған Жоғары жиілікті басқару сұраулары.

Бұл шабуылдар ағынды орнату жылдамдығында, контроллердің CPU жүктемесінде және пакеттерді жіберудегі сәйкессіздіктерде ауытқулар тудырды.

Әрбір орта әдебиеттерден алынған өкілдік осалдықтар мен шабуыл түрлерін модельдеді.

2.3. Машиналық оқыту моделі

Suricata signature қозғалтқышының ережелерге негізделген анықтау мүмкіндіктерін толықтыру үшін гибриді мәжбүрлі қоныс аударушылар архитектурасына аномалияға негізделген анықтау компоненті енгізілді. Бұл дизайн таңдауы 5g жүйелерінің дамып келе жатқан және гетерогенді қауіп ландшафтына негізделген, мұнда алдын ала анықталған қолтаңбаларға сәйкес келмейтін шабуылдар пайда болуы мүмкін және осылайша ережелерді сәйкестендіруден басқа әрекетінің ауытқуларын анықтауды қажет етеді. Ұсынылған архитектурада аномалияны анықтау Isolation Forest (IF) бақылаусыз модель ретінде қолдану арқылы жүзеге асырылады, ол қатерсіз телеметрияның бастапқы көрінісін зерттейді және аномалия ұпайларын уақыт терезелері бар қозғалыс ағындарында байқалатын ауытқуларға тағайындайды. Модель төмен кідіріс пен жиекке бағытталған операциялық талаптарға сәйкес келеді-5g / URLLC қауіпсіздік механизмдері өңдеудің қосымша кідірісін шектеуі керек, бұл телеметрияны жоғары жылдамдықпен қабылдауға жарамды есептеудің тиімді анықтау әдістерін ынталандырады. Сонымен қатар, практикалық бақылау құбырлары көбінесе ағындық/телеметриялық мүмкіндіктерді (мысалы, Zeek стиліндегі мүмкіндіктерді) алуға негізделгендіктен және барлық жағдайларда толық, жоғары сапалы белгілерді дәйекті түрде қамтамасыз етпеуі мүмкін болғандықтан, қатерсіз терезелерден бастапқы оқыту 5g-ге бағытталған бақылаудағы ауытқуларды анықтауға арналған қорғалған оқыту тәсілі болып табылады. Соңында, 5g-ге тән деректер жинақтары мен орталарды пайдалана отырып бағалау 5g

трафигінің сипаттамалары мен нақты шабуыл жағдайларында ML көмегімен анықтау үшін эмпирикалық негіздеуді қамтамасыз етеді (Siriwardhana et al., 2022).

2.3.1 Isolation Forest теориялық негіздері

Isolation Forest аномалиялар қалыпты бақылаулармен салыстырғанда "аз және әр түрлі" деген қағидаға негізделген. Деректердің қалыпты таралуын профильдеудің орнына, алгоритм мүмкіндіктер кеңістігін рекурсивті түрде бөлу арқылы ауытқуларды оқшаулайды.

$X = \{x_1, x_2, \dots, x_n\}$ деректер жиынын ескере отырып, Isolation Forest екілік ағаштар ансамбліні құрады (Isolation Forest немесе ағаштар деп аталады). Әрбір Isolation Forest салу кезінде алгоритм функцияны кездейсоқ таңдау арқылы жүзеге асырылады f кол жетімді мүмкіндіктер кеңістігінен. Бөлінген мән s содан кейін таңдалған мүмкіндіктің минималды және максималды мәндерімен анықталған ауқымда кездейсоқ таңдалады. Осы кездейсоқ таңдалған мүмкіндікті және бөлінген мәнді пайдаланып, деректер жиыны екі ішкі жиынға бөлінеді. Бұл бөлу процесі әрбір алынған ішкі жиынға рекурсивті түрде қолданылады. Рекурсивті бөлу екі тоқтату критерийінің бірі орындалғанға дейін жалғасады: бөлімде бір данасы болады немесе ағаштың алдын-ала анықталған максималды биіктігіне жетеді.

Белгілі бір бақылауды оқшаулау үшін қажет бөлінулер саны оның Isolation Forest ішіндегі жолының ұзындығына сәйкес келеді. Тез оқшауланған бақылаулар, яғни олар аз рекурсивті бөлінуді қажет етеді - жол ұзындығы қысқарады. Аномальды даналар әдетте сирек кездесетіндіктен және қалыпты деректерден айтарлықтай ерекшеленетіндіктен, оларды бөлудің бастапқы кезеңдерінде деректер жиынының қалған бөлігінен бөлу ықтималдығы жоғары. Демек, аномалиялар ағаштар ансамбліндегі жолдардың орташа ұзындығының қысқаруын көрсетеді, бұл олардың аномалия көрсеткіштерін есептеуге негіз болады.

2.3.2. Оқыту тәртібі

Isolation Forest моделі тек бақыланатын модельдеу эксперименттері нәтижесінде пайда болған қатерсіз бастапқы трафикті пайдалана отырып оқытылды. Тренинг Scapy негізіндегі пакеттерді әзірлеу және 5G шабыттандырылған бес ортада ағынды модельдеу арқылы бақыланатын эксперименттер арқылы жасалған қатерсіз бастапқы трафикті пайдалана отырып жүргізілді.: 5G қолдайтын MANET, 5g mMTC (IoT), гетерогенді 5G кесу, 5G NSA (LTE-A) және SDN қолдайтын 5G.

Әрбір орта үшін пакеттің жылдамдығы, ағынның ұзақтығы, байт саны, келу уақытының дисперсиясы және хаттаманың таралуы сияқты трафиктің ерекшеліктері 5g трафигінің құжатталған әрекетінің үлгілерінен алынған параметрленген статистикалық үлестірімдерден алынды. Оқу деректер жинағына зиянды немесе шабуылдаушы трафик енгізілмеген.

Нәтижесінде оқу корпусы қоршаған ортаға шамамен 10 000-50 000 базалық терезеден тұрды. Әрбір терезе белгіленген уақыт аралығында жинақталған телеметриялық суретті ұсынды. Бұл терезелер Isolation Forest моделін құрайтын Isolation Forest ансамблін салу үшін пайдаланылды.

Тек жақсы операциялық трафикке үйрету арқылы модель алдын ала анықталған шабуыл қолтаңбаларын есте сақтаудан гөрі қалыпты желі әрекетінің құрылымдық сипаттамаларын үйренеді. Бұл дизайн аномалияны анықтау бұрын байқалмаған немесе дамып келе жатқан шабуыл стратегияларын анықтауға мүмкіндік беретін белгіленген бастапқы үлгілерден ауытқуларға негізделгенін қамтамасыз етеді.

Isolation Forestның параметрлері келесідей конфигурацияланған:

Кесте 1 — Isolation Forest параметрлері.

Parameter	Value
Number of Trees	100
Subsample Size	256
Contamination	0.02
Random Seed	Fixed for reproducibility

Кесте 1 — ластану параметрі деректер жиынындағы ауытқулардың күтілетін үлесін бақылайды.

2.3.3. Edge Архитектурасындағы нақты уақыттағы қорытынды

Нақты уақыттағы жұмыс кезінде трафикті бақылау әрбір 5G шабыттандырылған ортада орналастырылған таратылған жиек агенттері арқылы жүзеге асырылады. Бұл агенттер өңдеудің үстеме шығындарын азайту және құрылымдық мүмкіндіктерді шығаруды қамтамасыз ету үшін шикі желілік трафикті тұрақты жұмыс уақыты терезелеріне үздіксіз біріктіреді. Әрбір уақыт терезесі үшін ағынның статистикалық сипаттамалары мен әрекетінің көрсеткіштерін түсіре отырып, сәйкес функция векторы шетінде жергілікті түрде есептеледі.

Содан кейін алынған функция векторлары артқы өңдеу модуліне жіберіледі, онда дайындалған Isolation Forest моделі қорытынды жасайды. Әрбір кіріс векторы үшін x , модель аномалия балын есептейді (x). Егер аномалия көрсеткіші (x) $> \tau$ сияқты алдын ала белгіленген τ шегінен асып кетсе, сәйкес терезе аномалия ретінде жіктеледі. Әйтпесе, бұл қалыпты трафик болып саналады.

Соңғы шешім гибриді шешім қабылдау механизмімен шығарылады, ол Suricata ережесі қозғалтқышынан алынған қолтаңбаға негізделген анықтау шығысын Isolation Forest моделі жасаған аномалияға негізделген шығыспен біріктіреді. Бұл біріктіру механизмі жүйеге белгілі қолтаңбаға сәйкес келетін шабуылдарды да, бұрын байқалмаған әрекеттер ауытқуларын да анықтауға мүмкіндік береді, осылайша гетерогенді 5G орталарында жалпы анықтау мүмкіндігін күшейтеді. Соңғы шешім логикасы 2-кестеде көрсетілген.

Кесте 2 — Шет архитектурасындағы нақты уақыттағы қорытынды.
Ережеге сәйкес келетін ML аномалиясының соңғы шешімі

Rule Match	ML Anomaly	Final Verdict
Yes	-	BLOCK
No	Yes	ALERT
No	No	ALLOW

Нәтижесі. Бұл бөлімде ұсынылған гибриді IDPS бес өкілдік 5G-бағытталған ортада эксперименттік бағалауы ұсынылған. Нәтижелерді талдаудың мақсаты - анықтау тиімділігін, жалған оң әрекеті, трафик жүктемесінің артуындағы масштабталуды және шетінде орналастырылған архитектуралардағы жауап кідірісін бағалау. Өнімділік стандартты енуді анықтау метрикасын, соның ішінде дәлдік, дәлдік, еске түсіру, F1 ұпайы, жалған оң жылдамдық (FPR) және анықтау кідірісін пайдаланып сандық түрде анықталды.

Бағалауда біріктіруге негізделген шешім қабылдаудың практикалық артықшылықтарын көрсету үшін гибриді анықтау тәсілін дербес қолтаңбаға негізделген және аномалияға негізделген механизмдермен салыстырады. Нәтижелер анықтау сенімділігі, есептеу тиімділігі және төмен кідіріспен 5G-ға негізделген орналастыруларға жарамдылығы туралы эмпирикалық дәлелдер келтіреді.

3.1. Анықтау дәлдігін бағалау

Осы бөлімшедегі нәтижелер 5G технологиясына негізделген бес түрлі ортада гибриді IDPS жүйесін имитациялық модельдеу арқылы бағалау деректерін қамтиды.

Гибриді IDPS жүйесі 5G-ге бағытталған бес түрлі ортада бағаланды. Анықтау тиімділігі «Дәлдік» (Accuracy), «Дәлділік коэффициенті» (Precision), «Толықтық» (Recall) және «F1-көрсеткіші» (F1-score) сияқты метрикалар арқылы өлшенді(кесте 3).

Кесте 3 — Бес 5G ортадағы анықтау өнімділігі.

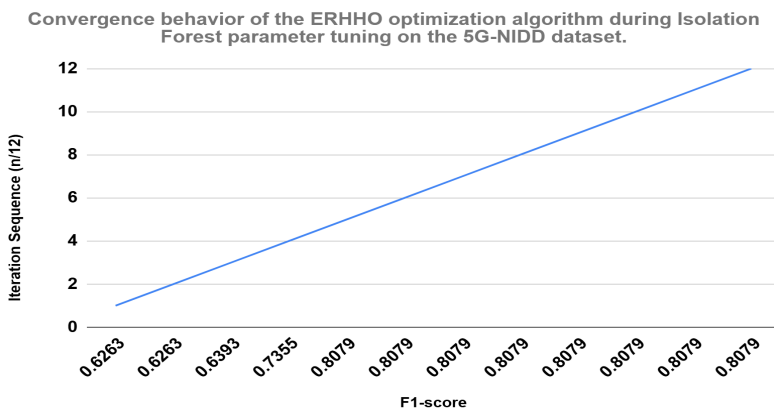
Environment	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)	False Positive Rate (%)
5G-enabled MANET	94.8	92.1	95.6	93.8	4.3
5G mMTC (IoT)	96.5	94.3	97.1	95.7	3.2
Heterogeneous 5G	95.2	93.7	94.9	94.3	3.9
5G NSA (LTE-A)	93.6	91.4	92.8	92.1	5.1
SDN-enabled 5G	97.1	95.8	96.9	96.3	2.7

Анықтаудың ең жоғары дәлдігі SDN қолдайтын 5G ортасында (97,1%) байқалды; бұл, ықтимал түрде, аномалияларды айқынырақ ажыратуға мүмкіндік беретін ағын әрекетінің құрылымдылығымен байланысты. Ең төменгі көрсеткіш 5G NSA (LTE-A) сценарийінде тіркелді, мұның себебі — басқару жазықтығындағы трафиктің күрделі сипаттамалары.

Гибридті модель тек қолтаңбаға (signature) негізделген анықтау әдісімен салыстырғанда жалған оң нәтижелер санын айтарлықтай азайтты (3.5-бөлімді қараңыз).

3.2 ERHNO оңтайландыру нәтижелері.

ERHNO оңтайландыру процесі барысында алгоритм он екі итерация бойы сәйкестік функциясын (fitness function) кезең-кезеңімен жақсартты. Оңтайландыру нәтижесінде, қорытынды тестілеу алдында валидациялық F1-көрсеткіші бастапқы 0,626 мәнінен соңғы 0,808 мәніне дейін артты; бұл модельдің жетілдірілген конфигурациясын анықтауда метаэвристикалық іздеу әдісінің тиімділігін көрсетті (сурет 2).



Сурет 2 — 5G-NIDD деректер жиынында Isolation Forest параметрлерін баптау кезіндегі ERHNO оңтайландыру алгоритмінің жинақталу сипаты

2-суретте оңтайландыру процесінің жинақталу сипаты көрсетілген. Сәйкестік мәні алғашқы бірнеше итерация кезінде қарқынды түрде артып, шамамен бес итерациядан кейін тұрақталады; бұл алгоритмнің параметрлердің тұрақты конфигурациясына жинақталатынын білдіреді. Мұндай сипаттама ERHNO іздеу әдісінің артық есептеу шығындарын болдырмай, параметрлер кеңістігін тиімді зерттейтінін көрсетеді.

3.3 Масштабталу мүмкіндігін бағалау.

Масштабталу мүмкіндігі трафик жүктемесін минутына 5 000-нан 100 000 оқиғаға дейін біртіндеп арттыру арқылы өлшенді. Гибридті анықтау жүйесінің өңдеу өткізу қабілеті жүйелік деңгейдегі мониторинг құралдарының көмегімен секундына оқиғалар санымен өлшенді. Өнімділік өңдеу өткізу қабілеті, орталық процессорды (CPU) пайдалану және жадты тұтыну көрсеткіштері бойынша бағаланды. 3.6. Жалпы бағалау қорытындысы (кесте 4).

Кесте 4 — Трафик жүктемесі артқан кездегі масштабталу өнімділігі. Трафик генерациясының қарқыны минутына оқиғалар санымен, ал анықтау конвейерінің өңдеу өткізу қабілеті секундына оқиғалар санымен өлшенеді.

Трафик жүктемесі (оқиға/мин)	Өңдеу өнімділігі (оқиға/сек)	Орталық процессорды пайдалану (%)	Жадты пайдалану (МБ)
5000	1,2	22	310
20000	4,65	38	420
50000	11,8	61	590
75000	16,9	72	710
100000	21,3	84	890

Бірліктердегі айырмашылық трафикті генерациялау жылдамдығы (минутына оқиғалар) мен жүйені өңдеудің өткізу қабілеті (секундына оқиғалар) арасындағы айырмашылықты көрсетеді.

Жүйе өнімділіктің төмендеуінсіз минутына 100 000 оқиғаға дейін сызықтық масштабталуды сақтап қалды. CPU пайдалануы пропорционалды түрде өсті, бірақ 85%-дан төмен қалды, бұл тіпті жоғары тығыздықтағы 5G трафик жүктемелерінде де шеткі орналастырудың мүмкін екенін көрсетеді.

Оқшаулау орманы әдетте GPU жеделдетуін қажет ететін терең оқыту тәсілдерімен салыстырғанда тұрақты жад тұтынуын көрсетті.

3.4 Гибридті және жеке анықтауды салыстыру.

Үш анықтау режимінің өнімділігі салыстырылды(кесте 5):

- Тек қолтаңбаны анықтау
- Оқшаулау орманы аномалиясын анықтау
- Гибридті (Қолтаңба + ML біріктіру)

Кесте 5 — Аномалияларды анықтау конфигурацияларының салыстырмалы жұмыс тиімділігі

Detection Mode	Accuracy (%)	False Positive Rate (%)	Detection Latency (ms)
Signature Only	88.4	9.7	3.2
Isolation Forest Only	93.1	5.4	6.8
Hybrid IDPS	96.2	3.8	5.1

Қолтаңбаға негізделген анықтау төмен кідіріспен қамтамасыз етті, бірақ жаңа шабуылдарды анықтай алмады.

Оқшаулау орманы белгісіз ауытқуларды анықтады, бірақ сәл жоғары кідіріс енгізді.

Гибридті тәсіл анықтау дәлдігі мен жауап беру жылдамдығын теңестірді, жалған оң нәтижелерді азайтты, сонымен бірге қолайлы кідіріс сақталды.

3.5 Жауап беру жылдамдығын бағалау.

Жауап беру кідірісі пакетті қабылдау мен соңғы анықтау шешімі арасындағы уақыт ретінде өлшенді(кесте 6).

Кесте 6 — Анықтау тиімділігін салыстыру

Environment	Average Latency (ms)	Maximum Latency (ms)
5G-enabled MANET	4.8	9.6
5G mMTC (IoT)	5.2	10.3
Heterogeneous 5G	5.6	11.1
5G NSA (LTE-A)	6.3	12.7
SDN-enabled 5G	4.4	8.9

Барлық кідіріс мәндері 15 мс-тен төмен деңгейде сақталып, URLLC талаптарына негізделген өнімділік шектеулерін қанағаттандырды.

Шеткі желіде (edge) орналастыру алдыңғы зерттеулерде (National Institute of Standards and Technology (NIST) et al., 2026) сипатталған орталықтандырылған IDS архитектураларымен салыстырғанда жауап беру уақытын айтарлықтай қысқартты.

3.6 Жалпы бағалау қорытындысы.

Эксперимент нәтижелері ұсынылған гибриді IDPS жүйесінің тек қолтанбаға (signature) негізделген IDPS-пен салыстырғанда анықтау тиімділігін едәуір арттыра алатынын көрсетеді. Атап айтқанда, гибриді архитектураның анықтау дәлдігі шамамен 8%-ға жақсарды, бұл механизмдер үйлесімінің тиімділігін айғақтайды. Сонымен қатар, қате оң нәтижелер (false positive) деңгейі 6%-ға төмендеді, яғни шешім қабылдау сенімділігі артып, жалған дабылдар азайды.

Өнімділік тұрғысынан алғанда, жүйе жоғары масштабталу мүмкіндігіне ие болды және минутына 100 000 оқиғаға дейінгі жүктеме кезінде де өнімділіктің айтарлықтай төмендеуінсіз тұрақты жұмыс істеді. Барлық бағаланған сценарийлерде анықтаудың орташа кідірісі 10 мс-тен төмен деңгейде сақталды, бұл 5G және URLLC сценарийлерінен туындайтын төмен кідіріспен жұмыс істеу талаптарына сай келеді. Жалпы алғанда, нәтижелер шеткі желіде орналастырылған заманауи 5G желісіне тән қатаң өнімділік талаптарына сәйкестікті және анықтаудың жоғары тиімділігін растайды.

3.7 Модельдерді салыстырмалы бағалау.

Аномалияларды анықтау модельдерінің тиімділігін бағалау үшін үш конфигурация салыстырылды:

- Параметрлері қолмен таңдалған Isolation Forest
- Random Forest көмегімен белгілерді (feature) таңдау және Isolation Forest үйлесімі
- ERHNO көмегімен оңтайландырылған Isolation Forest.

7-кестеде салыстырмалы нәтижелер көрсетілген.

Кесте 7 — Аномалияларды анықтау конфигурацияларының салыстырмалы жұмыс тиімділігі

Model	Accuracy (%)	Precision (%)	Recall (%)	F1 (%)	ROC-AUC (%)
RF + IF	55.3	90.1	29.7	44.7	80.2
IF Manual	61.6	86.9	43.2	57.7	82
IF + ERHNO	78.6	88.4	74.5	80.9	79.5

ERHNO көмегімен оңтайландырылған модель базалық модельдермен салыстырғанда «толықтық» (recall) және F1-көрсеткішін айтарлықтай жақсартты, бұл аномалияларды анықтау параметрлерін баптауда метаэвристикалық оңтайландырудың тиімділігін дәлелдеді.

Қорытынды. Бұл зерттеудің мақсаты – шеткі есептеу (Edge Computing – EC) архитектурасында іске асырылған және кідірісі төмен 5G орталарына арналған гибриді «Шабуылды анықтау және оның алдын алу жүйесі» (IDPS) шешімін эксперименталды түрде зерттеу болды. Ұсынылған жүйе белгілі және белгісіз қауіптерді анықтау үшін детерминирленген және сигнатураға негізделген анықтау әдістерін «Isolation Forest» (Оқшаулау орманы) атты оқытусыз (unsupervised) аномалияларды анықтау моделімен біріктіреді.

Аномалияларды анықтау бойынша салыстырмалы зерттеуде ERHNO көмегімен оңтайландырылған «Isolation Forest» моделі базалық модельдерге (қолмен бапталған «Isolation Forest» және «Random Forest» көмегімен белгілерді іріктеу әдісі) қарағанда әлдеқайда жақсы нәтиже көрсетті. Атап айтқанда, ERHNO моделі 80,9% F1-көрсеткішіне қол жеткізді, ал қолмен бапталған «Isolation Forest» үшін бұл көрсеткіш 57,7%, ал RF+IF үшін 44,7% болды. Абсолюттік мәнде ERHNO оңтайландырған модель 78,6% дәлдікке (accuracy), 88,4% нақтылыққа (precision), 74,5% толықтыққа (recall) және 80,9% F1-көрсеткішіне қол жеткізді. Бұл 5G трафигі жағдайында параметрлерді метаэвристикалық оңтайландыру аномалияларды анықтау тиімділігіне жай ғана белгілерді саралау әдісіне қарағанда көбірек үлес қосатынын көрсетеді.

5G технологиясына негізделген бес түрлі ортада (5G қолдайтын MANET, 5G mMTC (IoT), гетерогенді 5G, 5G NSA (LTE-A) және SDN қолдайтын 5G) жүргізілген эксперименталды бағалау гибриді тәсілдің жеке жұмыс істейтін анықтау механизмдерінен басым түсетінін көрсетті. Анықтау дәлдігі тек сигнатураға негізделген жүйелермен салыстырғанда шамамен 8%-ға жоғары болды, ал жалған оң нәтижелер (false positive) деңгейі 6%-ға дейін төмендеді. Жүйе минутына 100 мыңға дейін оқиғаны өңдей алды және орташа анықтау кідірісі 10 мс-тен аз болды, бұл кідірісі өте төмен (URLLC) сценарийлердің пайдалану талаптарына сай келеді.

Нәтижелер «Isolation Forest» сияқты жеңіл әрі оқытусыз жұмыс істейтін аномалияларды анықтау модельдерін шеткі есептеу архитектурасында сәтті енгізуге болатынын және олардың айтарлықтай есептеу ресурстарын қажет етпейтінін растайды. Гибриді IDPS ережеге негізделген және аномалияға

негізделген тәсілдерді біріктіру арқылы ресурстарды тиімді пайдалануды қамтамасыз ете отырып, анықтау мүмкіндігі мен жауап беру уақыты арасындағы тепе-теңді Бағалау модельдеу ортасында жүргізілді, бірақ ұсынылған архитектураны нақты әлемдегі орталардағы және 5G кіру деректер жиынтықтарындағы телеметрияны қабылдау архитектураларына оңай бейімдеуге болады. Жүргізіліп жатқан зерттеулер деректер жиынтықтарын кеңейтілген тексеру, таратылған оқыту механизмі, кесінділерді анықтау үшін бейімделгіш шекті оңтайландыру және жаңа 6G желі архитектураларының қауіпсіздік аспектілеріне бағытталады, бұл деректер санының артуына және күрделілігіне әкелуі мүмкін. Келесі буын сымсыз желілеріндегі масштабталуды бейімделгіш оқыту механизмдерін және федеративті аномалияларды анықтауды енгізу арқылы одан әрі жақсартуға болады.

Соңында, гибриді IDPS - жоғары анықтау сенімділігі мен қатаң төмен кідіріс талаптарына сай келетін алдағы 5G инфрақұрылымдары үшін шынайы және масштабталатын қауіпсіздік шешімі.

References

3GPP. Security Architecture and Procedures for 5G System (5GS); TS 33.501; 3rd Generation Partnership Project (3GPP): Sophia Antipolis, France, (2023) Available online: https://www.etsi.org/deliver/etsi_ts/133500_133599/133501/16.03.00_60/ts_133501v160300p.pdf (accessed on 10 February 2026) (in Eng.).

National Institute of Standards and Technology (NIST) 5G Cybersecurity Practice Guide (SP 1800-33); NIST: Gaithersburg, MD, USA, 2022. Available online: <https://www.nccoe.nist.gov/sites/default/files/2022-04/nist-5G-sp1800-33b-preliminary-draft.pdf> (accessed on 10 February 2026) (in Eng.).

European Union Agency for Cybersecurity (ENISA) ENISA Threat Landscape for 5G Networks; ENISA: Heraklion, Greece (2021). Available online: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021> (accessed on 10 February 2026) (in Eng.).

European Telecommunications Standards Institute (ETSI) MEC Security; ETSI White Paper. — No. 46, 2nd ed.; ETSI: Sophia Antipolis, France, 2022. Available online: <https://www.etsi.org/images/files/etsiwhitepapers/etsi-wp-46-2nd-ed-mec-security.pdf> (accessed on 10 February 2026) (in Eng.).

Park S., Kim D., Park Y., Cho H., Kim D., Kwon S. 5G Security Threat Assessment in Real Networks. *Sensors* (2021). Available online: <https://pmc.ncbi.nlm.nih.gov/articles/PMC8399903/> (accessed on 10 February 2026) (in Eng.).

Wazid M., Das A.K., Rodrigues J.J.P.C. Security in 5G-Enabled Internet of Things Communication: Issues and Challenges. *IEEE Access* 2021, 9. — P.1168–1184. Available online: <https://eprints.whiterose.ac.uk/id/eprint/172211/> (accessed on 10 February 2026) (in Eng.).

Ahmed M., et al. Cybersecurity Risks in 5G Networks: Challenges and Solutions. *SSRN Electronic Journal* 2022. Available online: <https://papers.ssrn.com> (accessed on 10 February 2026) (in Eng.).

Moustafa N. TON_IoT Telemetry Dataset: A New Generation Dataset of IoT and IIoT for Data-Driven Intrusion Detection Systems. *IEEE Access* 2020, 8. — P. 165130–165150. Available online: <https://dro.deakin.edu.au> (accessed on 10 February 2026) (in Eng.).

Ferrag M.A., et al. Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications for Centralized and Federated Learning. *IEEE Access* (2022), 10. — P. 40281–40306. Available online: <https://core.ac.uk/download/511306876.pdf> (accessed on 10 February 2026) (in Eng.).

Sharafaldin I., Lashkari A.H., Ghorbani A.A. Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization. ICISSP 2018; CSE-CIC-IDS2018 Dataset. Available online: <https://www.unb.ca/cic/datasets/ids-2018.html> (accessed on 10 February 2026) (in Eng.).

Siriwardhana Y., et al. 5G-NIDD: A Comprehensive Intrusion Detection Dataset Generated over 5G Wireless Network. arXiv 2022, arXiv:2212.01298. Available online: <https://arxiv.org/abs/2212.01298> (accessed on 10 February 2026) (in Eng.).

University College Dublin. 5G-NIDD Dataset Portal. Available online: <https://netslab.ucd.ie/netslab-datasets/5g-nidd-dataset/> (accessed on 10 February 2026) (in Eng.).

Idaho National Laboratory. 5GAD: 5G Attack Detection Dataset. Available online: <https://github.com/IdahoLabResearch/5GAD> (accessed on 10 February 2026) (in Eng.).

Bouke M.A., et al. Empirical Assessment of Machine Learning Models for Intrusion Detection Using 5G-NIDD Dataset. Internet of Things 2024, 26. — 101002 p. (in Eng.).

Imambayev A., et al. Machine Learning-Based Intrusion Detection for 5G Core Networks. Sensors 2022, 22. — 9957 p. (in Eng.).

Rodriguez C.A., et al. Zeek-Based Flow Feature Extraction for Efficient Intrusion Detection. Sensors 2022, 22. — 9326 p.

Gao S., et al. Security Threats and Countermeasures across the Lifecycle of 5G Network Slices. Electronics (2024), 13. — 1860 p. (in Eng.).

NDS Group. 5G UPF Intrusion Detection Using P4-Programmable Data Planes. Available online: https://github.com/nds-group/5G_UPF_Intrusion_Detection (accessed on 10 February 2026) (in Eng.).

Hussain R., et al. Security and Reliability in Ultra-Reliable Low-Latency Communications (URLLC). IEEE Communications Surveys & Tutorials 2021, 23. — P. 1894–1923 (in Eng.).

Bordel B., et al. Security Mechanisms for Ultra-Low Latency 5G Networks: Performance Evaluation. IEEE Access (2022), 10. — 9968044 p. (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.