MINISTRY OF SCIENCE AND HIGHER EDUCATION OF THE REPUBLIC OF KAZAKHSTAN

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РЕСПУБЛИКИ КАЗАХСТАН

KAZAKHSTAN

ХАЛЫҚАРАЛЫҚ УНИВЕРСИТЕТІ

INTERNATIONAL UNIVERSITY SINCE 2009

МЕЖДУНАРОДНЫЙ УНИВЕРСИТЕТ

INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES

Published since 2020.
Volume 7. 3 (27). 2026
July–September

ХАЛЫҚАРАЛЫҚ АҚПАРАТТЫҚ ЖӘНЕ КОММУНИКАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАР ЖУРНАЛЫ

2020 жылдан бері шығарылады
Том 7. 3 (27). 2026
Шілде-Қыркүйек

МЕЖДУНАРОДНЫЙ ЖУРНАЛ ИНФОРМАЦИОННЫХ И КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Издается с 2020 г.
Том 7. 3 (27). 2026
Июль-Сентябрь

Свидетельство о постановке на учет периодического печатного издания в Министерство информации и общественного развития Республики Казахстан № KZ82VPY00020475, выданное от 20.02.2020 г.

Зарегистрировано в Международном центре регистрации серийных изданий ISSN (ЮНЕСКО, Париж, Франция). ISSN 2708–2032 (print), ISSN 2708–2040 (online)

Журнал входит в Перечень научных изданий, рекомендуемых КОКНВО МНВО РК для публикации основных результатов научной деятельности.

EDITOR-IN-CHIEF:
Kateryna Kolesnikova — Doctor of Technical Sciences, professor, Vice-Rector for Research, International Information Technology University (Kazakhstan)

DEPUTY EDITOR-IN-CHIEF:
Madina Ipalakova — Candidate of Technical Sciences, associate professor, Director of the Research Department, International Information Technology University (Kazakhstan)

EDITORIAL BOARD:
Abdul Razak — PhD, professor, Department of Cybersecurity, International Information Technology University (Kazakhstan)
Lucio Tommaso De Paolis — Director of the R&D Department of the AVR Laboratory, Department of Engineering for Innovation, University of Salento (Italy)
Liz Bacon — Professor, Deputy Vice-Chancellor, Abertay University (United Kingdom)
Michele Pagano — PhD, Professor, University of Pisa (Italy)
Mukhtarbay Otelbayev — Doctor of Physical and Mathematical Sciences, professor, academician of the National Academy of Sciences of the Republic of Kazakhstan, professor of the Department of Mathematical and Computer Modeling, International Information Technology University (Kazakhstan)
Bolatbek Rysbaiuly — Doctor of Physical and Mathematical Sciences, professor, professor of the Department of Computing and Data Science, Astana IT University (Kazakhstan)
Yevgeniya Daineko — PhD, research professor, Department of Information Systems, International Information Technology University (Kazakhstan)
Nurzhan Duzbayev — PhD, associate professor, Vice-Rector for Digitalization and Innovation, International Information Technology University (Kazakhstan)
Bakhtgerei Sinchev — Doctor of Technical Sciences, professor, Department of Information Systems, International Information Technology University (Kazakhstan)
Nurgul Seilova — Candidate of Technical Sciences, Dean of the Faculty of Computer Technologies and Cybersecurity, International Information Technology University (Kazakhstan)
Ardak Mukhamediyeva — Candidate of Economic Sciences, Dean of the Faculty of Business, Media and Management, International Information Technology University (Kazakhstan)
Zamira Abdikalikova — PhD, associate professor, Head of the Department of Mathematical and Computer Modeling, International Information Technology University (Kazakhstan)
Yerlan Shildibekov — PhD, associate professor, Head of the Department of Economics and Business, International Information Technology University (Kazakhstan)
Damilya Yeskendirova — Candidate of Technical Sciences, associate professor, Head of the Department of Cybersecurity, International Information Technology University (Kazakhstan)
Aigul Niyazgulova — Candidate of Philological Sciences, Professor, Head of the Department of Media Communications and History of Kazakhstan, International Information Technology University (Kazakhstan)
Altai Aitmagambetov — Candidate of Technical Sciences, Professor, Department of Radio Engineering, Electronics and Telecommunications, International Information Technology University (Kazakhstan)
Yelena Bakhtiyarova — Candidate of Technical Sciences, associate professor, Head of the Department of Radio Engineering, Electronics and Telecommunications, International Information Technology University (Kazakhstan)
Kanibek Sansyzbay — PhD, research professor, Department of Cybersecurity, International Information Technology University (Kazakhstan)
Sakhybay Tynymbayev — Candidate of Technical Sciences, Professor, Research Professor, Department of Computer Engineering, International Information Technology University (Kazakhstan)
Ali Abd Almisreb — PhD, associate professor, Department of Cybersecurity, International Information Technology University (Kazakhstan)
Mohamed Ahmed Hamada — PhD, associate professor, Department of Information Systems, International Information Technology University (Kazakhstan)
Yang Im Chu — PhD, Professor, Gachon University (South Korea)
Tadeusz Wallas — PhD, Vice-Rector, Adam Mickiewicz University (Poland)
Orken Mamyrbayev — PhD, Deputy Director for Science, RSE Institute of Information and Computational Technologies, Committee for Science of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Kazakhstan)
Sergey Bushuyev — Doctor of Technical Sciences, professor, Director of the Ukrainian Project Management Association “UKRNET,” Head of the Department of Project Management, Kyiv National University of Construction and Architecture (Ukraine)
Svetlana Beloshitskaya — Doctor of Technical Sciences, professor, Department of Computing and Data Science, Astana IT University (Kazakhstan)

MANAGING EDITOR
Raushan Mrzabayeva — Master of Science, editor, International Information Technology University (Kazakhstan)

International Journal of Information and Communication Technologies
Periodicity: 4 times a year.
Languages: Kazakh, Russian, English
DOI prefix: 10.54309
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Thematic focus: "Information technology"; "Digital technologies in the development of socio-economic systems"; "Information security and communication technologies".
Distribution: Materials are distributed under the Creative Commons Attribution 4.0
Journal website: https://journal.iitu.edu.kz
Owner: International Information Technology University JSC (Almaty).
Copyright: © International Journal of Information and Communication Technologies, 2026

РЕДАКЦИЯ

БАС РЕДАКТОР:

Колесникова Катерина Викторовна — техника ғылымдарының докторы, профессор, Халықаралық ақпараттық технологиялар университетінің ғылыми-зерттеу қызметі жөніндегі проректор (Қазақстан)

БАС РЕДАКТОРДЫҢ ОРЫНБАСАРЫ:

Ипалакова Мадина Тулегеновна — техника ғылымдарының кандидаты, қауымдастырылған профессор, Халықаралық ақпараттық технологиялар университетінің ғылыми-зерттеу қызметі жөніндегі департамент директоры (Қазақстан)

РЕДАКЦИЯЛЫҚ АЛҚА:

Разак Абдул — PhD, Халықаралық ақпараттық технологиялар университеті киберқауіпсіздік кафедрасының профессоры (Қазақстан)

Лучио Томмазо де Паолис — Саленто Университеті (Италия) инновация және технологиялық инжиниринг департаменті AVR зертханасының зерттеу және әзірлеу бөлімінің директоры

Лиз Бэкон — профессор, Абертей Университеті (Ұлыбритания) вице-канцлерінің орынбасары

Микеле Пагано — PhD, Пиза Университетінің (Италия) профессоры

Өтелбаев Мухтарбай Өтелбайұлы — физика-математика ғылымдарының докторы, профессор, ҚР ҰҒА академигі, Халықаралық ақпараттық технологиялар университеті математика және компьютерлік модельдеу кафедрасының профессоры (Қазақстан)

Рысбайулы Болатбек — физика-математика ғылымдарының докторы, профессор, Есептеу және деректер ғылымдары департаментінің профессоры, Astana IT University (Казахстан)

Дайнеко Евгения Александровна — PhD, Халықаралық ақпараттық технологиялар университеті ақпараттық жүйелер кафедрасының профессор-зерттеушісі (Қазақстан)

Дузбаев Нуржан Токкужаевич — PhD, қауымдастырылған профессор, Халықаралық ақпараттық технологиялар университеті цифрландыру және инновациялар жөніндегі проректор (Қазақстан)

Синчев Бахтгерей Куспанович — техника ғылымдарының докторы, профессор, Халықаралық ақпараттық технологиялар университеті ақпараттық жүйелер кафедрасының профессоры (Қазақстан)

Сейлова Нургуль Абадуллаевна — техника ғылымдарының докторы, Халықаралық ақпараттық технологиялар университеті компьютерлік технологиялар және киберқауіпсіздік факультетінің деканы (Қазақстан)

Мухамедиева Ардак Габитовна — экономика ғылымдарының кандидаты, Халықаралық ақпараттық технологиялар университеті бизнеса медиа және басқару факультетінің деканы (Қазақстан)

Абдикаликова Замира Турсынбаевна — PhD, қауымдастырылған профессор, Халықаралық ақпараттық технологиялар университеті математика және компьютерлік модельдеу кафедрасының меңгерушісі (Қазақстан)

Шильдибеков Ерлан Жаржанович — PhD, қауымдастырылған профессор, Халықаралық ақпараттық технологиялар университеті экономика және бизнес кафедрасының меңгерушісі (Қазақстан)

Дамеля Максутовна Ескендирова — техника ғылымдарының кандидаты, қауымдастырылған профессор, Халықаралық ақпараттық технологиялар университеті киберқауіпсіздік кафедрасының меңгерушісі (Қазақстан)

Ниязгулова Айгуль Аскарбековна — филология ғылымдарының кандидаты, доцент, профессор, Халықаралық ақпараттық технологиялар университеті медиакоммуникация және Қазақстан тарихы кафедрасының меңгерушісі (Қазақстан)

Айтмагамбетов Алтай Зуфарович — техника ғылымдарының кандидаты, Халықаралық ақпараттық технологиялар университеті радиотехника, электроника және телекоммуникация кафедрасының профессоры (Қазақстан)

Бахтиярова Елена Ажибековна — техника ғылымдарының кандидаты, қауымдастырылған профессор, Халықаралық ақпараттық технологиялар университеті радиотехника, электроника және телекоммуникация кафедрасының меңгерушісі (Қазақстан)

Канибек Сансызбай — PhD, қауымдастырылған профессор, Халықаралық ақпараттық технологиялар университеті киберқауіпсіздік кафедрасының профессор-зерттеушісі (Қазақстан)

Тынымбаев Сахибай — техника ғылымдарының кандидаты, профессор, Халықаралық ақпараттық технологиялар университеті компьютерлік инженерия кафедрасының профессор-зерттеушісі (Қазақстан)

Алмисреб Али Абд — PhD, Халықаралық ақпараттық технологиялар университеті киберқауіпсіздік кафедрасының қауымдастырылған профессоры (Қазақстан)

Мохамед Ахмед Хамада — PhD, Халықаралық ақпараттық технологиялар университеті ақпараттық жүйелер кафедрасының қауымдастырылған профессоры (Қазақстан)

Янг Им Чу — PhD, Гачон университетінің профессоры (Оңтүстік Корея)

Тадеуш Валлас – PhD, Адам Мицкевич атындағы (Польша) университеттің проректоры

Мамырбаев Оркен Жумажанович — PhD, ҚР ҒЖБМ Ғылым комитеті ақпараттық және есептеу технологиялары институты ӨМК директорының ғылым жөніндегі орынбасары (Қазақстан)

Бушуев Сергей Дмитриевич — техника ғылымдарының докторы, профессор, Украинаның "УКРНЕТ" жобаларды басқару қауымдастығының директоры, Киев ұлттық құрылыс және сәулет университеті жобаларды басқару кафедрасының меңгерушісі (Украина)

Белощицкая Светлана Васильевна — техника ғылымдарының докторы, доцент, Astana IT University есептеу және деректер ғылымы кафедрасының профессоры (Қазақстан)

ЖАУАПТЫ РЕДАКТОР:

Мрзабаева Раушан Жалиевна — магистр, Халықаралық ақпараттық технологиялар университетінің редакторы (Қазақстан)

Халықаралық ақпараттық және коммуникациялық технологиялар журналы
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Префикс DOI: 10.54309
Мерзімділігі: жылына 4 рет.
Басылым тілі: қазақ, орыс, ағылшын.
Тақырып бағыты: "Ақпараттық технологиялар"; "Ақпараттық қауіпсіздік және коммуникациялық технологиялар"; "Әлеуметтік-экономикалық жүйелерді дамытудағы цифрлық технология".
Журнал сайты: https://journal.iitu.edu.kz
Тарату: материалдар Creative Commons Attribution 4.0 лицензиясы бойынша таратылады
Меншік иесі: АҚ «Халықаралық ақпараттық технологиялар университеті» (Алматы қ.).
Авторлық құқық: © Халықаралық ақпараттық және коммуникациялық технологиялар журналы, 2026

РЕДАКЦИЯ

ГЛАВНЫЙ РЕДАКТОР:

Колесникова Катерина Викторовна — доктор технических наук, профессор, проректор по научно-исследовательской деятельности Международного университета информационных технологий (Казахстан)

ЗАМЕСТИТЕЛЬ ГЛАВНОГО РЕДАКТОРА:

Ипалакова Мадина Тулегеновна — кандидат технических наук, ассоциированный профессор, директор департамента по научно-исследовательской деятельности Международного университета информационных технологий (Казахстан)

РЕДАКЦИОННАЯ КОЛЛЕГИЯ:

Разак Абдул — PhD, профессор кафедры кибербезопасности Международного университета информационных технологий (Казахстан)

Лучио Томмазо де Паолис — директор отдела исследований и разработок лаборатории AVR департамента инноваций и технологического инжиниринга Университета Саленто (Италия)

Лиз Бэкон — профессор, заместитель вице-канцлера Университета Абертей (Великобритания)

Микеле Пагано — PhD, профессор Университета Пизы (Италия)

Отелбаев Мухтарбай Отелбайулы — доктор физико-математических наук, профессор, академик НАН РК, профессор кафедры математического и компьютерного моделирования Международного университета информационных технологий (Казахстан)

Рысбайулы Болатбек — доктор физико-математических наук, профессор, профессор Astana IT University (Казахстан)

Дайнеко Евгения Александровна — PhD, профессор-исследователь кафедры информационных систем Международного университета информационных технологий (Казахстан)

Дузбаев Нуржан Токкужаевич — PhD, ассоциированный профессор, проректор по цифровизации и инновациям Международного университета информационных технологий (Казахстан)

Синчев Бахтгерей Куспанович — доктор технических наук, профессор, профессор кафедры информационных систем Международного университета информационных технологий (Казахстан)

Сейлова Нургуль Абадуллаевна — кандидат технических наук, декан факультета компьютерных технологий и кибербезопасности Международного университета информационных технологий (Казахстан)

Мухамедиева Ардак Габитовна — кандидат экономических наук, декан факультета бизнеса медиа и управления Международного университета информационных технологий (Казахстан)

Абдикаликова Замира Турсынбаевна — PhD, ассоциированный профессор, заведующая кафедрой математического и компьютерного моделирования Международного университета информационных технологий (Казахстан)

Шильдибеков Ерлан Жаржанович — PhD, ассоциированный профессор, заведующий кафедрой экономики и бизнеса Международного университета информационных технологий (Казахстан)

Дамеля Максутовна Ескендирова — кандидат технических наук, ассоциированный профессор, заведующая кафедрой кибербезопасности Международного университета информационных технологий (Казахстан)

Ниязгулова Айгуль Аскарбековна — кандидат филологических наук, доцент, профессор, заведующая кафедрой медиакоммуникаций и истории Казахстана Международного университета информационных технологий (Казахстан)

Айтмагамбетов Алтай Зуфарович — кандидат технических наук, профессор кафедры радиотехники, электроники и телекоммуникаций Международного университета информационных технологий (Казахстан)

Бахтиярова Елена Ажибековна — кандидат технических наук, ассоциированный профессор, заведующая кафедрой радиотехники, электроники и телекоммуникаций Международного университета информационных технологий (Казахстан)

Канибек Сансызбай – PhD, ассоциированный профессор, профессор-исследователь кафедры кибербезопасности, Международного университета информационных технологий (Казахстан)

Тынымбаев Сахибай – кандидат технических наук, профессор, профессор-исследователь кафедры компьютерной инженерии, Международного университета информационных технологий (Казахстан)

Алмисреб Али Абд — PhD, ассоциированный профессор кафедры кибербезопасности Международного университета информационных технологий (Казахстан)

Мохамед Ахмед Хамада — PhD, ассоциированный профессор кафедры информационных систем Международного университета информационных технологий (Казахстан)

Янг Им Чу — PhD, профессор университета Гачон (Южная Корея)

Тадеуш Валлас – PhD, проректор университета имен Адама Мицкевича (Польша)

Мамырбаев Оркен Жумажанович — PhD, заместитель директора по науке РГП Института информационных и вычислительных технологий Комитета науки МНВО РК (Казахстан)

Бушуев Сергей Дмитриевич — доктор технических наук, профессор, директор Украинской ассоциации управления проектами «УКРНЕТ», заведующий кафедрой управления проектами Киевского национального университета строительства и архитектуры (Украина)

Белощицкая Светлана Васильевна — доктор технических наук, доцент, профессор кафедры вычислений и науки о данных Astana IT University (Казахстан)

ОТВЕТСТВЕННЫЙ РЕДАКТОР:

Мрзабаева Раушан Жалиевна — магистр, редактор Международного университета информационных технологий (Казахстан)

Международный журнал информационных и коммуникационных технологий
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Префикс DOI: 10.54309
Периодичность: 4 выпусков в год.
Язык издания: казахский, русский, английский.
Тематическая направленность: "Информационные технологии"; "Информационная безопасность и коммуникационные технологии"; "Цифровые технологии в развитии социо-экономических систем".
Сайт журнала: https://journal.iitu.edu.kz
Распространение: материалы распространяются по лицензии Creative Commons Attribution 4.0
Собственник: АО «Международный университет информационных технологий» (г. Алматы).
Авторские права: © Международный журнал информационных и коммуникационных технологий, 2026

CONTENTS

DIGITAL TECHNOLOGIES IN THE DEVELOPMENT OF SOCIO-ECONOMIC SYSTEMS

A Adalbek, S.Ye. Kerimkhulle, K.D. Kuliev, O. Mekesh, Zh.Zh. Khamitova
DEVELOPMENT OF RESULT-ORIENTED DATA SMOOTHING MODELS AND ANALYSIS OF THEIR EFFECTIVENESS 11
A.T. Iskakova, G.E. Kurmankulova, K. Gromaszek, K.O. Togzhanova, R.S. Algozhayeva
APPLICATION OF MACHINE LEARNING AND DEEP LEARNING FOR PREDICTIVE PLANNING AND RESOURCE EFFICIENCY IN PRODUCTION SYSTEMS 30
A.B. Kassymova, R.K. Uskenbayeva, Zh.A. Sydykov, D. Omirzak, S. Kalibekov
ARCHITECTURE OF AN INTELLIGENT CHATBOT FOR SMART CITY: AI-BASED RECEIVING, ANALYSIS AND ROUTING OF CITIZEN REQUESTS 46
O.M. Olzhayev, B.S. Omarov, A. Suliman
YOLO-CBAM: A LIGHTWEIGHT NEURAL NETWORK MODEL WITH INTEGRATED ATTENTION MECHANISM FOR ROAD DAMAGE ANALYSIS 66
K. Yermagambetova, A. Sarsekeyeva, Y. Akhlassov
OVERCOMING FRAGMENTATION IN THE CLASSIFICATION OF DIGITAL CULTURAL HERITAGE: AN INTEGRATIVE MULTIDIMENSIONAL MODEL 78

INFORMATION TECHNOLOGY

D. Abzhanova, S. Sharipova
ARCHITECTURE AND PRACTICAL IMPLEMENTATION OF A DIGITAL PLATFORM FOR MONITORING AND DATA EXCHANGE ON TRANSBOUNDARY WATER RESOURCES IN THE ZHAMBYL REGION 101
A. Aitanuly, O.A. Ussatova
ENHANCING TWO-FACTOR AUTHENTICATION FOR CLOUD HEALTHCARE SECURITY: THE ROLE OF DEEP LEARNING 122
O. Alseitov, O. Kuchanskyi
PHYSICS-INFORMED HYBRID LEARNING FOR HOURLY POWER-PLANT EMISSIONS: A MULTI-POLLUTANT BENCHMARK WITH UNCERTAINTY AND TRANSFER 141
A.M. Akhmetova, D.O. Baizhanova, Zh.N. Alisheva, B.A. Shaimov
ADAPTIVE OUTPUT ROUTER FOR NATURAL LANGUAGE MODELS CONSIDERING KEY PERFORMANCE INDICATORS 160
A.K. Aitim
AUTOMATIC AND SEMI-AUTOMATIC ANNOTATION OF KAZAKH TEXT CORPORA 180
Z.E. Balabayev, S.V. Biloshchytska
HANDWRITTEN TEXT RECOGNITION FOR CHAGATAI MANUSCRIPTS: COMPARING CRNN TRAINING FROM SCRATCH AND TRANSFORMER-BASED TRANSFER LEARNING 198
D.B. Baumuratova, T.K. Zhukabayeva, K.A. Abdrakhmanov, Z. Ahmad, A.A. Seitov
A NEURO-DIGITAL LEARNING MODEL FOR AI DRIVEN DIGITAL TRANSFORMATION IN HIGHER EDUCATION 219
T. Daoyun, G.A. Amirkhanova, Fu Yanwei, Y. Faruzkyzy
MULTIMODAL SEMANTIC MANIPULATION IN FAKE VIDEOS AND ITS INFLUENCE MECHANISM ON USERS' PERCEIVED TRUST 241
Zh. Doumchariyev, J. Tussupov, A. Akynbekova, M. Khassanova, M. Kassim
ENSEMBLE AND HYBRID LEARNING FOR DIGITAL TWIN MILK CLASSIFICATION 258
K.Z. Igibayev, A.Kh. Kozbakova, O. Auelbekov , T. Merembayev, K. Yessentayev
STUDY OF A DYNAMIC MIXING DEVICE IN A BIOREACTOR USING IOT TECHNOLOGIES 279
A.N. Ismukanova, G. Kochshanova, D.V. Pleskachev, Zh. Sarsenbayeva, P. Schmidt
AUTOMATED CLASSIFICATION OF SCIENTIFIC DATA USING ARTIFICIAL INTELLIGENCE: A COMPARATIVE ANALYSIS OF TRANSFORMER ARCHITECTURES AND HYBRID APPROACHES 306
T. Zh. Kamalov, Ali Abd. Almisreb, Mohammed A. Saleh
INVESTIGATION OF HYBRID QUANTUM-CLASSICAL ALGORITHMS FOR MACHINE LEARNING 323
B. Karimkyzy, K.G. Karasenko, N.A. Alisherov, N.M. Muratbek, A. Karim

KEY PUBLICATIONS OF 2021–2025 ON ARTIFICIAL INTELLIGENCE METHODS IN THE MANUFACTURING AND DIAGNOSTICS OF MEDICAL DEVICES FOR GLYCEMIC MONITORING: A THEMATIC ANALYTICAL REVIEW 338
S.K. Kumyzbaeva, K.E. Baglanbaev, K.S. Sarkyt, M.Zh. Konyrova
THREE-PHASE TRAINING OF INTELLIGENT ENERGY MANAGEMENT FOR A HYBRID ENERGY SYSTEM WITH A CLIMATE-AWARE STATE REPRESENTATION 357
N.E. Karabayev, S.K. Serikbayeva, E. Benkhelif, B. Tassuov
RESEARCH ON THE ROBUSTNESS OF ENSEMBLE MACHINE LEARNING MODELS TO ADVERSARIAL ATTACKS IN INTRUSION DETECTION SYSTEMS FOR IOT NETWORKS 369
M. Nurtas, G. Kapyshev
A METHODOLOGICAL FRAMEWORK FOR THE PREPROCESSING AND INTEGRATION OF GEOSPATIAL AND GEOPHYSICAL DATA FOR MINERAL PROSPECTIVITY PREDICTION USING MACHINE LEARNING 392
A. Neftissov, A. Biloshchytskyi, I. Kazambayev, A. Medetkhan, L. Kirichenko
ENERGY EFFICIENT MICROCLIMATE STABILIZATION FOR SEALED ARCHIVAL STORAGE ENCLOSURES 405
A.Zh. Omurtayeva, U.T. Makhazhanova, A.K. Adilova, Sh.K. Yelezhanova, J. Kultan
AN ADAPTIVE NEURAL-FUZZY MODEL FOR ASSESSING INVESTMENT RISKS IN THE AGRI-INDUSTRIAL COMPLEX: ODERNISATION OF THE DECISION-SUPPORT ARCHITECTURE THROUGH THE INTEGRATION OF MACHINE LEARNING 421
N. Shazhdekeyeva, A. Mukhanbetkaliyeva, A. Abdigaliyeva, A. Zhanekeshova, L. Nurgaliyeva
COMPARATIVE ANALYSIS OF MATHEMATICAL MODELS OF COLLABORATIVE FILTERING IN THE DEVELOPMENT OF A MOVIE RECOMMENDER SYSTEM 445
S. Sharmukhanbet, G. Turmukhanova, O. Findik, V. Makhatova, M. Rakhmetov
AN INTELLIGENT PIPELINE DEFECT DETECTION SYSTEM USING AN IN-PIPE ROBOT 461

INFORMATION SECURITY AND COMMUNICATIONTECHNOLOGIES

S.Z. Daruish, A.U. Utegenova, A.U. Kalizhanova, Zh.Zh. Zhumabekova
MACHINE LEARNING FOR POLLUTION CLASSIFICATION IN ROCKET BOOSTER IMPACT AREAS 480
S.N. Issabayeva, A.K. Rysbayeva, Zh.B. Ibrayeva, N.R. Mussabekov, N.Sh. Akimzhan
MACHINE LEARNING-BASED CYBERATTACK DETECTION IN OT-NETWORKS: A COMPARATIVE ANALYSIS OF NETWORK ANOMALY CLASSIFICATION METHODS 495
G. Shangytbayeva, A.N. Amanov, M.K. Issenova, G.E. Berikkhanova, K.O. Shakerkhan
INFORMATION SECURITY IN GOVERNMENT CLOUD SERVICES: RISK ASSESSMENT AND PROTECTION STRATEGIES 512
Ye. N. Tursynbek, N. Albanbay, D. Djenouri
OPTIMISATION OF COMMUNICATION COSTS IN TWO-TIER FEDERATED LEARNING FOR CYBERATTACK DETECTION IN IOT NETWORKS 529
A. Tastemirov, S.B. Mukhanov, S.T. Amanzholova, B. Aldosh
A COMPARATIVE EVALUATION OF MACHINE LEARNING MODELS FOR ACTIVE DIRECTORY THREAT DETECTION: FEATURE-LEAKAGE CONTROL AND CROSS-SCENARIO VALIDATION ON WINDOWS SECURITY EVENT LOGS 545

МАЗМҰНЫ
ӘЛЕУМЕТТІК-ЭКОНОМИКАЛЫҚ ЖҮЙЕЛЕРДІ ДАМЫТУДАҒЫ ЦИФРЛЫҚ ТЕХНОЛОГИЯЛАР

А Адалбек, С.Е. Керімқұл, К.Д. Кулиев, О. Мекеш, Ж.Ж. Хамитова
ДЕРЕКТЕРДІҢ НӘТИЖЕ БАҒДАРЛАНҒАН ТЕГІСТЕУ МОДЕЛЬДЕРІН ӘЗІРЛЕУ ЖӘНЕ ОЛАРДЫҢ ТИІМДІЛІГІН ТАЛДАУ 11
А.Т. Искакова, Г.Е. Курманкулова, Конрад Громашек, К.О. Тогжанова, Р.С. Алгожаева
ӨНДІРІС ЖҮЙЕЛЕРІНДЕ БОЛЖАМДЫ ЖОСПАРЛАУ ЖӘНЕ РЕСУРСТАРДЫ ҮНЕМДЕУ ҮШІН МАШИНАЛЫҚ ЖӘНЕ ТЕРЕҢ ОҚЫТУДЫ ҚОЛДАНУ 30
А.Б. Касымова, Р.К. Ускенбаева, Ж.А. Сыдыков, Д. Өмірзақ, С. Калибеков
SMART CITY ҮШІН ИНТЕЛЛЕКТУАЛДЫ ЧАТ-БОТ АРХИТЕКТУРАСЫ: АЗАМАТТАРДЫҢ

ӨТІНІШТЕРІН ЖАСАНДЫ ИНТЕЛЛЕКТ НЕГІЗІНДЕ ҚАБЫЛДАУ, ТАЛДАУ ЖӘНЕ БАҒЫТТАУ 46
О.М. Олжаев, Б.С. Омаров, A.Suliman
YOLO-CBAM: ЖОЛДЫҢ ЗАҚЫМДАНУЫН ТАЛДАУҒА АРНАЛҒАН ИНТЕГРАЦИЯЛАНҒАН ЗЕЙІН МЕХАНИЗМІ БАР ЖЕҢІЛ САЛМАҚТЫ НЕЙРОНДЫҚ ЖЕЛІ МОДЕЛІ 66
К. Ермагамбетова, А. Сарсекеева, Е. Ахласов
ЦИФРЛЫҚ МӘДЕНИ МҰРАНЫ ЖІКТЕУДЕГІ ФРАГМЕНТАЦИЯНЫ ЕҢСЕРУ: ИНТЕГРАТИВТІ КӨПӨЛШЕМДІ МОДЕЛЬ 78

АҚПАРАТТЫҚ ТЕХНОЛОГИЯЛАР

Д.Е. Абжанова, С.Е. Шарипова
ЖАМБЫЛ ӨҢІРІНІҢ ТРАНСШЕКАРАЛЫҚ СУ РЕСУРСТАРЫН МОНИТОРИНГТЕУ ЖӘНЕ ДЕРЕКТЕР АЛМАСУҒА АРНАЛҒАН ЦИФРЛЫҚ ПЛАТФОРМАНЫҢ АРХИТЕКТУРАСЫ МЕН ПРАКТИКАЛЫҚ ІСКЕ АСЫРЫЛУЫ 101
А.Айтанұлы, О.А. Усатова
БҰЛТТЫ МЕДИЦИНАЛЫҚ ЖҮЙЕЛЕРДЕ ЕКІ ФАКТОРЛЫ АУТЕНТИФИКАЦИЯНЫ ЖАҚСАРТУ: ТЕРЕҢ ОҚЫТУ ӘДІСТЕРІНІҢ ҚОЛДАНУ МҮМКІНДІКТЕРІ 122
О. Альсеитов, О. Кучанский
ЭЛЕКТР СТАНЦИЯЛАРЫНЫҢ САҒАТТЫҚ ШЫҒАРЫНДЫЛАРЫН ФИЗИКАЛЫҚ ЗАҢДЫЛЫҚТАРДЫ ЕСКЕРЕТІН ГИБРИДТІ ОҚЫТУ: БЕЛГІСІЗДІК ПЕН ТАСЫМАЛДАУДЫ ЕСКЕРЕТІН КӨПЛАСТАУЫШТЫ БЕНЧМАРК 141
А.М. Ахметова, Д.О. Байжанова, Ж.Н. Алишева, Б.А. Шаймов
КРІ КӨРСЕТКІШТЕРІН ЕСКЕРЕ ОТЫРЫП, ТАБИҒИ ТІЛ МОДЕЛЬДЕРІНЕ АРНАЛҒАН ШЫҒЫС МАРШРУТТАУЫНЫҢ АДАПТИВТІ ЖҮЙЕСІ 160
Ә.Қ. Әйтім
ҚАЗАҚ МӘТІНДІК КОРПУСТАРЫН АВТОМАТТЫ ЖӘНЕ ЖАРТЫЛАЙ АВТОМАТТЫ АННОТАЦИЯЛАУ 180
Ж.Е. Балабаев, С.В. Белощицкая
ШАҒАТАЙ ҚОЛЖАЗБАЛАРЫНЫҢ МӘТІНІН ТАНУ: CRNN-ДІ НӨЛДЕН БАСТАП ОҚЫТУ МЕН ТРАНСФОРМЕР НЕГІЗІНДЕГІ ТРАНСФЕРЛІК ОҚЫТУДЫ САЛЫСТЫРУ 198
Д.Б. Баумуратова, Т.К. Жукабаева, К.А. Абдрахманов, З. Ахмад, А.А. Сеитов
ЖОҒАРЫ БІЛІМ БЕРУДЕ AI НЕГІЗДЕЛГЕН ЦИФРЛЫҚ ТРАНСФОРМАЦИЯҒА АРНАЛҒАН НЕЙРО-ЦИФРЛЫҚ ОҚЫТУ МОДЕЛІ 219
Т. Даоюн, Г. Амирханова, Фу Яньвэй, Е. Фарузқызы
ФЕЙК ВИДЕОЛАРДАҒЫ МУЛЬТИМОДАЛЬДЫ СЕМАНТИКАЛЫҚ МАНИПУЛЯЦИЯНЫҢ ПАЙДАЛАНУШЫЛАРДЫҢ ҚАБЫЛДАЙТЫН СЕНІМІНЕ ӘСЕР ЕТУ МЕХАНИЗМІ 241
Ж. Доумчариева, Д. Тусупов, А. Акынбекова, М. Хасанова, М. Кассим
ЦИФРЛЫҚ ЕГІЗДЕГІ СҮТ САПАСЫН АНСАМБЛЬДІК ЖӘНЕ ГИБРИДТІ ОҚЫТУ АРҚЫЛЫ ЖІКТЕУ 258
Қ.З. Игибаев, А.Х. Козбакова, О. Әуелбеков, Т. Мерембаев, Қ. Есентаев
БИОРЕАКТОРДА IoT ТЕХНОЛОГИЯЛАРЫН ПАЙДАЛАНА ОТЫРЫП ДИНАМИКАЛЫҚ АРАЛАСТЫРУ ҚҰРЫЛҒЫСЫН ЗЕРТТЕУ 279
А.Н. Исмуканова, Г.Кощанова, Д.В. Плескачев, Ж.Сарсенбаева, П. Шмидт
ЖАСАНДЫ ИНТЕЛЛЕКТ НЕГІЗІНДЕ ҒЫЛЫМИ ДЕРЕКТЕРДІ АВТОМАТТЫ ТҮРДЕ ЖІКТЕУ: ТРАНСФОРМЕР АРХИТЕКТУРАЛАРЫ МЕН ГИБРИДТІ ТӘСІЛДЕРДІҢ САЛЫСТЫРМАЛЫ ТАЛДАУЫ 306
Т.Ж. Камалов, Али Абд. Альмисреб, Мохаммед А. Салех
МАШИНАЛЫҚ ОҚЫТУҒА АРНАЛҒАН ГИБРИДТІ КВАНТТЫҚ-КЛАССИКАЛЫҚ АЛГОРИТМДЕРІН ЗЕРТТЕУ 323
Б. Кәрімқызы, К.Г. Карасенко, Н.А. Әлішеров, Н.М. Мұратбек, А. Кәрім
2021–2025 ЖЫЛДАР АРАЛЫҒЫНДАҒЫ ГЛИКЕМИЯЛЫҚ МОНИТОРИНГКЕ АРНАЛҒАН МЕДИЦИНАЛЫҚ ҚҰРЫЛҒЫЛАРДЫ ӨНДІРУ ЖӘНЕ ДИАГНОСТИКАЛАУДАҒЫ ЖАСАНДЫ ИНТЕЛЛЕКТ ӘДІСТЕРІ БОЙЫНША НЕГІЗГІ ЖАРИЯЛАНЫМДАР 338
С. К. Кумызбаева, К.Е. Багланбаев, К.С. Саркыт, М. Конырова
КҮЙ-ЖАЙДЫ КЛИМАТҚА СЕЗІМТАЛ ҰСЫНУМЕН ГИБРИДТІ ЭНЕРГОЖҮЙЕНІҢ ИНТЕЛЛЕКТУАЛДЫ ЭНЕРГОМЕНЕДЖМЕНТІН ҮШФАЗАЛЫ ОҚЫТУ 357
Н.Е. Қарабаев, С.К. Серикбаева, Е. Бенкхелифа, Б. Тасуов

IOT-ЖЕЛІЛЕРІНДЕГІ БАСЫП КІРУДІ АНЫҚТАУЖҮЙЕЛЕРІНДЕ МАШИНАЛЫҚ ОҚЫТУДЫҢ АНСАМБЛЬДІ КҮЛГІЛЕРІНІҢ БӘСЕКЕЛЕС ШАБУЫЛДАРҒА ТӨЗІМДІЛІГІН ЗЕРТТЕУ 369
М. Нұртас, Ғ. Капышев
МАШИНАЛЫҚ ОҚЫТУДЫ ҚОЛДАНА ОТЫРЫП, ПАЙДАЛЫ ҚАЗБАЛАРДЫҢ ПЕРСПЕКТИВАЛЫЛЫҒЫН БОЛЖАУ ҮШІН ГЕОКЕҢІСТІКТІК ЖӘНЕ ГЕОФИЗИКАЛЫҚ ДЕРЕКТЕРДІ АЛДЫН АЛА ӨҢДЕУ ЖӘНЕ БІРІКТІРУДІҢ ӘДІСТЕМЕЛІК НЕГІЗІ 392
А. Нефтиссов, А. Билощицкий, И. Казамбаев, А. Медетхан, Л. Кириченко
ГЕРМЕТИКАЛЫҚ АРХИВТІК САҚТАУ ҚАПТАМАЛАРЫНДА МИКРОКЛИМАТТЫ ЭНЕРГИЯ ТИІМДІЛІГІН ЕСКЕРЕ ОТЫРЫП ТҰРАҚТАНДЫРУ 405
Ә.Ж. Омуртаева, У.Т. Махажанова, А.К. Адилова, Ш.К. Ележанова, Я. Култан
АГРОӨНЕРКӘСІПТІК КЕШЕНДЕГІ ИНВЕСТИЦИЯЛЫҚ ТӘУЕКЕЛДЕРДІ БАҒАЛАУҒА АРНАЛҒАН БЕЙІМДЕЛГІШ НЕЙРОНДЫҚ-БҰЛДЫР МОДЕЛЬ: МАШИНАЛЫҚ ОҚЫТУДЫ ИНТЕГРАЦИЯЛАУ АРҚЫЛЫ ШЕШІМ ҚАБЫЛДАУДЫ ҚОЛДАУ СӘУЛЕТІН ЖАҢҒЫРТУ 421
Н. Шаждекеева, А. Мұханбетқалиева, А. Әбдіғалиева, А. Жанекешова, Л. Нұрғалиева
ФИЛЬМДЕРДІ ҰСЫНУ ЖҮЙЕСІН ҚҰРУ КЕЗІНДЕГІ КОЛЛАБОРАТИВТІК СҮЗГІЛЕУДІҢ МАТЕМАТИКАЛЫҚ МОДЕЛЬДЕРІН САЛЫСТЫРМАЛЫ ТАЛДАУ 445
С. Шармұханбет, Г. Тұрмұханова, О. Финдик, В. Махатова, М. Рахметов
ҚҰБЫРІШІЛІК РОБОТТЫ ПАЙДАЛАНУ АРҚЫЛЫ ҚҰБЫР АҚАУЛАРЫН АНЫҚТАУДЫҢ ЗИЯТКЕРЛІК ЖҮЙЕСІ 461

АҚПАРАТТЫҚ ҚАУІПСІЗДІК ЖӘНЕ КОММУНИКАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАРҒА АРНАЛҒАН

С.З. Дәруіш, А.У. Утегенова, А.У. Калижанова, Ж.Ж. Жумабекова
ЗЫМЫРАН ТАСЫМАЛДАУШЫЛАРДЫҢ ҚҰЛАУ АЙМАҚТАРЫНЫҢ ЛАСТАНУЫН МАШИНАЛЫҚ ОҚЫТУМЕН ЖІКТЕУ 480
С.Н. Исабаева, А.К. Рысбаева, Ж.Б. Ибраева, Н.Р. Муссабеков, Н.Ш. Акимжан
МАШИНАЛЫҚ ОҚЫТУ НЕГІЗІНДЕ ОТ-ЖЕЛІЛЕРІНДЕГІ КИБЕРШАБУЫЛДАРДЫ АНЫҚТАУ: ЖЕЛІЛІК АНОМАЛИЯЛАРДЫ ЖІКТЕУ ӘДІСТЕРІНІҢ САЛЫСТЫРМАЛЫ ТАЛДАУЫ 495
Г.А. Шангытбаева, А.Н. Аманов, М.К. Исенова, Г.Е. Берикханова, Қ.О. Шакерхан
МЕМЛЕКЕТТІК ОРГАНДАРДЫҢ БҰЛТТЫ СЕРВИСТЕРІНДЕГІ АҚПАРАТТЫҚ ҚАУІПСІЗДІК: ТӘУЕКЕЛДЕРДІ БАҒАЛАУ ЖӘНЕ ҚОРҒАУ СТРАТЕГИЯЛАРЫ 512
Е.Н. Турсынбек, Н. Албанбай, Д. Дженоури
IOT ЖЕЛІЛЕРІНДЕ КИБЕРШАБУЫЛДАРДЫ АНЫҚТАУ ҮШІН ЕКІ ДЕҢГЕЙЛІ ФЕДЕРАЦИЯЛАНҒАН ОҚЫТУДАҒЫ БАЙЛАНЫС ШЫҒЫНДАРЫН ОҢТАЙЛАНДЫРУ 529
А. Тастемиров, С.Т. Аманжолова, Б. Алдош, С.Б. Муханов
ACTIVE DIRECTORY ЖҮЙЕСІНДЕ ҚАУІПТЕРДІ АНЫҚТАУ ҮШІН МАШИНАЛЫҚ ОҚЫТУ МОДЕЛЬДЕРІН САЛЫСТЫРМАЛЫ БАҒАЛАУ: WINDOWS ҚАУІПСІЗДІК ОҚИҒАЛАРЫ ЖУРНАЛДАРЫНДА БЕЛГІ ЖЫЛЫСТАУЫН БАҚЫЛАУ ЖӘНЕ КРОСС-СЦЕНАРЛЫҚ ВАЛИДАЦИЯ 545

СОДЕРЖАНИЕ
ЦИФРОВЫЕ ТЕХНОЛОГИИ В РАЗВИТИИСОЦИО-ЭКОНОМИЧЕСКИХ СИСТЕМ

А Адалбек, С.Е. Керимкулов, К.Д. Кулиев, О. Мекеш, Ж.Ж. Хамитова
РАЗРАБОТКА РЕЗУЛЬТАТИВНО-ОРИЕНТИРОВАННЫХ МОДЕЛЕЙ СГЛАЖИВАНИЯ ДАННЫХ И АНАЛИЗ ИХ ЭФФЕКТИВНОСТИ 11
А.Т. Искакова, Г.Е. Курманкулова, К. Громашек, К.О. Тогжанова, Р.С. Алгожаева
ПРИМЕНЕНИЕ МЕТОДОВ МАШИННОГО И ГЛУБОКОГО ОБУЧЕНИЯ ДЛЯ ПРОГНОЗНОГО ПЛАНИРОВАНИЯ И РЕСУРСОСБЕРЕЖЕНИЯ В ПРОИЗВОДСТВЕННЫХ СИСТЕМАХ 30
А.Б. Касымова, Р.К. Ускенбаева, Ж.А.Сыдыков, Д. Омирзак, С. Калибеков
АРХИТЕКТУРА ИНТЕЛЛЕКТУАЛЬНОГО ЧАТ-БОТА ДЛЯ SMART CITY: ПРИЁМ, АНАЛИЗ И МАРШРУТИЗАЦИЯ ОБРАЩЕНИЙ ГРАЖДАН НА ОСНОВЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА 46
О.М. Олжаев, Б.С. Омаров, A.Suliman
YOLO-CBAM: ЛЕГКОВЕСНАЯ НЕЙРОСЕТЕВАЯ МОДЕЛЬ С ИНТЕГРИРОВАННЫМ МЕХАНИЗМОМ ВНИМАНИЯ ДЛЯ АНАЛИЗА ДОРОЖНЫХ ПОВРЕЖДЕНИЙ 66
К. Ермагамбетова, А. Сарсекеева, Е. Ахласов
ПРЕОДОЛЕНИЕ ФРАГМЕНТАЦИИ В КЛАССИФИКАЦИИ ЦИФРОВОГО КУЛЬТУРНОГО НАСЛЕДИЯ:

ИНТЕГРАТИВНАЯ МНОГОМЕРНАЯ МОДЕЛЬ 78

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Д.Е. Абжанова, С.Е. Шарипова
АРХИТЕКТУРА И ПРАКТИЧЕСКАЯ РЕАЛИЗАЦИЯ ЦИФРОВОЙ ПЛАТФОРМЫ МОНИТОРИНГА И ОБМЕНА ДАННЫМИ О ТРАНСГРАНИЧНЫХ ВОДНЫХ РЕСУРСАХ ЖАМБЫЛСКОГО РЕГИОНА 101
А. Айтанулы, О.А. Усатова
СОВЕРШЕНСТВОВАНИЕ ДВУХФАКТОРНОЙ АУТЕНТИФИКАЦИИ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОБЛАЧНЫХ МЕДИЦИНСКИХ СИСТЕМ: ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ МЕТОДОВ ГЛУБОКОГО ОБУЧЕНИЯ 122
О. Альсеитов, О. Кучанский
ФИЗИЧЕСКИ ИНФОРМИРОВАННОЕ ГИБРИДНОЕ ОБУЧЕНИЕ ДЛЯ ПОЧАСОВОГО ПРОГНОЗИРОВАНИЯ ВЫБРОСОВ ЭЛЕКТРОСТАНЦИЙ: МНОГОКОМПОНЕНТНЫЙ БЕНЧМАРК С ОЦЕНКОЙ НЕОПРЕДЕЛЁННОСТИ И ПЕРЕНОСИМОСТЬЮ МОДЕЛЕЙ 141
А.М. Ахметова, Д.О. Байжанова, Ж.Н. Алишева, Б.А. Шаймов
АДАПТИВНЫЙ МАРШРУТИЗАТОР ВЫВОДА С УЧЕТОМ КЛЮЧЕВЫХ ПОКАЗАТЕЛЕЙ ЭФФЕКТИВНОСТИ ДЛЯ МОДЕЛЕЙ ЕСТЕСТВЕННОГО ЯЗЫКА 160
Ә.Қ. Әйтім
АВТОМАТИЧЕСКАЯ И ПОЛУАВТОМАТИЧЕСКАЯ АННОТАЦИЯ КАЗАХСКИХ ТЕКСТОВЫХ КОРПУСОВ 180
Ж.Е. Балабаев, С.В. Белощицкая
РАСПОЗНАВАНИЕ РУКОПИСНОГО ТЕКСТА ШАГАТАЙСКИХ РУКОПИСЕЙ: СРАВНЕНИЕ ОБУЧЕНИЯ CRNN С НУЛЯ И ТРАНСФЕРНОГО ОБУЧЕНИЯ НА БАЗЕ ТРАНСФОРМЕРОВ 198
Д.Б. Баумуратова, Т.К. Жукабаева, К.А. Абдрахманов, З. Ахмад, А.А. Сеитов
НЕЙРО-ЦИФРОВАЯ МОДЕЛЬ ОБУЧЕНИЯ ДЛЯ ЦИФРОВОЙ ТРАНСФОРМАЦИИ ВЫСШЕГО ОБРАЗОВАНИЯ С ПОМОЩЬЮ AI 219
Т. Даоюн, Г. Амирханова, Фу Яньвэй, Е. Фарузкызы
МЕХАНИЗМ ВЛИЯНИЯ МУЛЬТИМОДАЛЬНОЙ СЕМАНТИЧЕСКОЙ МАНИПУЛЯЦИИ В ФЕЙКОВЫХ ВИДЕО НА ВОСПРИНИМАЕМОЕ ДОВЕРИЕ ПОЛЬЗОВАТЕЛЕЙ 241
Ж. Доумчариева, Д. Тусупов, А. Акынбекова, М. Хасанова, М. Кассим
КЛАССИФИКАЦИЯ КАЧЕСТВА МОЛОКА В ЦИФРОВОМ ДВОЙНИКЕ АНСАМБЛЕВЫМИ И ГИБРИДНЫМИ МЕТОДАМИ 258
К.З. Игибаев, А.Х. Козбакова, О. Ауелбеков, Т. Мерембаев, К. Есентаев
ИССЛЕДОВАНИЕ УСТРОЙСТВА ДИНАМИЧЕСКОГО ПЕРЕМЕШИВАНИЯ В БИОРЕАКТОРЕ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИЙ IoT 279
А. Н. Исмуканова, Г.Кощанова, Д.В. Плескачев, Ж.Сарсенбаева, П. Шмидт
АВТОМАТИЗИРОВАННАЯ КЛАССИФИКАЦИЯ НАУЧНЫХ ДАННЫХ НА ОСНОВЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА: СРАВНИТЕЛЬНЫЙ АНАЛИЗ ТРАНСФОРМЕРНЫХ АРХИТЕКТУР И ГИБРИДНЫХ МЕТОДОВ 306
Т.Ж. Камалов, Али Абд. Альмисреб, Мохаммед А. Салех
ИССЛЕДОВАНИЕ ГИБРИДНЫХ КВАНТОВО-КЛАССИЧЕСКИХ АЛГОРИТМОВ ДЛЯ МАШИННОГО ОБУЧЕНИЯ 323
Б. Каримкызы, К.Г. Карасенко, Н.А. Алишеров, Н.М. Муратбек, А. Карим
КЛЮЧЕВЫЕ ПУБЛИКАЦИИ 2021–2025 ГОДОВ ПО МЕТОДАМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПРОИЗВОДСТВЕ И ДИАГНОСТИКЕ МЕДИЦИНСКИХ ИЗДЕЛИЙ ДЛЯ ГЛИКЕМИЧЕСКОГО МОНИТОРИНГА 338
С.К. Кумызбаева, К.Е. Багланбаев, К.С. Сарқыт, М.Ж. Конырова
ТРЁХФАЗОВОЕ ОБУЧЕНИЕ ИНТЕЛЛЕКТУАЛЬНОГО ЭНЕРГОМЕНЕДЖМЕНТА ГИБРИДНОЙ ЭНЕРГОСИСТЕМЫ С КЛИМАТО-ОСВЕДОМЛЁННЫМ ПРЕДСТАВЛЕНИЕМ СОСТОЯНИЯ 357
Н.Е. Қарабаев, С.К. Серикбаева, Е. Бенкхелифа, Б. Тасуов
ИССЛЕДОВАНИЕ УСТОЙЧИВОСТИ АНСАМБЛЕВЫХ МОДЕЛЕЙ МАШИННОГО ОБУЧЕНИЯ К СОСТЯЗАТЕЛЬНЫМ АТАКАМ В СИСТЕМАХ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ IOT-СЕТЕЙ 369
М. Нуртас, Г. Капышев
МЕТОДОЛОГИЧЕСКАЯ ОСНОВА ПРЕДВАРИТЕЛЬНОЙ ОБРАБОТКИ И ИНТЕГРАЦИИ ГЕОПРОСТРАНСТВЕННЫХ И ГЕОФИЗИЧЕСКИХ ДАННЫХ ДЛЯ ПРОГНОЗИРОВАНИЯ ПЕРСПЕКТИВНО-

СТИ МИНЕРАЛЬНЫХ РЕСУРСОВ С ИСПОЛЬЗОВАНИЕМ МАШИННОГО ОБУЧЕНИЯ 392
А. Нефтиссов, А. Билощицкий, И. Казамбаев, А. Медетхан, Л. Кириченко
ЭНЕРГОЭФФЕКТИВНАЯ СТАБИЛИЗАЦИЯ МИКРОКЛИМАТА В ГЕРМЕТИЧНЫХ АРХИВНЫХ ХРАНИЛИЩАХ 405
А.Ж. Омуртаева, У.Т. Махажанова, А.К. Адилова, Ш.К. Ележанова, Я.Култан
АДАПТИВНАЯ НЕЙРО-НЕЧЕТКАЯ МОДЕЛЬ ДЛЯ ОЦЕНКИ ИНВЕСТИЦИОННЫХ РИСКОВ В АГРОПРОМЫШЛЕННОМ КОМПЛЕКСЕ: МОДЕРНИЗАЦИЯ АРХИТЕКТУРЫ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ПОСРЕДСТВОМ ИНТЕГРАЦИИ МАШИННОГО ОБУЧЕНИЯ 421
Н. Шаждекеева, А. Муханбеткалиева, А. Абдигалиева, А. Жанекешова, Л. Нургалиева
СРАВНИТЕЛЬНЫЙ АНАЛИЗ МАТЕМАТИЧЕСКИХ МОДЕЛЕЙ КОЛЛАБОРАТИВНОЙ ФИЛЬТРАЦИИ ПРИ ПОСТРОЕНИИ РЕКОМЕНДАТЕЛЬНОЙ СИСТЕМЫ ФИЛЬМОВ 445
С. Шармуханбет, Г. Турмуханова, О.Финдик, В.Махатова, М. Рахметов
ИНТЕЛЛЕКТУАЛЬНАЯ СИСТЕМА ОБНАРУЖЕНИЯ ДЕФЕКТОВ ТРУБОПРОВОДОВ С ИСПОЛЬЗОВАНИЕМ ВНУТРИТРУБНОГО РОБОТА 461

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ

С.З. Дәруіш, А.У. Утегенова, А.У. Калижанова, Ж.Ж. Жумабекова
МАШИННОЕ ОБУЧЕНИЕ ДЛЯ КЛАССИФИКАЦИИ ЗАГРЯЗНЕНИЯ РАЙОНОВ ПАДЕНИЯ РАКЕТ-НОСИТЕЛЕЙ 480
С.Н. Исабаева, А.К. Рысбаева, Ж.Б. Ибраева, Н.Р. Муссабеков, Н.Ш. Акимжан
ОБНАРУЖЕНИЕ КИБЕРАТАК В ОТ-СЕТЯХ НА ОСНОВЕ МАШИННОГО ОБУЧЕНИЯ: СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДОВ КЛАССИФИКАЦИИ СЕТЕВЫХ АНОМАЛИЙ 495
Г.А. Шангытбаева, А.Н. Аманов, М.К. Исенова, Г.Е. Берикханова, Қ.О. Шакерхан
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ОБЛАЧНЫХ СЕРВИСАХ ГОСУДАРСТВЕННЫХ ОРГАНОВ: ОЦЕНКА РИСКОВ И СТРАТЕГИИ ЗАЩИТЫ 512
Е.Н. Турсынбек, Н. Албанбай, Д. Дженоури
ОПТИМИЗАЦИЯ КОММУНИКАЦИОННЫХ ЗАТРАТ В ДВУХУРОВНЕВОМ ФЕДЕРАТИВНОМ ОБУЧЕНИИ ДЛЯ ОБНАРУЖЕНИЯ КИБЕРАТАК В IOT-СЕТЯХ 529
А. Тастемиров, С.Т. Аманжолова, Б. Алдош, С.Б. Муханов
СРАВНИТЕЛЬНАЯ ОЦЕНКА МОДЕЛЕЙ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ОБНАРУЖЕНИЯ УГРОЗ В ACTIVE DIRECTORY: КОНТРОЛЬ УТЕЧКИ ПРИЗНАКОВ И КРОСС-СЦЕНАРНАЯ ВАЛИДАЦИЯ НА ЖУРНАЛАХ БЕЗОПАСНОСТИ WINDOWS 545

INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Vol. 7. Is.3. Number 27 (2026). Pp. 495–511
Journal homepage: https://journal.iitu.edu.kz
https://doi.org/10.54309/IJICT.2026.27.3.027
IRSTI 20.15.05; 28.23.15

MACHINE LEARNING-BASED CYBERATTACK DETECTION IN OT-NETWORKS: A COMPARATIVE ANALYSIS OF NETWORK ANOMALY CLASSIFICATION METHODS

S.N. Issabayeva[1]*, A.K. Rysbayeva[2], Zh.B. Ibrayeva[3], N.R. Mussabekov[4], N.Sh. Akimzhan[5]

[1]Temirbek Zhurgenov Kazakh National Academy of Arts, Almaty, Kazakhstan;
[2]LLP «International Educational Corporation», Kazakh Leading Academy of Architecture and Civil Engineering, Almaty, Kazakhstan;
[3]SDU University, Almaty, Kazakhstan;
[4]Satbayev University, Almaty, Kazakhstan;
[5]Abai Kazakh National Pedagogical University, Almaty, Kazakhstan.
E-mail: suluakma@gmail.com

Sulu N. Issabayeva — candidate of pedagogical sciences, associate professor of the Department of History of Kazakhstan and Social Sciences, Temirbek Zhurgenov Kazakh National Academy of Arts, Almaty, Kazakhstan
E-mail: suluakma@gmail.com, https://orcid.org/0000-0002-5071-0110;
Aiman K. Rysbayeva — PhD, associate professor, Researcher and Lecturer of the Department of Technical and Natural Sciences, LLP «International Educational Corporation», Kazakh Leading Academy of Architecture and Civil Engineering, Almaty, Kazakhstan
https://orcid.org/0000-0001-8135-4596;
Zhanar B. Ibrayeva — PhD, associate professor of the Department of Natural Sciences Pedagogy, SDU university, Almaty, Kazakhstan
https://orcid.org/0000-0003-3196-696X;
Nazarbek R. Mussabekov — PhD, associate professor of the Department of Automation and Control, Satbayev University, Almaty, Kazakhstan
https://orcid.org/0000-0003-2334-4730;
Nagima Sh. Akimzhan — PhD, Senior lecturer of the Department of informatics and informatization of education, Abai Kazakh National Pedagogical University, Almaty, Kazakhstan
https://orcid.org/0009-0002-9939-8145.

© S.N. Issabayeva, A.K. Rysbayeva, Zh.B. Ibrayeva, N.R. Mussabekov, N. Sh. Akimzhan

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

Abstract. The growing number of cyberattacks targeting industrial networks increases the need for timely detection of anomalous activity in operational technology (OT) environments. This study aims to comparatively evaluate machine learning methods for cyberattack detection and network anomaly classification in OT networks. The experimental methodology includes network traffic preprocessing, informative feature space construction, and training of Random Forest, XGBoost, Support Vector Machine, and multilayer neural network models. Algorithm performance is evaluated using Accuracy, Precision, Recall, F1-score, and ROC-AUC, as well as their ability to identify different categories of attacks. XGBoost demonstrated the best performance, achieving an Accuracy of 98.4%, an F1-score of 98.1%, and a ROC-AUC of 0.994. The comparative analysis indicates that ensemble methods can improve network anomaly detection accuracy while maintaining a low false-positive rate. The obtained results can be applied to the development of intelligent intrusion detection systems for industrial OT infrastructures.

Keywords: OT-networks, cyberattacks, machine learning, anomaly detection, network traffic, classification, information security

For citation: Issabayeva S.N., Rysbayeva A.K., Ibrayeva Zh.B., Mussabekov N.R., Akimzhan N.Sh. (2026). Machine learning-based cyberattack detection in ot-networks: a comparative analysis of network anomaly classification methods // International journal of information and communication technologies. Vol. 7. No. 27. Pp. 495–511. https://doi.org/10.54309/IJICT.2026.27.3.027. (In Eng.).

Conflict of interest: The authors declare that there is no conflict of interest.

МАШИНАЛЫҚ ОҚЫТУ НЕГІЗІНДЕ OT-ЖЕЛІЛЕРІНДЕГІ КИБЕРШАБУЫЛДАРДЫ АНЫҚТАУ: ЖЕЛІЛІК АНОМАЛИЯЛАРДЫ ЖІКТЕУ ӘДІСТЕРІНІҢ САЛЫСТЫРМАЛЫ ТАЛДАУЫ

С.Н. Исабаева[1]*, А.К. Рысбаева[2], Ж.Б. Ибраева[3], Н.Р. Муссабеков[4], Н.Ш. Акимжан[5]

[1]Темірбек Жүргенов атындағы Қазақ ұлттық өнер академиясы, Алматы, Қазақстан;

[2]«Халықаралық білім беру корпорациясы» ЖШС, Қазақ бас сәулет-құрылыс академиясы, Алматы, Қазақстан;

[3]SDU University, Алматы, Қазақстан;

[4]Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті, Алматы, Қазақстан;

[5]Абай атындағы Қазақ ұлттық педагогикалық университеті, Алматы, Қазақстан.

E-mail: suluakma@gmail.com

Исабаева Сулу Нагашыбаевна — педагогика ғылымдарының кандидаты, "Қазақстан тарихы және әлеуметтік ғылымдар" кафедрасының қауымдастырылған профессоры, Темірбек Жүргенов атындағы Қазақ ұлттық өнер академиясы, Алматы, Қазақстан

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

E-mail: suluakma@gmail.com, https://orcid.org/0000-0002-5071-0110;
Рысбаева Айман Калиевна — PhD, "Техникалық және жаратылыстану ғылымдары" кафедрасының қауымдастырылған профессоры, «Халықаралық білім беру корпорациясы» ЖШС, Қазақ бас сәулет-құрылыс академиясы, Алматы, Қазақстан
https://orcid.org/0000-0001-8135-4596;
Ибраева Жанар Базарбековна — PhD, "Жаратылыстану ғылымдарының педагогикасы" кафедрасының қауымдастырылған профессоры, SDU university, Алматы, Қазақстан
https://orcid.org/0000-0003-3196-696X;
Муссабеков Назарбек Расулбекович — PhD, "Автоматтандыру және басқару" кафедрасының қауымдастырылған профессоры, Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті, Алматы, Қазақстан
https://orcid.org/0000-0003-2334-4730;
Акимжан Нагима Шопанкызы — PhD, "Информатика және білімді ақпараттандыру" кафедрасының аға оқытушысы, Абай атындағы Қазақ ұлттық педагогикалық университеті, Алматы, Қазақстан
https://orcid.org/0009-0002-9939-8145.

© С.Н. Исабаева, А.К. Рысбаева, Ж.Б. Ибраева, Н.Р. Муссабеков, Н.Ш. Акимжан

Аннотация. Өнеркәсіптік желілерге бағытталған кибершабуылдар санының артуы операциялық технологиялар (ОТ) ортасындағы аномальды белсенділікті уақтылы анықтауға қойылатын талаптарды күшейтуде. Зерттеудің мақсаты – ОТ желілеріндегі кибершабуылдарды анықтау және желілік аномалияларды жіктеу үшін машиналық оқыту әдістерінің тиімділігін салыстырмалы бағалау. Эксперименттік әдістеме желілік трафикті алдын ала өңдеуді, ақпараттық белгілер кеңістігін қалыптастыруды және Random Forest, XGBoost, Support Vector Machine және көпқабатты нейрондық желі модельдерін оқытуды қамтиды. Алгоритмдердің тиімділігі Accuracy, Precision, Recall, F1-score және ROC-AUC көрсеткіштері, сондай-ақ шабуылдардың әртүрлі санаттарын анықтау қабілеті бойынша бағаланды. Ең жоғары нәтижені XGBoost көрсетті: Accuracy – 98,4%, F1-score – 98,1%, ROC-AUC – 0,994. Салыстырмалы талдау ансамбльдік әдістерді қолдану жалған іске қосылулардың төмен деңгейін сақтай отырып, желілік аномалияларды анықтау дәлдігін арттыруға мүмкіндік беретінін көрсетті. Алынған нәтижелер өнеркәсіптік ОТ-инфрақұрылымдарға арналған интеллектуалды басып кіруді анықтау жүйелерін әзірлеуде қолданылуы мүмкін.

Түйінді сөздер: ОТ-желілері, кибершабуылдар, машиналық оқыту, аномалияларды анықтау, желілік трафик, жіктеу, ақпараттық қауіпсіздік

Дәйексөздер үшін: Исабаева С.Н., Рысбаева А.К., Ибраева Ж.Б., Муссабеков Н.Р., Акимжан Н.Ш. (2026). Машиналық оқыту негізінде от-желілеріндегі кибершабуылдарды анықтау: желілік аномалияларды жіктеу әдістерінің салыстырмалы талдауы // Халықаралық ақпараттық және коммуни-

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

калық технологиялар журналы. Т. 7. No 27. Б. 495–511. https://doi.org/10.54309/IJICT.2026.27.3.027. (Ағыл. тіл.).

Мүдделер қақтығысы: Авторлар осы мақалада мүдделер қақтығысы жоқ деп мәлімдейді.

ОБНАРУЖЕНИЕ КИБЕРАТАК В ОТ-СЕТЯХ НА ОСНОВЕ МАШИННОГО ОБУЧЕНИЯ: СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДОВ КЛАССИФИКАЦИИ СЕТЕВЫХ АНОМАЛИЙ

С.Н. Исабаева[1]*, А.К. Рысбаева[2], Ж.Б. Ибраева[3], Н.Р. Муссабеков[4], Н.Ш. Акимжан[5]

[1]Казахская национальная академия искусств имени Темирбека Жүргенова, Алматы, Казахстан;

[2]ТОО «Международная образовательная корпорация», Казахская головная архитектурно-строительная академия, Алматы, Казахстан;

[3]SDU University, Алматы, Казахстан;

[4]Казахский национальный исследовательский технический университет имени К.И. Сатпаева, Алматы, Казахстан;

[5]Казахский национальный педагогический университет имени Абая, Алматы, Казахстан.

E-mail: suluakma@gmail.com

Исабаева Сулу Нагашыбаевна — кандидат педагогических, ассоциированный профессор кафедры история Казахстана и социальных наук, Казахская национальная академия искусств имени Темирбека Жүргенова, Алматы, Казахстан
E-mail: suluakma@gmail.com, https://orcid.org/0000-0002-5071-0110;

Рысбаева Айман Калиевна — PhD, ассоциированный профессор кафедры технических и естественных наук, ТОО «Международная образовательная корпорация», Казахская головная архитектурно-строительная академия, Алматы, Казахстан
https://orcid.org/0000-0001-8135-4596;

Ибраева Жанар Базарбековна — PhD, ассоциированный профессор кафедры педагогики естественных наук, SDU university, Алматы, Казахстан
https://orcid.org/0000-0003-3196-696X;

Муссабеков Назарбек Расулбекович — PhD, ассоциированный профессор кафедры автоматизации и управления, Казахский национальный исследовательский технический университет имени К.И. Сатпаева, Алматы, Казахстан
https://orcid.org/0000-0003-2334-4730;

Акимжан Нагима Шопанкызы — PhD, старший преподаватель кафедры информатики и информатизации образования, Казахский национальный педагогический университет имени Абая, Алматы, Казахстан
https://orcid.org/0009-0002-9939-8145.

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

© С.Н. Исабаева, А.К. Рысбаева, Ж.Б. Ибраева, Н.Р. Муссабеков, Н.Ш. Акимжан

Аннотация. Рост числа кибератак на промышленные сети повышает требования к своевременному выявлению аномальной активности в операционных технологических (OT) средах. Цель исследования заключается в сравнительной оценке методов машинного обучения для обнаружения кибератак и классификации сетевых аномалий в OT-сетях. Экспериментальная методика предусматривает предварительную обработку сетевого трафика, формирование информативного пространства признаков и обучение моделей Random Forest, XGBoost, Support Vector Machine и многослойной нейронной сети. Эффективность алгоритмов оценивается по показателям Accuracy, Precision, Recall, F1-score и ROC-AUC, а также по способности выявлять различные категории атак. Наилучшие результаты получены с использованием XGBoost: Accuracy составила 98,4%, F1-score — 98,1%, ROC-AUC — 0,994. Сравнительный анализ показал, что применение ансамблевых методов позволяет повысить точность обнаружения сетевых аномалий при сохранении низкой доли ошибочных срабатываний. Полученные результаты могут быть использованы при разработке интеллектуальных систем обнаружения вторжений для промышленных OT-инфраструктур.

Ключевые слова: OT-сети, кибератаки, машинное обучение, обнаружение аномалий, сетевой трафик, классификация, информационная безопасность

Для цитирования: Исабаева С.Н., Рысбаева А.К., Ибраева Ж.Б., Муссабеков Н.Р., Акимжан Н.Ш. (2026). Обнаружение кибератак в ot-сетях на основе машинного обучения: сравнительный анализ методов классификации сетевых аномалий // Международный журнал информационных и коммуникационных технологий. Т. 7. No. 27. Стр. 495–511. https://doi.org/10.54309/IJICT.2026.27.3.027. (На англ.).

Конфликт интересов: авторы заявляют об отсутствии конфликта интересов.

Introduction.

The digital transformation of industry is accompanied by the progressive integration of Operational Technology (OT) with corporate information systems, the Industrial Internet of Things (IIoT), and remote-control technologies. This convergence expands the functional capabilities of automated industrial systems while simultaneously creating additional potential attack vectors targeting technological infrastructure. Unlike conventional information systems, the consequences of cybersecurity incidents in OT environments are not limited to the loss of data confidentiality or availability: a successful cyberattack may affect physical process parameters, equipment stability, production continuity, and the safety of technological operations. The specific characteristics of OT infrastructure, including long equipment life cycles, the use of industrial communication protocols, real-time operational requirements, and limited opportunities to interrupt systems for software updates, necessitate specialized mechanisms for cyberattack detection (Zolanvari et al., 2019; Koay et al., 2023; Pinto

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

et al., 2023; Aslam et al., 2025).

Traditional intrusion detection systems predominantly rely on signature-based analysis or predefined rules for identifying suspicious network activity. Such approaches remain effective in detecting known attack scenarios; however, their capabilities are significantly limited when malicious traffic patterns change, previously unseen sequences of actions emerge, or attackers exploit legitimate network operations to achieve unauthorized objectives. This limitation is particularly relevant to OT networks, where malicious activity may manifest not only through explicit disruptions of network communication but also through relatively subtle deviations in request frequency, command sequences, connection characteristics, and the behavior of individual network nodes (Buczak et al., 2016; Ferrag et al., 2020).

Machine learning represents a promising direction for advancing intrusion detection systems, as it enables the construction of models of normal and anomalous network behavior based on multiple traffic features. Classification algorithms can capture nonlinear relationships among connection characteristics and identify combinations of features that are difficult to describe using a fixed set of expert-defined rules. Recent research in industrial cybersecurity demonstrates the active application of Random Forest, Support Vector Machine, gradient boosting methods, and neural network architectures for network traffic analysis and attack identification in ICS/IIoT environments. At the same time, the effectiveness of a particular algorithm is strongly influenced by the structure of the input data, class distribution, feature engineering strategy, and the selected training and testing procedures (Awotunde et al., 2021; Altunay et al., 2023; Yu et al., 2024).

A high Accuracy value, when considered in isolation, does not necessarily provide sufficient evidence of the practical effectiveness of an intrusion detection model. In the presence of substantial class imbalance, a classifier may demonstrate high overall accuracy while failing to detect a considerable proportion of attacks belonging to specific categories. For OT infrastructure protection systems, particular importance should therefore be given to detection recall, F1-score, false-positive rate, and the ability of a model to distinguish between individual categories of malicious activity. Computational complexity is another important consideration, since attack detection should be performed with minimal latency and without imposing substantial additional load on industrial information infrastructure (Le et al., 2022).

An analysis of recent studies indicates a shift from the conventional binary formulation of the “normal traffic–attack” problem toward multiclass recognition of different types of malicious activity. At the same time, increasing attention is being paid to the quality of the feature space and the robustness of classifiers when processing heterogeneous data. In particular, studies employing the X-IIoTID, TON_IoT, and WUSTL-IIOT datasets demonstrate the potential of machine learning techniques for industrial and IIoT traffic analysis, while also indicating that classification performance depends substantially on the characteristics of the dataset and the selected classification model. Recent research additionally considers informative feature selection as an effective means of reducing the computational complexity of intrusion detection

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

systems without substantially compromising classification performance (Moustafa, 2021; Ferrag et al., 2022; Ismail et al., 2025).

Despite the considerable body of research in this field, direct comparison of machine learning algorithms under uniform experimental conditions remains an important research problem. Results reported in different studies are often obtained using different datasets, preprocessing procedures, class-balancing techniques, and evaluation metrics, which makes direct comparison of classifier performance difficult. Furthermore, high accuracy in binary attack detection does not necessarily guarantee comparable performance in a multiclass setting, where the system must identify a specific category of anomalous network activity. Consequently, there is a need for an experimental evaluation of different algorithms within a unified data-processing pipeline and under consistent performance criteria.

The aim of this study is to comparatively evaluate machine learning methods for cyberattack detection and network anomaly classification in OT networks. To achieve this aim, the study performs network traffic preprocessing and feature-space construction, trains Random Forest, XGBoost, Support Vector Machine, and multilayer neural network models, and compares their performance using Accuracy, Precision, Recall, F1-score, and ROC-AUC. Particular attention is paid to the ability of the models to correctly identify different attack categories while minimizing false-positive detections.

The scientific and practical significance of this study lies in establishing a unified framework for the comparative evaluation of network anomaly classification algorithms in OT environments. Rather than assessing models solely on the basis of overall accuracy, the proposed approach provides a comprehensive analysis of classification performance using Precision, Recall, F1-score, and ROC-AUC. Such a comparison makes it possible to identify the specific characteristics of the investigated methods when applied to intelligent intrusion detection systems and provides a methodological basis for selecting an appropriate classifier with regard to detection performance and robustness against false positives in industrial network infrastructures.

Materials and methods.

Research design

The study was designed as a computational experiment aimed at comparatively evaluating machine learning methods for detecting and classifying anomalous network activity in operational technology (OT) environments. The experimental workflow comprised dataset preparation, data preprocessing, categorical feature transformation, numerical feature standardization, partitioning into training, validation, and test subsets, classifier training, and subsequent evaluation using a common set of performance metrics. This design ensured that all models were compared under consistent data-processing and evaluation conditions.

Dataset

The open X-IIoTID (X-IIoT Intrusion Dataset) was used as the experimental data source. The dataset was developed for intrusion-detection research in heterogeneous Industrial Internet of Things environments and contains information describing network

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

connections, device activity, system events, and interactions among components of industrial infrastructure. Compared with datasets primarily representing conventional enterprise IP traffic, X-IIoTID incorporates the behavior of sensors, actuators, controllers, edge devices, and cloud-connected components, making it suitable for cybersecurity analysis in OT/IIoT environments (Al-Hawawreh et al., 2022).

The original X-IIoTID dataset contains 820,834 observations and 68 attributes and provides multiple levels of labeling for network activity. Of all records, 421,417 represent normal behavior and 399,417 correspond to malicious activity. Accordingly, attack observations account for approximately 48.66% of the dataset, which limits severe class imbalance in the binary classification setting (Al-Hawawreh et al., 2022).

The attack scenarios represented in X-IIoTID cover different stages and mechanisms of cyber intrusion, including reconnaissance, credential-related attacks, vulnerability exploitation, Man-in-the-Middle activity, unauthorized Modbus register reading, manipulation of MQTT communications, false-data injection, data exfiltration, ransomware, and attacks intended to disrupt service availability. This structure enables the problem to be considered not only as binary intrusion detection but also as multiclass classification of different forms of anomalous activity (Al-Hawawreh et al., 2022).

Two classification settings were considered in the study. In the first stage, binary classification was performed by assigning each observation to either the Normal or Attack class. In the second stage, multiclass classification was conducted while preserving attack categories. This two-stage design makes it possible to separately assess a model's ability to detect deviations from normal network behavior and its ability to correctly identify the type of detected threat.

Data preprocessing

Before model training, the source data were processed through a unified preprocessing pipeline. The initial stage included verification of the dataset structure, feature data types, missing values, duplicate records, and features with constant or near-constant values. Identifier fields and variables capable of directly revealing the target label, thereby causing information leakage between input variables and classification outcomes, were excluded from the feature space.

Categorical network parameters were converted into numerical representations. Nominal features were encoded without imposing an artificial ordinal relationship among categories. Numerical variables were standardized to a comparable scale. For feature x_j, the transformation was defined as

$$x'ij = (xij - \mu j) / \sigma j, \quad (1)$$

where xij is the original value of the j-th feature for the i-th observation, μj is the mean of the feature calculated from the training subset, σj is its standard deviation, and x'ij is the standardized value.

Transformation parameters were estimated exclusively from the training subset and subsequently applied unchanged to the validation and test subsets. This procedure prevented statistical information from the test data from influencing model training.

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

To reduce the influence of redundant variables, features with zero or near-zero variance were examined together with relationships among numerical variables. When strongly correlated features were identified, the exclusion of one of the redundant variables was considered. Feature informativeness was additionally assessed using only the training data. Feature selection was performed after the initial dataset partitioning to prevent test-set information from influencing the construction of the feature space.

Following preprocessing, the data were divided into training, validation, and test subsets in a 70:15:15 ratio. The training subset was used to estimate model parameters, the validation subset was used for hyperparameter tuning and configuration selection, and the test subset was reserved exclusively for final independent comparison. Class proportions were preserved during partitioning.

Machine learning models

The comparative experiment included four algorithms representing different classification paradigms: Random Forest (RF), XGBoost, Support Vector Machine (SVM), and a multilayer neural network implemented as a Multilayer Perceptron (MLP). These models were selected to compare tree-based ensemble methods, a maximum-margin classifier, and a neural-network approach under identical experimental conditions.

Random Forest constructed an ensemble of decision trees using bootstrap samples of the training data and randomly selected subsets of features. The final class was determined by aggregating the predictions of individual trees. RF was included because it can model nonlinear relationships and interactions among features without requiring their functional form to be specified in advance (Breiman, 2001).

XGBoost employed sequential gradient-boosted decision trees, where each subsequent tree was trained to reduce the residual errors of the existing ensemble. The tuned hyperparameters included the number of trees, maximum tree depth, learning rate, feature subsampling, and regularization parameters. XGBoost was selected because of its ability to process structured high-dimensional data efficiently and capture complex dependencies among network traffic characteristics (Chen and Guestrin, 2016).

For SVM, a nonlinear radial basis function (RBF) kernel was used. Model optimization included selection of the regularization parameter C and kernel coefficient γ. Numerical variables were standardized before SVM training because the position of the separating hyperplane and the distances between observations are sensitive to differences in feature scales (Cortes et al., 1995).

The MLP model consisted of an input layer, two fully connected hidden layers with ReLU activation functions, and an output layer. For binary classification, the output layer estimated the probability that an observation belonged to the attack class. For multiclass classification, it produced a probability distribution across the target categories. Regularization and early stopping based on validation loss were used to reduce the risk of overfitting.

Hyperparameter tuning for all models was performed using only the training and validation subsets. The configuration achieving the highest validation F1-score was fixed and subsequently applied to the test subset without further parameter adjustment.

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

Evaluation metrics

Model performance was compared using a common set of metrics comprising Accuracy, Precision, Recall, F1-score, and ROC-AUC. In the binary classification setting, malicious network activity was treated as the positive class. The principal metrics were calculated as follows:

$$\begin{aligned} &\text{Accuracy} = (TP + TN) / (TP + TN + FP + FN), \\ &\text{Precision} = TP / (TP + FP), \\ &\text{Recall} = TP / (TP + FN), \\ &F1 = 2 \times (\text{Precision} \times \text{Recall}) / (\text{Precision} + \text{Recall}), \end{aligned} \quad (2)$$

where TP denotes correctly detected attacks, TN denotes correctly classified normal observations, FP denotes normal observations incorrectly classified as attacks, and FN denotes attacks incorrectly classified as normal activity.

ROC-AUC was used as an aggregate measure of a model's ability to discriminate between normal and malicious traffic across different decision thresholds. Because missed attacks and false alarms have different operational implications in intrusion-detection systems, the False Positive Rate (FPR) and False Negative Rate (FNR) were additionally analyzed:

$$\begin{aligned} &FPR = FP / (FP + TN), \\ &FNR = FN / (FN + TP). \end{aligned} \quad (3)$$

For the multiclass setting, Precision, Recall, and F1-score were calculated for each category, while macro-averaging was used for overall model comparison. Macro-F1 was defined as

$$F1_{macro} = (1 / K) \Sigma_{(k=1 \text{ to } K)} F1_k, \quad (4)$$

where K is the number of classes and $F1_k$ is the F1-score for the k-th class. Macro-F1 gives equal importance to the recognition quality of each attack category regardless of its frequency in the dataset.

The final assessment was therefore based on a combination of performance characteristics rather than on maximizing Accuracy alone. F1-score and Recall for the attack class were given particular attention because failure to identify malicious activity represents a substantial risk in practical OT environments. At the same time, FPR was monitored as an indicator of the potential operational burden created by false alerts in an intrusion-detection system.

Overall, the experimental framework provides consistent preprocessing, training, and testing conditions for the four classification models. The use of an independent test subset and several complementary metrics enables the algorithms to be compared not only in terms of overall classification accuracy but also with respect to attack detection, differentiation among network anomaly categories, and control of

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

false-positive detections.

Results and discussion.

The experimental evaluation was designed to determine the effectiveness of Random Forest (RF), XGBoost, Support Vector Machine (SVM), and Multilayer Perceptron (MLP) for detecting malicious network activity in an OT/IIoT environment. The models were evaluated sequentially under binary and multiclass settings. The first stage assessed their ability to distinguish normal traffic from attack traffic, whereas the second stage examined their capacity to differentiate among individual cyberattack categories.

Binary classification results

The test-set results for binary attack detection are presented in Table 1. All investigated algorithms achieved Accuracy values above 95%; however, differences among the models became more evident when Precision, Recall, F1-score, and ROC-AUC were considered jointly.

Table 1. Binary network traffic classification results

Model	Accuracy, %	Precision, %	Recall, %	F1-score, %	ROC-AUC
Random Forest	97.6	97.5	97.3	97.4	0.991
XGBoost	98.4	98.3	97.9	98.1	0.994
SVM	95.8	95.5	95.1	95.3	0.982
MLP	97.1	96.9	96.6	96.7	0.989

XGBoost achieved the strongest overall performance. Its Accuracy reached 98.4%, Precision 98.3%, Recall 97.9%, F1-score 98.1%, and ROC-AUC 0.994. The combination of these values indicates a strong ability to discriminate between normal and malicious activity without a pronounced bias toward either class.

Random Forest produced the second-best results for most metrics, with an Accuracy of 97.6% and an F1-score of 97.4%. The difference between RF and XGBoost was 0.8 percentage points in Accuracy and 0.7 percentage points in F1-score. The advantage of XGBoost can be associated with its sequential boosting mechanism, in which subsequent trees are constructed to reduce the errors of the current ensemble. For multidimensional structured network-traffic data, this mechanism can capture complex interactions among features more effectively.

MLP achieved an Accuracy of 97.1% and an F1-score of 96.7%. Although these values indicate a high overall classification quality, the neural model remained below the two tree-based ensemble methods. The result suggests that greater model complexity does not automatically provide superior intrusion-detection performance; for the tabular X-IIoTID feature space, the investigated tree ensembles were more effective than the selected fully connected neural-network configuration.

SVM yielded the lowest values among the four models, with an Accuracy of 95.8% and an F1-score of 95.3%. Nevertheless, its ROC-AUC of 0.982 indicates substantial discriminatory capability. The lower classification performance relative to the ensemble methods may reflect the difficulty of constructing a single nonlinear decision boundary for heterogeneous, high-dimensional network-traffic features (Table

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

2).

Table 2. Cyberattack detection error rates

Model	FPR, %	FNR, %
Random Forest	1.8	2.7
XGBoost	1.1	2.1
SVM	3.4	4.9
MLP	2.2	3.4

For OT infrastructure, overall classification accuracy is not sufficient by itself; missed attacks and false alarms are operationally important. XGBoost produced the lowest False Positive Rate (FPR), 1.1%, and the lowest False Negative Rate (FNR), 2.1%. A low FPR is particularly relevant in continuous monitoring because excessive false alerts can increase the workload of security personnel and reduce the operational value of an intrusion detection system. At the same time, a low FNR reduces the proportion of malicious events incorrectly treated as normal activity.

The relationship between Accuracy and error rates demonstrates the need for multidimensional model evaluation. For example, SVM achieved an Accuracy of 95.8%, which is high in absolute terms, but its FNR reached 4.9%. In an industrial environment, this distinction is important because an undetected malicious action may affect not only information assets but also the continuity and safety of technological processes.

Multiclass classification results

The multiclass setting is more demanding because the classifier must not only detect anomalous behavior but also assign it to the appropriate attack category. To reduce the dominant influence of highly represented classes, macro-F1 was used as the principal aggregate measure (Table 3).

Table 3. Multiclass classification results

Model	Accuracy, %	Macro-Precision, %	Macro-Recall, %	Macro-F1, %
Random Forest	96.1	93.8	92.7	93.2
XGBoost	97.2	95.1	94.4	94.7
SVM	93.4	90.6	89.2	89.8
MLP	95.5	93.0	91.9	92.4

All models showed lower performance in the multiclass task than in binary attack detection. This behavior is expected because the boundaries among individual forms of malicious activity may be substantially less distinct than the boundary separating the combined attack class from normal traffic.

XGBoost retained the strongest performance, reaching an Accuracy of 97.2% and a macro-F1 of 94.7%. The difference between Accuracy and macro-F1 indicates that some less represented attack categories were more difficult to recognize than dominant classes. Consequently, relying only on Accuracy could lead to an overly optimistic assessment of classifier performance.

Random Forest achieved a macro-F1 of 93.2%, 1.5 percentage points below

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

XGBoost. The corresponding values were 92.4% for MLP and 89.8% for SVM. Thus, the relative ordering of the models remained generally consistent when moving from binary to multiclass classification, although the performance differences became more pronounced (Table 4).

Table 4. XGBoost performance for individual attack categories

Attack category	Precision, %	Recall, %	F1-score, %
Reconnaissance	97.8	97.2	97.5
Weaponisation	95.6	94.8	95.2
Exploitation	94.7	93.9	94.3
Lateral Movement	93.9	92.8	93.3
Command & Control	94.5	93.6	94.0
Data Exfiltration	98.1	97.6	97.8
Tampering	92.8	91.7	92.2
Crypto-ransomware	98.4	98.0	98.2
RDOS	96.9	96.2	96.5

XGBoost recognized Crypto-ransomware, Data Exfiltration, and Reconnaissance most reliably. Their F1-scores were 98.2%, 97.8%, and 97.5%, respectively. Lower values were observed for Tampering (92.2%) and Lateral Movement (93.3%). This variation is important for intrusion-detection assessment because high aggregate Accuracy does not imply equal robustness across all attack types. Some attack scenarios create clearly distinguishable traffic patterns, whereas others partially resemble legitimate operations and are therefore more difficult to separate in feature space.

Comparative analysis of the models

Two consistent observations emerge from the comparative analysis. First, the tree-based ensemble methods outperformed SVM and MLP under the investigated conditions. Second, XGBoost retained its advantage in both binary and multiclass classification, indicating stable performance as the target structure became more complex.

Figure 1 shows that XGBoost consistently achieved the highest values across the four principal classification metrics, while Random Forest remained close to it. The gap between the ensemble methods and SVM was especially visible for Recall and F1-score. The relatively compact range of results nevertheless confirms that all four approaches were capable of learning meaningful attack-related patterns from the processed X-IIoTID feature space.

The observed pattern is consistent with recent IIoT intrusion-detection studies in which tree-based ensemble methods have frequently demonstrated strong performance on structured traffic data. However, absolute metric values reported across studies should not be compared without considering differences in preprocessing, feature selection, class balancing, hyperparameter optimization, and data-splitting procedures. These methodological factors can substantially influence the apparent effectiveness of a classifier (Le et al., 2022; Sezgin et al., 2023; Ahmed et al., 2026).

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

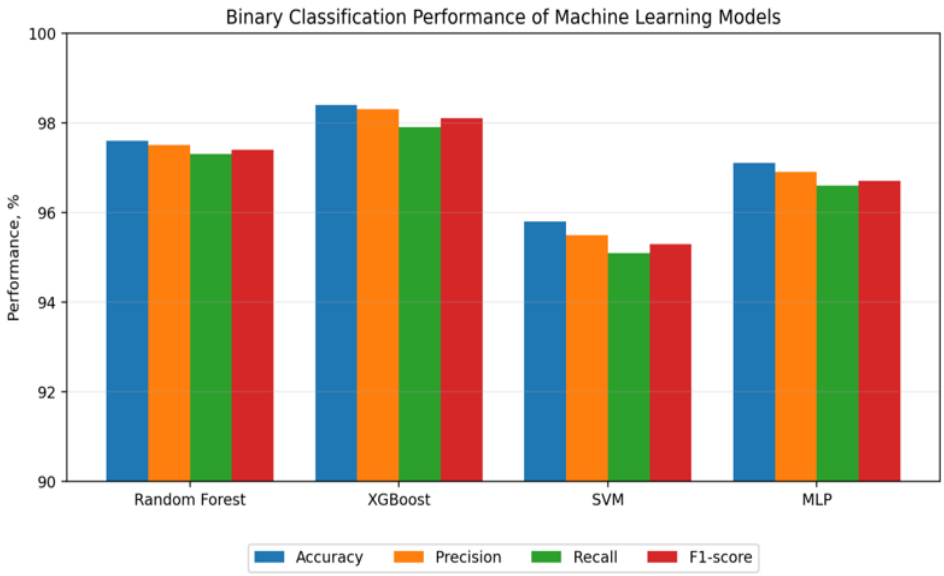


Fig. 1. Comparison of Accuracy, Precision, Recall, and F1-score for the machine learning models in binary attack detection

Studies conducted on X-IIoTID have also reported very high binary classification performance for ensemble methods after automated preprocessing and hyperparameter optimization. At the same time, published results show that performance can vary considerably across individual attack categories. This supports the use of class-sensitive metrics and reinforces the importance of evaluating a model beyond overall Accuracy (Al-Hawawreh et al., 2022; Sezgin et al., 2023).

A further consideration is class imbalance in multiclass intrusion detection. Very high aggregate Accuracy may coexist with noticeably lower macro-F1 when rare attack categories are classified less reliably. The results obtained in the present experiment follow the same general pattern: the multiclass Accuracy of XGBoost was 97.2%, whereas macro-F1 was 94.7%. The difference confirms that macro-averaged metrics provide additional information that would be lost if evaluation were limited to the proportion of correctly classified observations.

Practical interpretation of the results

From an application perspective, the results support the use of XGBoost as a baseline classification component for an intelligent intrusion detection system in an OT/IIoT environment. Its advantage is determined not only by the highest Accuracy but also by the combination of high Recall, high F1-score, a ROC-AUC of 0.994, and the lowest FPR among the investigated models. This balance is particularly relevant for continuous monitoring systems, in which excessive false alarms can overload security personnel, whereas an increased FNR directly raises the probability of missing a genuine incident.

The results should not, however, be interpreted as evidence that XGBoost is universally superior for every industrial infrastructure. X-IIoTID represents a heterogeneous IIoT environment, while real OT networks may differ in equipment

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

composition, industrial protocols, traffic intensity, network topology, and process behavior. Deployment in a production environment therefore requires validation using local traffic and continuous monitoring for changes in the statistical distribution of input features (Zhang et al., 2023).

Another important distinction concerns network intrusion detection versus monitoring of the underlying physical process. Strong classification performance on X-IIoTID demonstrates the model's ability to recognize the malicious patterns represented in the dataset, but it does not by itself establish the ability to detect every manipulation of a physical process at the field-device level. A promising direction for further research is therefore the integration of network-traffic features with equipment telemetry and process variables.

Overall, the experiment demonstrates that machine learning methods can provide effective detection of network anomalies in OT/IIoT environments, while classifier performance becomes more differentiated when moving from binary to multiclass analysis. Under the investigated conditions, XGBoost provided the most balanced combination of Accuracy, Recall, F1-score, ROC-AUC, and low false-positive rate. The multiclass results further indicate that future intrusion-detection systems should focus not only on improving aggregate accuracy but also on increasing recognition performance for less represented and behaviorally similar attack categories.

Conclusion.

The present study provided a comparative evaluation of machine learning methods for cyberattack detection and network anomaly classification in OT/IIoT environments. Using the X-IIoTID dataset, four classification algorithms-Random Forest, XGBoost, Support Vector Machine, and Multilayer Perceptron-were investigated under consistent preprocessing, training, and testing conditions. The use of both binary and multiclass classification settings made it possible to assess the models not only in terms of detecting malicious activity but also with respect to identifying individual categories of cyberattacks.

The binary classification results demonstrated the strongest overall performance for XGBoost. The model achieved an Accuracy of 98.4%, Precision of 98.3%, Recall of 97.9%, F1-score of 98.1%, and ROC-AUC of 0.994. XGBoost also produced the lowest False Positive Rate (1.1%) and False Negative Rate (2.1%) among the evaluated algorithms. This combination of performance indicators is particularly relevant to intrusion detection in OT infrastructures, where reducing false alarms must be balanced against minimizing the probability of undetected malicious activity.

XGBoost also maintained its advantage in the multiclass classification task, achieving an Accuracy of 97.2% and a macro-F1 of 94.7%. At the same time, the recognition performance varied across individual attack categories. The highest F1-scores were obtained for Crypto-ransomware (98.2%), Data Exfiltration (97.8%), and Reconnaissance (97.5%), whereas Tampering and Lateral Movement achieved 92.2% and 93.3%, respectively. These differences confirm that overall classification accuracy should not be considered the sole criterion for evaluating an intelligent intrusion detection system. In OT networks, particular attention should be paid to class-specific

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

performance, including the recognition of less represented and behaviorally similar attack categories.

The comparative analysis further demonstrated that, under the investigated experimental conditions, tree-based ensemble methods outperformed SVM and the evaluated MLP configuration. Nevertheless, these findings should not be interpreted as evidence of the universal superiority of a particular algorithm for every industrial infrastructure. Real-world OT networks differ in equipment composition, industrial communication protocols, network architecture, traffic intensity, and the characteristics of underlying technological processes. Therefore, practical deployment requires validation of the selected model using traffic from the target infrastructure, followed by continuous monitoring for changes in feature distributions.

Thus, the objective of the study was achieved: machine learning methods were compared under a unified experimental framework, and their specific characteristics for detecting and classifying network anomalies in OT/IIoT environments were identified. The obtained results indicate that XGBoost represents a promising foundation for the classification component of an intelligent intrusion detection system when high detection capability and a low false-positive rate are required.

Future research should focus on integrating network traffic characteristics with industrial equipment telemetry and physical process variables, as well as evaluating model robustness against previously unseen attacks. Further investigation of adaptive detection mechanisms capable of responding to changes in normal network behavior over time is also warranted. Another important direction is the development of interpretable classification mechanisms that can provide cybersecurity specialists with transparent explanations of model decisions.

REFERENCES

Ahmed A.A., Abdullah T.A.A. (2026). An Enhanced XGBoost-Based Framework for Efficient Multi-Class Cyber Threat Detection in Industrial IoT Networks // Technologies. — Vol. 14. — No. 5. Article 274. DOI: https://doi.org/10.3390/technologies14050274 (in Eng.).

Al-Hawawreh M., Sitnikova E., Aboutorab N. (2022). X-IIoTID: A Connectivity-Agnostic and Device-Agnostic Intrusion Data Set for Industrial Internet of Things // IEEE Internet of Things Journal. — Vol. 9. — No. 5. Pp. 3962–3977. DOI: https://doi.org/10.1109/JIOT.2021.3102056 (in Eng.).

Altunay H.C., Albayrak Z. (2023). A Hybrid CNN+LSTM-Based Intrusion Detection System for Industrial IoT Networks // Engineering Science and Technology, an International Journal. — Vol. 38. — Article 101322. DOI: https://doi.org/10.1016/j.jestch.2022.101322 (in Eng.).

Aslam M.M., Tufail A., Irshad M.N. (2025). Survey of Deep Learning Approaches for Securing Industrial Control Systems: A Comparative Analysis // Cyber Security and Applications. — Vol. 3. — Article 100096. DOI: https://doi.org/10.1016/j.csa.2025.100096 (in Eng.).

Awotunde J.B., Chakraborty C., Adeniyi A.E. (2021). Intrusion Detection in Industrial Internet of Things Network-Based on Deep Learning Model with Rule-Based Feature Selection // Wireless Communications and Mobile Computing. — Vol. 2021. — Article 7154587. — Pp. 17. DOI: https://doi.org/10.1155/2021/7154587 (in Eng.).

Breiman L. (2001). Random Forests // Machine Learning. — Vol. 45. — No. 1. — Pp. 5–32. DOI: https://doi.org/10.1023/A:1010933404324 (in Eng.).

Buczak A.L., Guven E. (2016). A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection // IEEE Communications Surveys & Tutorials. — Vol. 18. — No. 2. — Pp. 1153–1176. DOI: https://doi.org/10.1109/COMST.2015.2494502 (in Eng.).

Chen T., Guestrin C. (2016). XGBoost: A Scalable Tree Boosting System // Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD '16). — New York:

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

Association for Computing Machinery. Pp. 785–794. DOI: https://doi.org/10.1145/2939672.2939785 (in Eng.).

Cortes C., Vapnik V. (1995). Support-Vector Networks // Machine Learning. — Vol. 20. — Pp. 273–297. DOI: https://doi.org/10.1007/BF00994018 (in Eng.).

Ferrag M.A., Friha O., Hamouda D., Maglaras L., Janicke H. (2022). Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications for Centralized and Federated Learning // IEEE Access. — Vol. 10. — Pp. 40281–40306. DOI: https://doi.org/10.1109/ACCESS.2022.3165809 (in Eng.).

Ferrag M.A., Maglaras L., Moschoyiannis S., Janicke H. (2020). Deep Learning for Cyber Security Intrusion Detection: Approaches, Datasets, and Comparative Study // Journal of Information Security and Applications. — Vol. 50. — Article 102419. DOI: https://doi.org/10.1016/j.jisa.2019.102419 (in Eng.).

Ismail S., Dandan S., Qushou A. (2025). Intrusion Detection in IoT and IIoT: Comparing Lightweight Machine Learning Techniques Using TON_IoT, WUSTL-IIOT-2021, and EdgeIIoTset Datasets // IEEE Access. — Vol. 13. — Pp. 73468–73485. DOI: https://doi.org/10.1109/ACCESS.2025.3554083 (in Eng.).

Koay A.M.Y., Ko R.K.L., Hettema H., Radke K. (2023). Machine Learning in Industrial Control System (ICS) Security: Current Landscape, Opportunities and Challenges // Journal of Intelligent Information Systems. — Vol. 60. — No. 2. — Pp. 377–405. DOI: https://doi.org/10.1007/s10844-022-00753-1 (in Eng.).

Le T.-T.-H., Oktian Y.E., Kim H. (2022). XGBoost for Imbalanced Multiclass Classification-Based Industrial Internet of Things Intrusion Detection Systems // Sustainability. — Vol. 14. — No. 14. Article 8707. DOI: https://doi.org/10.3390/su14148707 (in Eng.).

Moustafa N. (2021). A New Distributed Architecture for Evaluating AI-Based Security Systems at the Edge: Network TON_IoT Datasets // Sustainable Cities and Society. — Vol. 72. — Article 102994. DOI: https://doi.org/10.1016/j.scs.2021.102994 (in Eng.).

Pinto A., Herrera L.-C., Donoso Y., Gutierrez J.A. (2023). Survey on Intrusion Detection Systems Based on Machine Learning Techniques for the Protection of Critical Infrastructure // Sensors. — Vol. 23. — No. 5. Article 2415. DOI: https://doi.org/10.3390/s23052415 (in Eng.).

Sezgin A., Boyacı A. (2023). AID4I: An Intrusion Detection Framework for Industrial Internet of Things Using Automated Machine Learning // Computers, Materials & Continua. — Vol. 76. — No. 2. — Pp. 2121–2143. DOI: https://doi.org/10.32604/cmc.2023.040287 (in Eng.).

Yu J., Shvetsov A.V., Alsamhi S.H. (2024). Leveraging Machine Learning for Cybersecurity Resilience in Industry 4.0: Challenges and Future Directions // IEEE Access. — Vol. 12. — Pp. 159579–159596. DOI: https://doi.org/10.1109/ACCESS.2024.3482987 (in Eng.).

Zhang J., Luo C., Carpenter M., Min G. (2023). Federated Learning for Distributed IIoT Intrusion Detection Using Transfer Approaches // IEEE Transactions on Industrial Informatics. — Vol. 19. — No. 7. — Pp. 8159–8169. DOI: https://doi.org/10.1109/TII.2022.3216575 (in Eng.).

Zolanvari M., Teixeira M.A., Gupta L., Khan K.M., Jain R. (2019). Machine Learning-Based Network Vulnerability Analysis of Industrial Internet of Things // IEEE Internet of Things Journal. — Vol. 6. — No. 4. — Pp. 6822–6834. DOI: https://doi.org/10.1109/JIOT.2019.2912022 (in Eng.).

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES

ХАЛЫҚАРАЛЫҚ АҚПАРАТТЫҚ ЖӘНЕ КОММУНИКАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАР ЖУРНАЛЫ

МЕЖДУНАРОДНЫЙ ЖУРНАЛ ИНФОРМАЦИОННЫХ И КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Собственник:
АО «Международный университет информационных технологий» (Казахстан, Алматы)

Главный редактор:
Колесникова Катерина Викторовна

Ответственный редактор:
Мрзабаева Раушан Жалиевна

Компьютерная верстка:
Калабай Замзагуль Ертугановна

Сайт журнала: https://journal.iitu.edu.kz
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)

Подписано в печать 30.09.2026.
050040 г. Алматы, ул. Манаса 34/1, каб. 709, тел: +7 (727) 244-51-09).

Издание АО "Международного университета информационных технологий"