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. 369–391
Journal homepage: https://journal.iitu.edu.kz
https://doi.org/10.54309/IJICT.2026.27.3.020
УДК 004.056.5

RESEARCH ON THE ROBUSTNESS OF ENSEMBLE MACHINE LEARNING MODELS TO ADVERSARIAL ATTACKS IN INTRUSION DETECTION SYSTEMS FOR IOT NETWORKS

N.E. Karabayev[1], S.K. Serikbayeva[1]*, E. Benkhelif[1,2], B. Tassuov[3]
[1]L.N. Gumilyov Eurasian National University, Astana, Kazakhstan;
[2]Staffordshire University, Staffordshire, United Kingdom;
[3]Taraz University named after M.Kh.Dulaty, Taraz, Kazakhstan.
E-mail:inf_8585@mail.ru

Nurdaulet Karabayev — Doctoral student at the L.N. Gumilyov Eurasian National University, Astana, Kazakhstan
https://orcid.org/0009-0008-6532-6382;
Sandugash Serikbayeva — PhD, Senior Lecturer of the Department of Information Systems, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan
E-mail: inf_8585@mail.ru, https://orcid.org/0000-0002-3627-3321;
Elhadj Benkhelifa — PhD, Professor of Computer Science and Artificial Intelligence, Staffordshire University, Staffordshire, United Kingdom; L.N. Gumilyov Eurasian National University, Astana, Kazakhstan
https://orcid.org/0000-0001-6168-2664;
Bolat Tassuov — Associate Professor, Department of Physics and Informatics, Taraz University named after M.Kh. Dulaty, Taraz, Kazakhstan
https://orcid.org/0000-0002-2000-6720.

© N. Karabayev, S. Serikbayeva, E. Benkhelifa, B. Tassuov

Abstract. This paper investigates the robustness of ensemble machine learning models against adversarial attacks in the context of multiclass intrusion detection in IoT networks. The experimental framework is built upon the ToN-IoT dataset, widely used for evaluating intrusion detection systems. Three ensemble models are employed for multiclass network traffic classification: XGBoost, Random Forest, and LightGBM. Data preprocessing includes removal of irrelevant features, one-hot encoding of categorical attributes, standardization, and train-test splitting. Principal Component Analysis (PCA) is applied to examine the effect of dimensionality reduction on model robustness. To evaluate model robustness, two types of attacks are implemented: Gaussian Noise Attack and FGSM (Fast Gradient Sign Method).

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

Since ensemble models are non-differentiable, adversarial examples for FGSM are generated via a surrogate neural network using a transfer-based approach. Additionally, adversarial training is investigated as a defense strategy, involving augmentation of the training set with adversarial examples followed by model retraining. Classification quality is assessed using Accuracy and F1-score metrics, with analysis of performance degradation under varying noise levels and perturbation magnitudes. Model behavior is interpreted through SHAP analysis. All experiments were repeated with five random seeds and independent stratified splits; results are reported as mean ± standard deviation, and a multilayer perceptron (MLP) is included as a neural-network baseline. The results demonstrate high accuracy across all three models on clean data, with a notable decline in performance under adversarial attacks. Random Forest exhibits the greatest robustness among the evaluated methods. It is established that applying PCA improves model robustness, while adversarial training effectively mitigates the impact of FGSM attacks. The findings confirm the promise of ensemble methods combined with adversarial training for building reliable IDS in IoT environments.

Keywords: intrusion detection, Internet of Things, adversarial attacks, FGSM, ensemble learning, adversarial training, SHAP

For citation: Karabayev N., Serikbayeva S., Benkhelifa E., Tassuov B. (2026). Research on the robustness of ensemble machine learning models to adversarial attacks in intrusion detection systems for iot networks // International journal of information and communication technologies. Vol. 7. No. 27. Pp. 369–391. https://doi.org/10.54309/IJICT.2026.27.3.020. (In Russ.)

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

Financing. *Thiswork is carried out by the staff of the L.N.GumilyovEurasianNationalUniversity with thefinancialsupport of the ScienceCommittee of the Ministry of ScienceandHigherEducation of the Republic of Kazakhstan(Grantno. AP23489127).*

ІОТ-ЖЕЛІЛЕРІНДЕГІ БАСЫП КІРУДІ АНЫҚТАУЖҮЙЕЛЕРІНДЕ МАШИНАЛЫҚ ОҚЫТУДЫҢ АНСАМБЛЬДІ КҮЛГІЛЕРІНІҢ БӘСЕКЕЛЕС ШАБУЫЛДАРҒА ТӨЗІМДІЛІГІН ЗЕРТТЕУ

Н.Е. Қарабаев[1], С.К. Серикбаева[1]*, Е. Бенкхелифа[1,2], Б. Тасуов[3]

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

[2]Стаффордшир университеті, Стаффордшир Ұлыбритания;

[3]М. Х. Дулати атындағы Тараз университеті, Тараз, Қазақстан.

E-mail:inf_8585@mail.ru

Қарабаев Нұрдәулет Ерланұлы — докторант, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан

https://orcid.org/0009-0008-6532-6382;

Серикбаева Сандугаш Курманбековна — PhD, ақпараттық жүйелер кафедрасының аға оқытушысы, Л.Н. Гумилев атындағы Еуразия ұлттық университеті,

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

Астана, Қазақстан
E-mail: inf_8585@mail.ru, https://orcid.org/0000-0002-3627-3321;
Бенхелифа Елхадж — PhD, компьютерлікғылымдаржәнежасанды интеллект профессоры, Стаффордшир университеті, Стаффордшир Ұлыбритания; Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан
https://orcid.org/0000-0001-6168-2664;
Тасуов Болат — физика және информатика кафедрасының қауысдастырылған профессоры, М.Х. Дулати атындағы Тараз университеті, Тараз, Қазақстан
https://orcid.org/0000-0002-2000-6720.

© Н.Е. Қарабаев, С.К. Серикбаева, Е. Бенкхелифа, Б. Тасуов

Аннотация. Бұл жұмыста IoT-желілеріндегі көпкласты шабуылдарды анықтау контекстінде ансамбльдік машиналық оқыту модельдерінің adversarial әсерлерге төзімділігі зерттеледі. Эксперименттік база шабуылдарды анықтау жүйелерін бағалауда кеңінен қолданылатын ToN-IoT деректер жиынтығы негізінде қалыптастырылған. Желілік трафикті көпкласты жіктеу міндетін шешу үшін үш ансамбльдік модель пайдаланылады: XGBoost, Random Forest және LightGBM. Деректерді алдын ала өңдеу кезеңі маңызсыз белгілерді жоюды, категориялық атрибуттарды one-hot encoding әдісімен кодтауды, стандарттауды және деректерді оқыту мен тестілік жиынтықтарға бөлуді қамтиды. Модельдердің тұрақтылығына өлшемділікті азайтудың әсерін талдау мақсатында негізгі компоненттер әдісі (PCA) қолданылады. Модельдердің робастылығын бағалау үшін шабуылдардың екі түрі жүзеге асырылды: Gaussian Noise Attack және FGSM (Fast Gradient Sign Method). Ансамбльдік модельдер дифференциалданбайтын болғандықтан, FGSM үшін adversarial мысалдарды генерациялау transfer-based тәсілін қолданатын суррогаттық нейрондық желі арқылы орындалады. Қосымша ретінде adversarial training әдісі зерттелді, ол оқыту жиынтығын adversarial мысалдармен толықтырып, модельдерді қайта оқытуды қарастырады. Жіктеу сапасы Accuracy және F1-score метрикалары арқылы бағаланып, әртүрлі шу деңгейлері мен perturbation жағдайларындағы көрсеткіштердің төмендеуі талданады. Модельдердің мінез-құлқын интерпретациялау SHAP-талдау көмегімен жүргізіледі. Барлық эксперименттер бес түрлі random seed мәнімен және тәуелсіз стратификацияланған бөлулермен қайталанып, нәтижелер орташа мән ± стандартты ауытқу түрінде берілді; нейрондық желілік базалық модель ретінде көпқабатты перцептрон (MLP) қосылды. Алынған нәтижелер барлық үш модельдің таза деректердегі жоғары дәлдігін көрсете отырып, adversarial шабуылдар әсерінен сапаның едәуір төмендейтінін дәлелдейді. Қарастырылған әдістер арасында ең жоғары тұрақтылықты Random Forest көрсетті. PCA қолдану модельдердің робастылығын арттыратыны, ал adversarial training FGSM-шабуылдарының әсерін тиімді төмендететіні анықталды. Нәтижелер IoT-ортада сенімді IDS жүйелерін құру үшін adversarial training-пен үйлестірілген ансамбльдік әдістердің перспективалы екенін растайды.

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

Түйінді сөздер: шабуылдарды анықтау, заттар интернеті, қарсыластық шабуылдар, FGSM, ансамбльдік оқыту, adversarial training, SHAP

Дәйексөздер үшін: Қарабаев Н.Е., Серикбаева С.К., Бенкхелифа Е., Тасуов Б. (2026). IOT-желілеріндегі басып кіруді анықтау жүйелерінде машиналық оқытудың ансамбльдік үлгілерінің бәсекелес шабуылдарға төзімділігін зерттеу // Халықаралық ақпараттық және коммуникалық технологиялар журналы. Т. 7. No 27. Б. 369–391. https://doi.org/10.54309/IJICT.2026.27.3.020. (Орыс. тіл.).

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

Қаржыландыру. *Бұл жұмыс «Л.Н. Гумилев атындағы Еуразия ұлттық университеті «КЕАҚ қызметкерлерімен Қазақстан Республикасы Ғылым және жоғары білім министрлігі Ғылым комитетінің қаржылық қолдауымен жүргізіледі (Грант№AP23489127).*

ИССЛЕДОВАНИЕ УСТОЙЧИВОСТИ АНСАМБЛЕВЫХ МОДЕЛЕЙ МАШИННОГО ОБУЧЕНИЯ К СОСТЯЗАТЕЛЬНЫМ АТАКАМ В СИСТЕМАХ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ IOT-СЕТЕЙ

Н.Е. Қарабаев[1], С.К. Серикбаева[1]*, Е. Бенкхелифа[1,2], Б. Тасуов[3]

[1]Евразийский национальный университет имени Л.Н. Гумилева, Астана, Казахстан;

[2]Стаффордшир университет, Стаффордшир, Великобритания;

[3]Таразский университет им.М. Х. Дулати, Тараз, Казахстан.

E-mail:inf_8585@mail.ru

Қарабаев Нұрдәулет Ерланұлы — докторант, Евразийского национального университета имени Л.Н. Гумилева, Астана, Казахстан
https://orcid.org/0009-0008-6532-6382;

Серикбаева Сандугаш Курманбековна — PhD, старший преподаватель кафедры информационных систем, Евразийского национального университета имени Л.Н. Гумилева, Астана, Казахстан
E-mail: inf_8585@mail.ru, https://orcid.org/0000-0002-3627-3321;

Елхадж Бенхелифа — PhD, профессор компьютерных наук и искусственного интеллекта, Стаффордширский университет, Стаффордшир, Великобритания; Евразийский национальный университет имени Л.Н. Гумилева, Астана, Казахстан
https://0000-0001-6168-2664;

Тасуов Болат — ассоцированный профессор кафедры Физика и информатика Таразский университет имени М.Х. Дулати, Тараз, Казахстан
https://orcid.org/0000-0002-2000-6720.

© Н.Е. Қарабаев, С.К. Серикбаева, Е. Бенкхелифа, Б. Тасуов

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

Аннотация. В данной работе исследуется устойчивость ансамблевых моделей машинного обучения к состязательным (adversarial) воздействиям в контексте мультиклассового обнаружения вторжений в IoT-сетях. Экспериментальная база формируется на основе набора данных ToN-IoT, широко применяемого для оценки систем обнаружения вторжений.Для решения задачи мультиклассовой классификации сетевого трафика используются три ансамблевые модели: XGBoost, Random Forest и LightGBM. Предобработка данных включает удаление нерелевантных признаков, one-hot encoding категориальных атрибутов, стандартизацию и разбиение на обучающую и тестовую выборки. С целью анализа влияния снижения размерности на устойчивость моделей применяется метод главных компонент (PCA). Для оценки робастности моделей реализованы два вида атак: Gaussian Noise Attack и FGSM (Fast Gradient Sign Method). Поскольку ансамблевые модели являются недифференцируемыми, генерация состязательных примеров для FGSM осуществляется посредством суррогатной нейронной сети с использованием transfer-based подхода. Дополнительно исследуется метод adversarial training, предполагающий дополнение обучающей выборки состязательными примерами и последующее дообучение моделей.Качество классификации оценивается по метрикам Accuracy и F1-score с анализом деградации показателей при различных уровнях шума и величинах возмущений. Поведение моделей интерпретируется с помощью SHAP-анализа. Все эксперименты повторены для пяти значений random seed с независимыми стратифицированными разбиениями, результаты представлены как среднее ± стандартное отклонение; в качестве нейросетевого базового уровня добавлен многослойный перцептрон (MLP).Полученные результаты свидетельствуют о высокой точности всех трёх моделей на чистых данных при заметном снижении качества под воздействием атак. Random Forest демонстрирует наибольшую устойчивость среди рассмотренных методов. Установлено, что применение PCA повышает робастность моделей, а adversarial training эффективно снижает влияние FGSM-атак. Результаты подтверждают перспективность ансамблевых методов в сочетании с adversarial training для построения надёжных IDS в IoT-окружениях.

Ключевые слова: обнаружение вторжений, Интернет вещей, состязательные атаки, FGSM, ансамблевое обучение, adversarial training, SHAP

Для цитирования: Карабаев Н.Е., Серикбаева С.К., Бенкхелифа Е., Тасуов Б. (2026). Исследование устойчивости ансамблевых моделей машинного обучения к состязательным атакам в системах обнарения вторжений IOT-сетей // Международный журналинформационных и коммуникационных технологий. Т. 7. No. 27. Стр. 369–391. https://doi.org/10.54309/IJICT.2026.27.3.020. (На русс.).

Конфликт интересов: авторы заявляют об отсутствии конфликтаинтересов.

Финансирование. *Настоящая работа сотрудниками НАО «Евразийский национальный университет имени Л.Н. Гумилева» проводится при финансовой поддержке Комитета науки Министерства науки и высшего образования Республики Казахстан (Грант № AP23489127).*

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

Введение.

Развитие экосистем Интернета вещей (IoT) и промышленного Интернета вещей (IIoT) сопровождается стремительным увеличением числа подключённых устройств, образующих распределённую сетевую инфраструктуру, ориентированную на непрерывный обмен данными. По прогнозам аналитиков, к 2028 году ожидается подключение более 35 миллиардов IoT-устройств (Diro et al., 2018). Подобная масштабируемость в сочетании с ограниченными вычислительными ресурсами узлов, гетерогенностью протоколов и высокой динамикой трафика создаёт значительную уязвимость перед киберугрозами, включая DoS/DDoS, сканирование, инъекции и атаки типа «человек посередине» (MoustafaN et al., 2021).

Системы обнаружения вторжений (IDS), функционирующие на основе методов машинного обучения, получили широкое распространение в задачах защиты IoT-инфраструктур благодаря способности автоматически выявлять аномалии без явного программирования сигнатурных правил. Тем не менее широко задокументирован феномен состязательных атак — целенаправленных малых возмущений входных данных, способных нарушить корректность предсказаний даже высокоточных классификаторов (Goodfellow et al., 2015). Данное обстоятельство ставит под сомнение практическую надёжность ML-based IDS в реальных условиях эксплуатации.

Исследования в области adversarial machine learning применительно к задачам сетевой безопасности носят преимущественно точечный характер и концентрируются либо на нейросетевых архитектурах, либо на бинарных постановках задачи. Вопрос устойчивости ансамблевых древовидных алгоритмов в условиях мультиклассовой классификации сетевых атак остаётся недостаточно изученным. Ряд работ указывает, что ансамблевые методы могут проявлять бóльшую устойчивость к шуму по сравнению с нейронными сетями, однако систематическое сравнение в transfer-based attack сценарии практически отсутствует.

Целью настоящей работы является сравнительная оценка устойчивости ансамблевых моделей XGBoost, Random Forest и LightGBM к состязательным атакам при мультиклассовом обнаружении вторжений в IoT-сетях на наборе данных ToN-IoT. Последовательно решаются задачи предобработки данных, обучения базовых и PCA-моделей, оценки устойчивости к гауссовскому шуму и FGSM-атаке, реализации adversarial training, а также SHAP-интерпретации результатов, а также сопоставления с нейросетевой базовой моделью (MLP) при многократном повторении экспериментов.

Обзор работы

Задача обнаружения вторжений в IoT-сетях средствами машинного обучения активно исследуется с конца 2010-х годов. (Diro A., 2018) предложили распределённые нейронные сети для обнаружения атак в IoT-средах, продемонстрировав превосходство подходов глубокого обучения над традиционными сигнатурными методами. Тем не менее авторы не рассматривали устойчивость предложенных моделей к состязательным воздействиям, что существенно огра-

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

ничивает применимость их результатов в реальных условиях.

Набор данных ToN-IoT был разработан (Moustafa et al., 2021) в рамках проекта UNSW для оценки AI-based cybersecurity applications. Автор описывает многоуровневую архитектуру сбора трафика, охватывающую телеметрию IoT/IIoT-сервисов, журналы операционных систем и сетевые потоки, и указывает на пригодность датасета для мультиклассовой классификации атак.

Фундаментальный вклад в понимание состязательных атак внесла работа (Goodfellow et al., 2015), предложивших метод FGSM как минимальное по норме возмущение, максимально увеличивающее ошибку классификатора. Применение FGSM к нейросетевым IDS детально исследовалось в работе (Yang et al., 2018), выявившей значительную деградацию качества классификации даже при малых значениях ε.

Устойчивость древовидных ансамблей изучалась (Chen et al., 2019), показавшими, что ансамблевые методы не обеспечивают автоматической защиты от adversarial возмущений, однако проявляют бóльшую устойчивость к переносным атакам по сравнению с нейронными сетями. Transfer-based атаки анализировались (Papernot et al., 2017), продемонстрировавшими значительную переносимость состязательных возмущений между разнородными архитектурами.

Влияние снижения размерности на adversarial robustness изучалось (Bhagoji et al., 2018) PCA может снижать эффективность L2-ограниченных атак, однако не является надёжной защитой. Adversarial training системно обоснован (Madry et al., 2018) как минимаксная задача обучения, повышающая устойчивость при умеренном снижении точности на чистых данных. Метод SHAP предложен (Lundberg et al., 2017) для объяснения предсказаний на основе теории Шепли.

Сравнительный анализ XGBoost, Random Forest и LightGBM в задачах обнаружения вторжений показал сопоставимые результаты на бинарной классификации, однако при дисбалансе классов XGBoost несколько превосходит конкурентов по F1-score (Trabajo et al., 2020; Hall et al., 2022) выявили, что Random Forest в среднем устойчивее к случайному шуму по сравнению с XGBoost. При мультиклассовой постановке рекомендуется использование взвешенного F1-score как более информативной метрики (Yen et al., 2021).

Авторы (Sharafaldin et al., 2019) применяли adversarial training для повышения устойчивости классификаторов на датасете CIC-IDS-2017 и выявили trade-off между robustness и точностью на чистых данных, аналогичный наблюдаемому в настоящем исследовании. (Chen et al., 2016) формализовалиалгоритм XGBoost, (Breiman, 2001) Random Forest, (Ke et al., 2017) LightGBM. (Mirsky et al., 2018) показали применимость ансамблей автоэнкодеров для онлайн-обнаружения вторжений в IoT-сетях.

Авторы (Abdelmoumin et al., 2022) провели масштабное сравнение ML-моделей для аномального обнаружения в IoT и подтвердили высокую эффективность ансамблевых подходов. (Wressnegger et al., 2013) акцентировали различие между постановками аномального обнаружения и классификации. (Zhang et al., 2019) предложили иерархическую архитектуру для инспекции сетевого трафика.

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

EU AI Act (European Parliament, 2024) устанавливает нормативные требования к объяснимости систем ИИ в критически важных приложениях, что подчёркивает значимость SHAP-анализа.

Анализ рассмотренных исследований показывает, что несмотря на высокую точность ансамблевых моделей на чистых данных, их устойчивость к adversarial воздействиям в условиях IoT/IIoT-сетей остаётся недостаточно изученной. Существующие работы преимущественно рассматривают adversarial атаки применительно к нейронным сетям, тогда как комплексная оценка robustness tree-based ансамблей в мультиклассовой постановке представлена фрагментарно. Применение surrogate neural network для transfer-based FGSM-атаки на недифференцируемые модели является реалистичным и практически значимым сценарием. Вопрос сравнительной устойчивости bagging и boosting подходов, влияния PCA на adversarial robustness и эффективности adversarial training в контексте мультиклассового обнаружения вторжений на наборе данных ToN-IoT остаётся открытым, что и составляет основной вклад настоящей работы.

Материалы и методы.

В качестве экспериментальной базы использована сетевая часть набора данных ToN-IoT, разработанного для оценки AI-систем кибербезопасности в средах IoT/IIoT. От многих классических датасетов для обнаружения вторжений ToN-IoT отличается тем, что отражает сценарии Industry 4.0: данные формировались в распределённой инфраструктуре, где сенсоры, контроллеры, шлюзы и облачные сервисы обменивались трафиком в режиме, близком к реальной эксплуатации.

Из всего состава датасета рассматривалась только его сетевая компонента. Каждая запись соответствует отдельному соединению и характеризуется набором атрибутов: адресными и портовыми параметрами, протокольными полями (proto, service, conn_state), количественными характеристиками трафика (duration, src_bytes, dst_bytes, src_pkts, dst_pkts и др.), а также полями DNS, SSL и HTTP. В наборе присутствуют два столбца разметки: label — бинарная метка (normal / attack) и type — многоклассовая метка, различающая нормальный трафик и девять категорий атак: backdoor, DDoS, DoS, injection, MITM, password, ransomware, scanning, XSS. В данной работе целевой переменной служит type, что соответствует задаче мультиклассовой классификации.

Датасет содержит как числовые, так и категориальные признаки, а распределение классов неравномерно: некоторые типы атак встречаются значительно реже нормального трафика. Это потребовало использования не только метрики Accuracy, но и weighted F1-score для корректной оценки качества классификации.

Перед обучением моделей данные прошли несколько последовательных этапов обработки. В первую очередь был исключён столбец label во избежание утечки информации, поскольку он напрямую связан с целевой переменной type. Из признакового пространства удалены IP-адреса src_ip и dst_ip: их включение могло бы привести к запоминанию конкретных адресов, ассоциированных с атаками, вместо обобщения на уровне поведенческих характеристик трафика. До-

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

полнительно были исключены высококардинальные текстовые поля dns_query, ssl_subject, ssl_issuer, http_uri и http_user_agent, способные вызвать чрезмерный рост размерности после кодирования и риск переобучения.

Записи с пропущенными значениями удалялись методом listwisedeletion. Категориальные признаки (proto, service, conn_state, http_method, ssl_version и др.) преобразованы с помощью one-hotencoding; целевая переменная type — посредством LabelEncoder. Числовые признаки стандартизированы с использованием StandardScaler (нулевое среднее, единичное стандартное отклонение). Стандартизация необходима по трём причинам: она обеспечивает корректную работу PCA, стабилизирует обучение surrogate-сети и позволяет применять GaussianNoise и FGSM-возмущения в сопоставимых масштабах по всем признакам. Данные разделены на обучающую и тестовую выборки в соотношении 70/30 со стратификацией по целевой переменной.

В исследовании применялись три ансамблевые модели: XGBoost, RandomForest и LightGBM. Их выбор обусловлен доказанной эффективностью на табличных данных, способностью учитывать нелинейные зависимости и широким использованием в задачах обнаружения вторжений.

XGBoost и LightGBM относятся к семейству методов градиентного бустинга: каждое следующее дерево исправляет ошибки предыдущих, последовательно снижая остаточную ошибку ансамбля. RandomForest строится иначе: деревья обучаются независимо на случайных подвыборках данных и признаков, а итоговое решение формируется голосованием. Именно это различие между boosting и bagging важно для анализа устойчивости: голосование в RandomForest потенциально сглаживает влияние отдельных возмущений, тогда как boosting-модели формируют более сложные и, возможно, более чувствительные границы решений. Все три модели использовались с параметрами по умолчанию; настройка гиперпараметров не входила в задачи работы, что позволило сосредоточиться на сравнении robustness, а не на достижении максимальной точности.

Для сопоставления с нейросетевыми подходами, рассмотренными в обзоре литературы, в эксперимент включена базовая нейросетевая модель — многослойный перцептрон (MLP). Чтобы FGSM-атака на MLP оставалась transfer-based и была сопоставима с атакой на ансамблевые модели, MLP обучалась независимо от surrogate-сети: с другой архитектурой и другой инициализацией весов (параметры приведены в подразделе «Воспроизводимость экспериментов»). Атака непосредственно на surrogate-сеть соответствовала бы white-box сценарию и не была бы корректной точкой сравнения.

Общая архитектура исследования представлена на рисунке 1. Пайплайн включает шесть этапов: предобработку данных ToN-IoT, построение ансамблевых моделей, оценку на различных типах данных (чистые, зашумлённые, состязательные, PCA), adversarialtraining, финальное сравнение и выводы.

На первом этапе модели обучались на чистых стандартизированных данных и оценивались на тестовой выборке — это baseline, относительно которого измерялась деградация при последующих воздействиях.

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

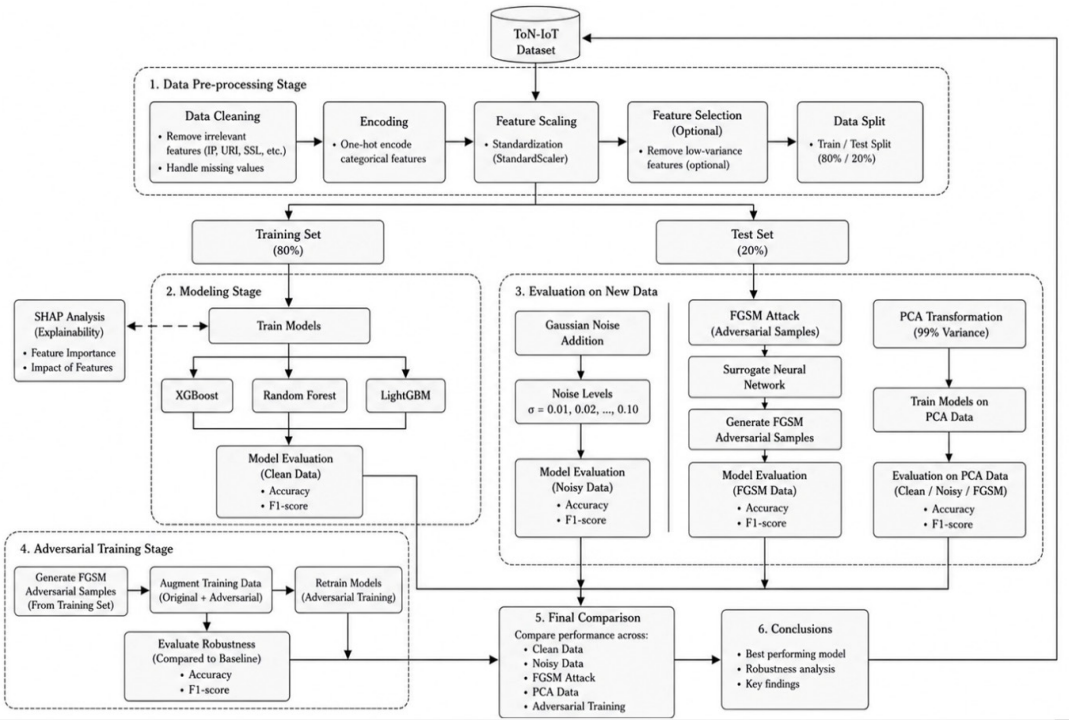


Рис. 1. Общая схема экспериментального pipeline исследования adversarial robustness ансамблевых IDS-моделей на наборе данных ToN-IoT

На втором этапе оценивалась устойчивость к Gaussian Noise Attack. К тестовым данным добавлялся гауссов шум $N(0, \sigma)$ с уровнями $\sigma \in \{0.01, 0.03, 0.05, 0.10\}$, что позволило проследить характер снижения качества в зависимости от интенсивности случайных искажений.

Выбор диапазона значений σ и ε обусловлен следующим. Поскольку признаки стандартизованы, σ и ε выражены в долях стандартного отклонения признака: значение 0.01 соответствует возмущению порядка 1 % естественного разброса признака, 0.10–10 %. Это область «малых» возмущений, в которой изменённое соединение остаётся статистически правдоподобным; по порядку величины она сопоставима с ограничениями L∞-атак, принятыми в базовых работах по состязательному обучению (например, ε = 8/255 ≈ 0.031 у (Madry et al., 2018)). Верхняя граница 0.10 выбрана по результатам предварительных прогонов: уже при этом значении точность базовых ансамблевых моделей снижается до 0.2–0.4 (рис. 6, табл. 1), и дальнейшее увеличение σ и ε не даёт дополнительной информации о сравнительной устойчивости моделей. Сетка {0.01, 0.03, 0.05, 0.10} близка к логарифмической и позволяет подробнее описать начальный участок кривой деградации.

Третийэтапбылпосвящён FGSM (Fast Gradient Sign Method). Поскольку XGBoost, Random Forest и LightGBM недифференцируемы, adversarial-примерыгенерировалисьчерез surrogate neural network — полносвязнуюсетьс ReLU-акти-

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

вациями Dropout, обученнуюнатехжеданныхвтечение 20 эпох. Сгенерированные примеры затем применялись к основным моделям в transfer-based сценарии при $\varepsilon \in \{0.01, 0.03, 0.05, 0.10\}$. Такой подход моделирует реалистичную black-box ситуацию, когда атакующий не имеет доступа к внутренней структуре целевой IDS-модели.

Четвёртый этап — PCA-эксперимент. Метод главных компонент применялся с сохранением 99% объяснённой дисперсии: после преобразования обучались отдельные версии всех трёх моделей и тестировались в тех же условиях (clean / Gaussian / FGSM). PCA здесь выступает не как средство защиты, а как метод снижения размерности, влияние которого на robustness проверялось эмпирически. Для FGSM adversarial-примеры сначала строились в исходном стандартизированном пространстве, затем преобразовывались ранее обученным PCA-преобразованием.

На пятом этапе выполнялся adversarialtraining. Обучающая выборка дополнялась FGSM-примерами, сгенерированными при $\varepsilon = 0.03$; получившийся расширенный набор использовался для переобучения каждой модели. Модели с adversarialtraining тестировались на clean, noisy и FGSM-данных, что позволило зафиксировать возможный trade-off между robustness и точностью на чистых данных.

На шестом, заключительном этапе проводился SHAP-анализ (SHapley Additive exPlanations) на части тестовой выборки для всех трёх моделей. Summary bar plots позволили определить признаки с наибольшим вкладом в предсказания и сопоставить логику принятия решений у XGBoost, Random Forest и LightGBM. В контексте adversarial robustness высокая SHAP-значимость конкретного признака означает, что его изменение при атаке способно существенно повлиять на выход модели.

Поскольку summary bar plots показывают лишь среднюю абсолютную величину SHAP-значений, анализ дополнен beeswarm-диаграммами для ключевых классов, которые отражают направление влияния признаков: положительное SHAP-значение повышает, а отрицательное — понижает оценку вероятности соответствующего класса.

Качество классификации оценивалось по двум метрикам: Accuracy (доля верно классифицированных объектов) и weighted F1-score, который усредняет F1-score по всем классам с учётом их представленности. В условиях дисбаланса классов, характерного для IDS-датасетов, F1-score даёт более корректную картину, чем Accuracy, которая может оставаться высокой за счёт доминирующего класса. При анализе устойчивости к adversarial воздействиям рассчитывался также FGSM AccuracyDrop — разность между точностью на чистых и adversarial данных, отражающая степень деградации модели под атакой.

Результаты и обсуждение.

Качество классификации на чистых данных

На первом этапе все три модели были обучены на стандартизированных данных и протестированы на чистой тестовой выборке. Результаты показали, что

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

XGBoost, RandomForest и LightGBM достигают сопоставимо высокой точности: значения Accuracy и weighted F1-score у каждой из моделей превышают 0.988. Это свидетельствует о том, что после проведённой предобработки признаковое пространство содержит достаточно информации для надёжного разграничения нормального трафика и девяти категорий атак без каких-либо дополнительных ухищрений.

Столь высокие показатели объясняются несколькими факторами. Во-первых, сетевая часть ToN-IoT включает признаки, специфичные для конкретных протоколов и типов атак, что само по себе облегчает классификацию. Во-вторых, ансамблевые tree-based алгоритмы хорошо справляются с нелинейными зависимостями в табличных данных. Вместе с тем высокая точность на cleandata ещё не означает устойчивости модели в реальной среде, где входной трафик может содержать шум или подвергаться преднамеренным манипуляциям.

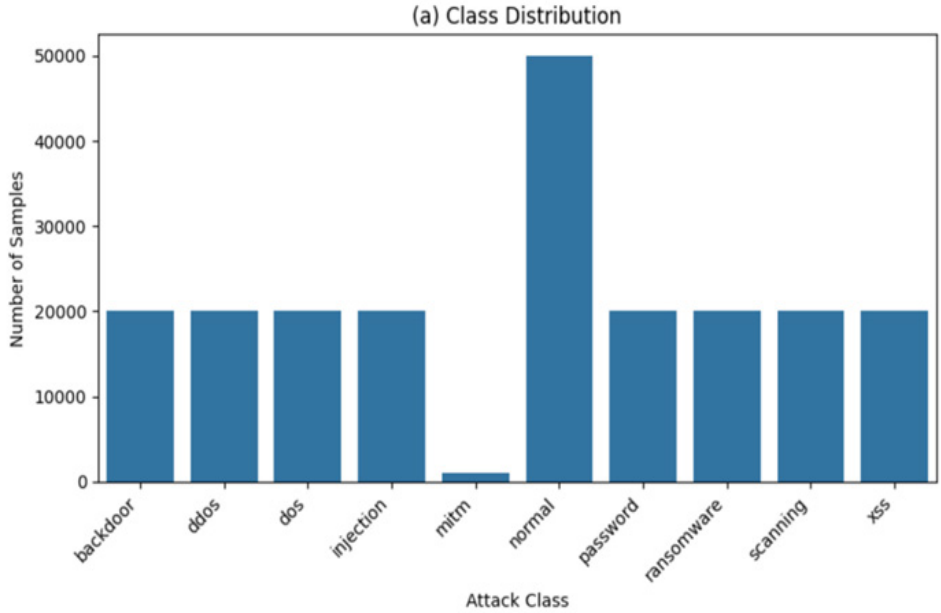


Рис. 2. Распределение классов в сетевой части ToN-IoT

На рис. 2 представлено распределение классов в используемом наборе данных. Хорошо видно, что классы существенно несбалансированы: нормальный трафик и ряд атак (DoS, DDoS, scanning) представлены значительно большим числом записей, тогда как MITM и ransomware встречаются значительно реже. Именно поэтому для оценки качества классификации наряду с Accuracy применялся weighted F1-score, который учитывает представленность каждого класса и штрафует модель за ошибки на редких категориях.

Анализ значимости признаков

Перед обучением моделей была проведена предварительная оценка информативности признаков с использованием MutualInformation. Данный метод позволяет количественно оценить степень статистической зависимости между

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

каждым входным признаком и целевой переменной, причём в отличие от линейной корреляции он чувствителен и к нелинейным связям.

Как следует из рис.3, наибольший вклад в различение классов вносят признаки, характеризующие объём и направленность трафика: src_bytes, dst_bytes, dst_pkts, а также параметры соединения conn_state и service. Это ожидаемо: атаки типа DoS/DDoS и scanning порождают трафик с аномально большим числом пакетов или байтов, тогда как MITM и injection могут проявляться через нестандартные состояния соединения. Признаки с высокими значениями MutualInformation одновременно являются потенциально уязвимыми с adversarial точки зрения: целенаправленное изменение именно этих характеристик способно существенно исказить предсказание модели.

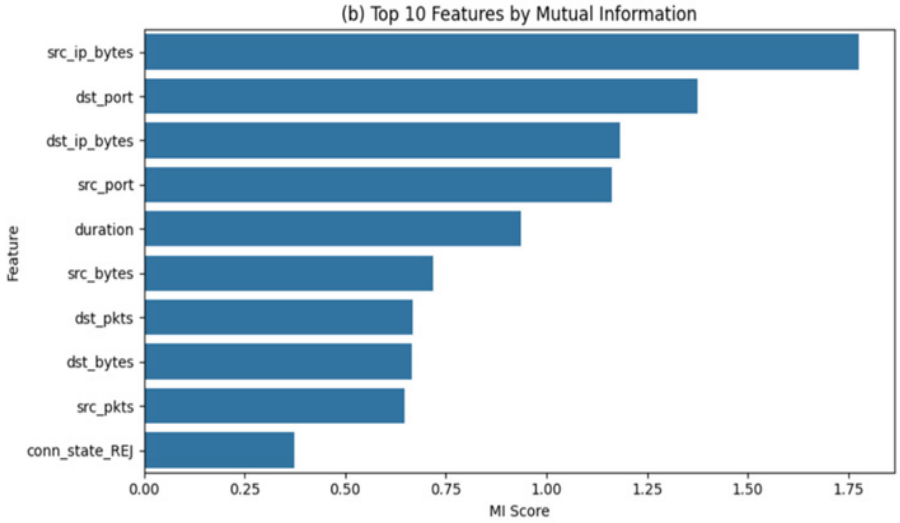


Рис. 3. Топ-10 наиболее информативных признаков по MutualInformation

Визуализация признакового пространства (PCA)

Визуализация подтверждает, что классы в целом разделимы в пространстве главных компонент, хотя ряд категорий атак образует перекрывающиеся области. Именно это перекрытие объясняет, почему модели чувствительны к adversarial perturbations: объект, находящийся вблизи границы между классами, может сменить принадлежность уже при незначительном смещении в признаковом пространстве. Кроме того, высокая плотность точек в центральной зоне указывает на то, что нормальный трафик и некоторые типы атак занимают смежные области, что дополнительно усложняет задачу робастной классификации.

Устойчивость к Gaussian Noise

На следующем этапе к тестовым данным добавлялся гауссов шум с уровнями $\sigma \in \{0.01, 0.03, 0.05, 0.10\}$. Результаты показали ожидаемую деградацию качества классификации по мере увеличения интенсивности шума у всех трёх моделей. Однако степень этой деградации существенно различалась (Рис.6): Random Forest сохранял относительно стабильные показатели при малых значе-

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

ниях σ, тогда как XGBoost и LightGBM демонстрировали более резкое снижение Accuracy и F1-score уже при σ = 0.05.

Для анализа геометрической структуры данных была выполнена проекция признакового пространства на плоскость первых двух главных компонент. На рис. 4 и 5 представлены двумерная и трёхмерная PCA-проекции соответственно.

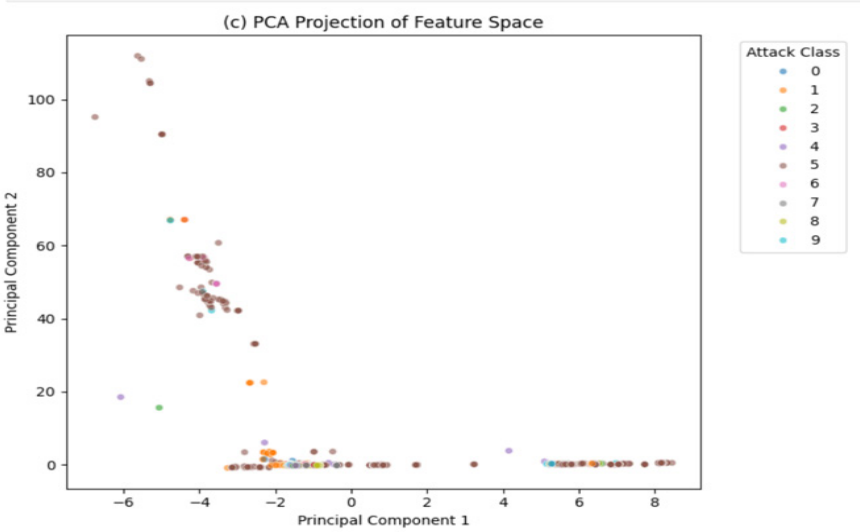


Рис. 4. Двумерная PCA-проекция признакового пространства ToN-IoT

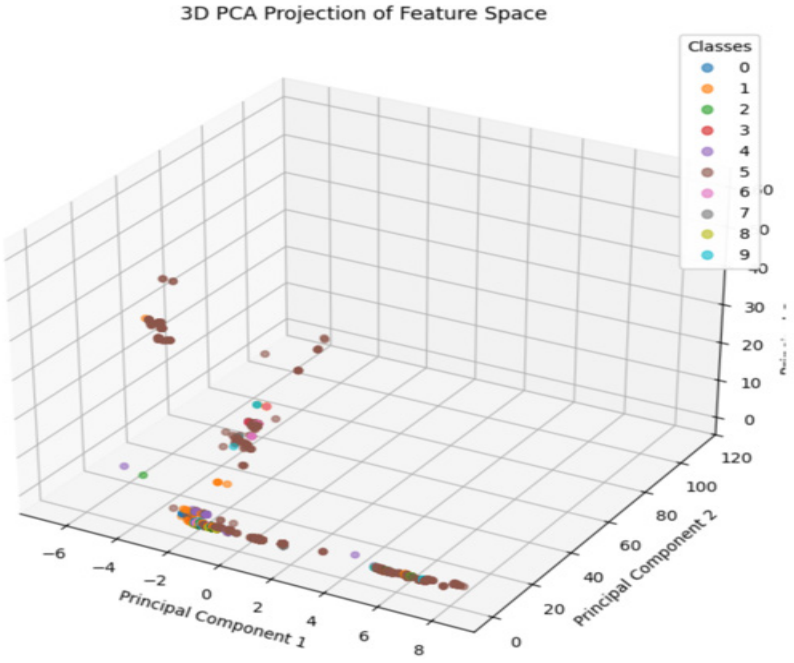


Рис. 5. Трёхмерная PCA-проекция признакового пространства ToN-IoT

Устойчивость Random Forest к случайным возмущениям объясняется его

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

ансамблевой структурой: голосование множества независимых деревьев фактически усредняет отклик, что частично компенсирует случайные искажения отдельных признаков. В boosting-моделях деревья взаимно зависимы — каждое исправляет ошибки предыдущего, — поэтому изменения во входных данных сильнее распространяются по всей цепочке, что делает итоговое предсказание более чувствительным к шуму.

Следует отметить, что заметное снижение точности всех моделей наблюдается уже при σ = 0.01. Вероятной причиной является тяжёлый хвост распределения объёмных признаков (src bytes, dst bytes, duration): их стандартное отклонение определяется редкими очень большими значениями, поэтому после стандартизации типичные малые значения сжаты в узкий интервал, в котором плотно расположены пороги разбиения деревьев. Даже малый в относительных единицах шум переводит такие объекты через пороги. Применение логарифмического преобразования log(1 + x) к объёмным признакам перед стандартизацией могло бы снизить этот эффект; его проверка запланирована в дальнейшей работе.

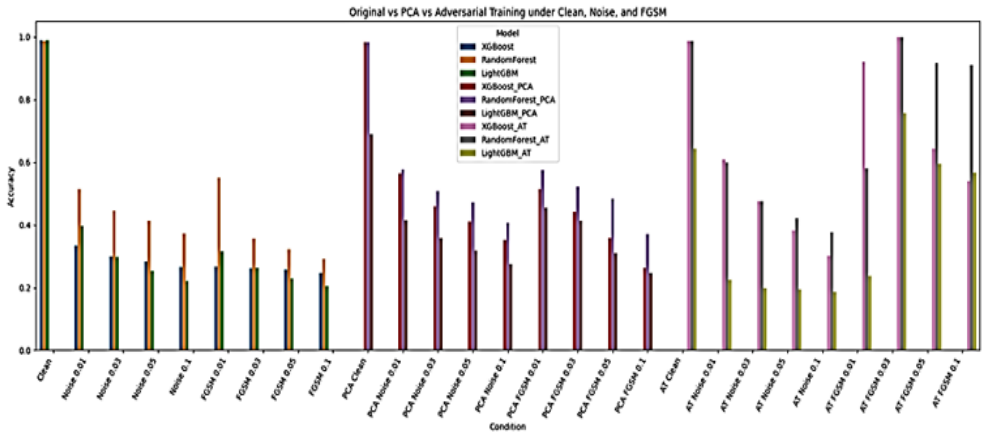


Рис. 6. Accuracy базовых, PCA- и AT-моделей в условиях Clean, Gaussian Noise и FGSM (один запуск, seed = 0)

Устойчивость к FGSM-атаке

Для оценки устойчивости к направленным adversarial возмущениям применялся метод FGSM. Поскольку XGBoost, Random Forest и LightGBM являются недифференцируемыми алгоритмами, adversarial-примеры генерировались через surrogate neural network, обученную на тех же данных, после чего переносились на основные модели (transfer-based сценарий). Значения параметра ε варьировались в диапазоне {0.01, 0.03, 0.05, 0.10}.

Результаты, представленные на рис. 6, свидетельствуют о том, что FGSM-атака оказывает более выраженное влияние на качество классификации по сравнению с аналогичным по интенсивности гауссовым шумом. Это объясняется принципиальным различием двух воздействий: Gaussian Noise изменяет признаки случайно, тогда как FGSM направленно смещает их в сторону, максимально

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

увеличивающую функцию потерь. Тем не менее transfer-based подход снижает эффективность атаки по сравнению с white-box сценарием: adversarial-примеры, созданные на surrogate-сети, не идеально совпадают с теми возмущениями, которые были бы оптимальны для дерева решений. Это подтверждается тем, что при $\varepsilon = 0.01$ деградация у всех трёх моделей оставалась относительно умеренной.

Среди базовых моделей наибольшее падение Accuracy под FGSM-атакой зафиксировано у XGBoost (FGSM Accuracy Drop ≈ 0.731; табл. 3) и LightGBM (≈ 0.735), тогда как у Random Forest этот показатель составил ≈ 0.608. Таким образом, несмотря на то что все три алгоритма обнаружения вторжений уязвимы к направленным adversarial воздействиям, Random Forest проявляет относительно бóльшую устойчивость. Полученные данные согласуются с общей тенденцией: bagging снижает дисперсию предсказаний, что частично смягчает эффект transfer-based атак.

4.6. Влияние снижения размерности (PCA)

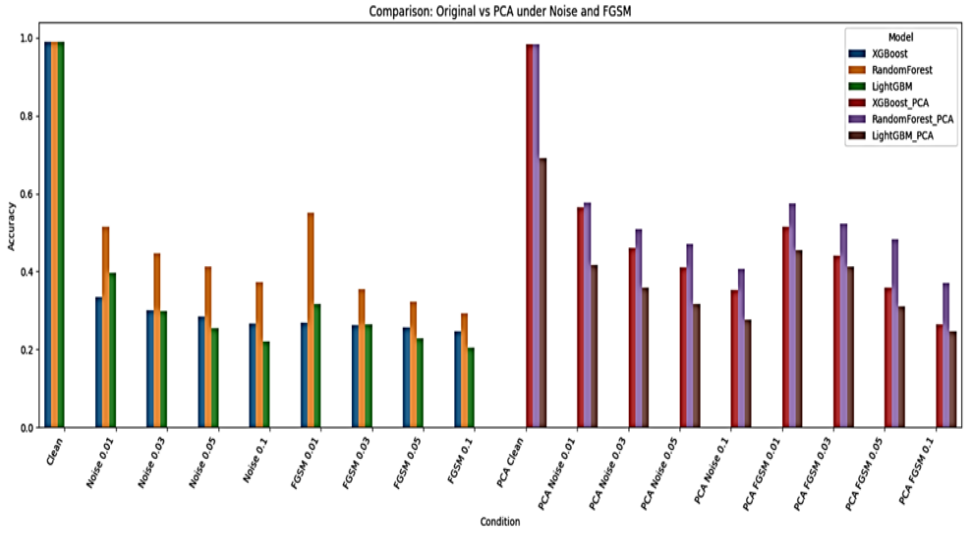


Рис. 7. Accuracy исходных и PCA-моделей в условиях Clean, Gaussian Noise и FGSM (один запуск, seed = 0)

На рис. 7 сопоставлена точность исходных моделей и моделей, обученных после PCA-преобразования. При сохранении 99% дисперсии количество признаков сокращается, что позволяет устранить часть избыточных и коррелированных измерений без существенной потери структуры данных. После PCA-преобразования были обучены отдельные версии XGBoost, Random Forest и LightGBM, которые тестировались в тех же условиях, что и базовые модели.

Качество PCA-моделей на чистых данных незначительно уступало базовому уровню (Accuracy ≈ 0.982–0.983 у XGBoost_PCA и RandomForest_PCA против ≈ 0.988–0.989 у исходных моделей). Вместе с тем при Gaussian Noise PCA-варианты показали сопоставимую или несколько лучшую устойчивость. При FGSM, однако, картина неоднозначна: FGSM Accuracy Drop у RandomForest_PCA соста-

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

вил ≈ 0.495, что в целом хуже, чем у RandomForest_AT, но лучше, чем у базового RandomForest. Это указывает на то, что PCA сам по себе не является надёжным механизмом защиты от направленных adversarial атак, хотя частично снижает влияние случайного шума за счёт проекции в пространство максимальной дисперсии.

Adversarial Training

Наиболее практически значимым результатом работы является оценка adversarial training. После дополнения обучающей выборки FGSM-примерами (ε = 0.03) и переобучения моделей их устойчивость к adversarial атакам существенно возросла. Подробные результаты представлены на рис. 8.

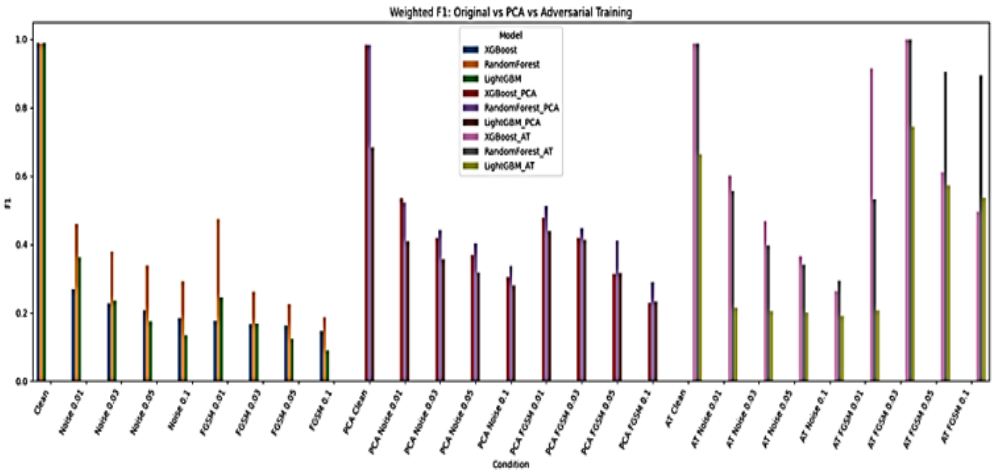


Рис. 8. Weighted F1-score базовых, PCA- и AT-моделей в условиях Clean, Gaussian Noise и FGSM (один запуск, seed = 0)

Из рис. 8 видно, что RandomForest_AT достиг FGSM Accuracy Drop ≈ 0.136 против ≈ 0.608 у исходного Random Forest — снижение более чем в четыре раза. Аналогичная динамика наблюдается у XGBoost_AT (Drop ≈ 0.212 против ≈ 0.731). Таким образом, включение adversarial-примеров в обучающую выборку позволяет модели заблаговременно «познакомиться» с характером возможных возмущений и выработать более устойчивые границы решений.

Вместе с тем необходимо отметить важный аспект: adversarial training у LightGBM_AT привёл к неожиданному снижению качества на чистых данных (Accuracy ≈ 0.643), что указывает на trade-off между robustness и точностью. Данный эффект объясняется тем, что расширенная выборка с adversarial-примерами может содержать примеры, «конфликтующие» с исходными границами решений градиентного бустинга, что затрудняет оптимизацию. Для XGBoost_AT и RandomForest_AT подобной просадки на clean data не наблюдалось (Accuracy ≈ 0.988), что свидетельствует о том, что *adversarial training* хорошо совместим с этими алгоритмами при выбранных параметрах.

Возможные причины просадки LightGBM_AT на чистых данных следующие. Во-первых, LightGBM наращивает деревья по листьям (leaf-wise) и при

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

параметрах по умолчанию (num_leaves = 31, отсутствие L1/L2-регуляризации) склонен подстраиваться под локальные особенности выборки. FGSM-примеры смещены одновременно по всем признакам, включая one-hot-столбцы, которые после возмущения принимают недопустимые дробные значения, и модель может формировать листья под эти артефакты в ущерб исходному распределению. Во-вторых, гистограммная дискретизация признаков (max_bin = 255) в LightGBM строится по расширенной выборке, и возмущённые объекты смещают границы бинов для признаков с тяжёлым хвостом, снижая разрешение в области чистых данных. В-третьих, расширенная выборка содержит «конфликтующие» объекты: возмущённый пример одного класса может попадать в область, занимаемую другим классом. Скорость обучения, по-видимому, не является единственной причиной: XGBoost_AT с более высокой скоростью обучения (0.3) аналогичной просадки не показал.

Для устранения эффекта целесообразно: (1) снизить learning_rate до 0.03–0.05 с пропорциональным увеличением числа деревьев и ранней остановкой по чистой валидационной выборке; (2) ввести регуляризацию (lambda_l1, lambda_l2, min_child_samples ≥ 50, feature_fraction и bagging_fraction ≈ 0.8); (3) применять возмущения только к непрерывным признакам либо проецировать one-hot-столбцы на допустимые значения {0, 1}; (4) уменьшить долю состязательных примеров в обучающей выборке или присвоить им меньший вес (sample_weight). Систематический подбор этих параметров для LightGBM_AT является предметом дальнейшей работы.

Интерпретация моделей (SHAP)

Для понимания того, на основе каких признаков строятся предсказания каждой модели, был проведён SHAP-анализ. На рис. 9–11 представлены summary bar plots для XGBoost, Random Forest и LightGBM соответственно. Высота столбца отражает среднее абсолютное значение SHAP для данного признака, то есть его суммарный вклад в отклонение предсказания от базового уровня.

.Вместе с тем имеются и различия. XGBoost уделяет заметно большее внимание портовым признакам и ряду HTTP-атрибутов, тогда как RandomForest более равномерно распределяет значимость между несколькими группами признаков. LightGBM занимает промежуточное положение. С точки зрения adversarialrobustness концентрация важности на небольшом наборе признаков означает, что модель уязвима: достаточно целенаправленно изменить один-два ключевых атрибута, чтобы вызвать ошибочную классификацию. Напротив, более равномерное распределение SHAP-значимости у RandomForest косвенно объясняет его бóльшую устойчивость к FGSM-атакам.

Сравнение рис. 9–11 позволяет выявить как общие закономерности, так и различия в логике принятия решений. Во всех трёх моделях в числе наиболее значимых оказываются признаки, отражающие объём трафика (src_bytes, dst_bytes) и тип сервиса (service). Это согласуется с результатами анализа MutualInformation (рис. 3) и подтверждает, что поведенческие характеристики сетевого потока несут основную классификационную нагрузку.

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

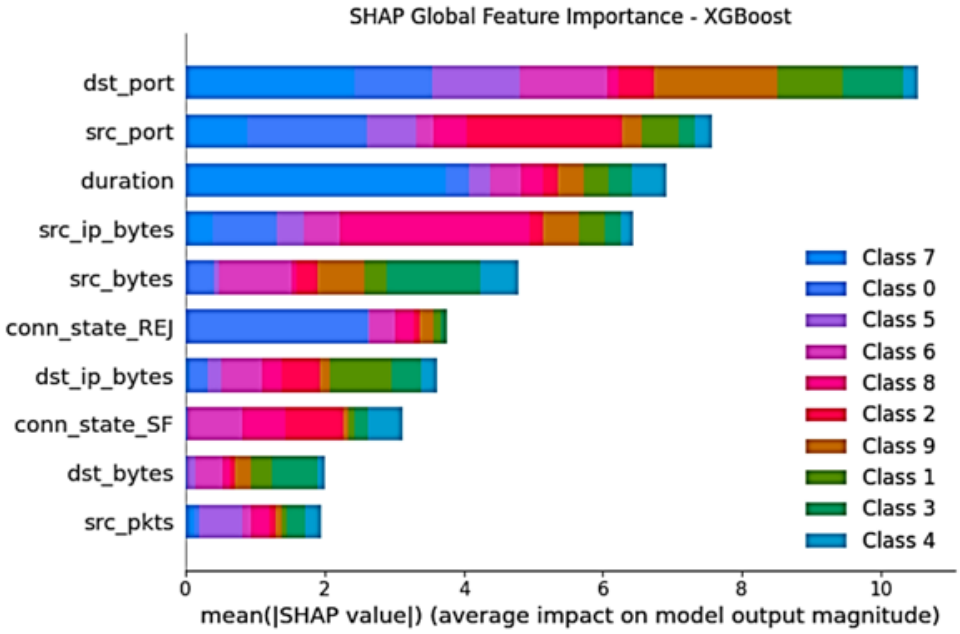


Рис. 9. SHAP summary plot дляXGBoost

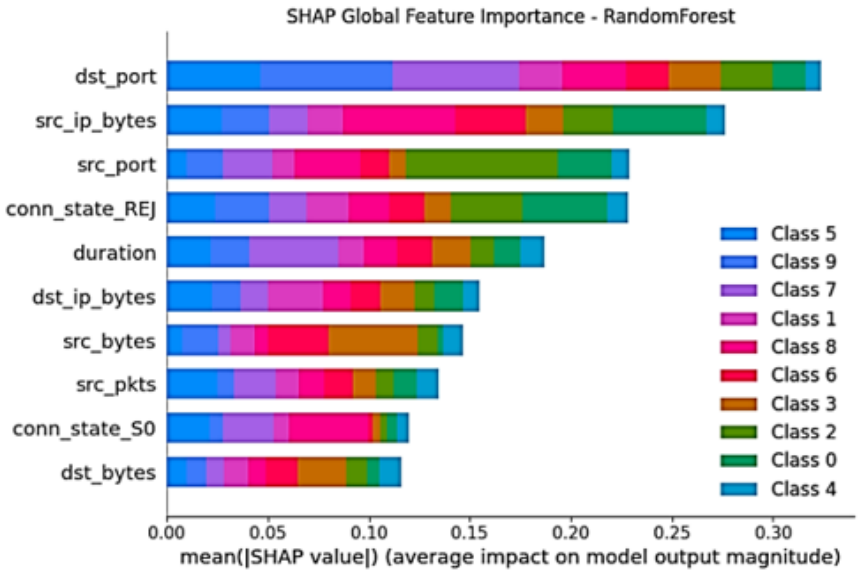


Рис. 10. SHAP summary plot для Random Forest

Сводное сравнение и обсуждение

Совокупность полученных результатов позволяет сделать ряд выводов. Все три ансамблевые модели демонстрируют высокое качество обнаружения вторжений на чистых данных, что подтверждает пригодность XGBoost, RandomForest и LightGBM для задачи мультиклассовой классификации сетевого трафика в IoT/IIoT-средах. Однако их устойчивость к adversarial воздействиям

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

существенно различается, причём bagging-модель (RandomForest) в большинстве сценариев превосходит boosting-альтернативы.

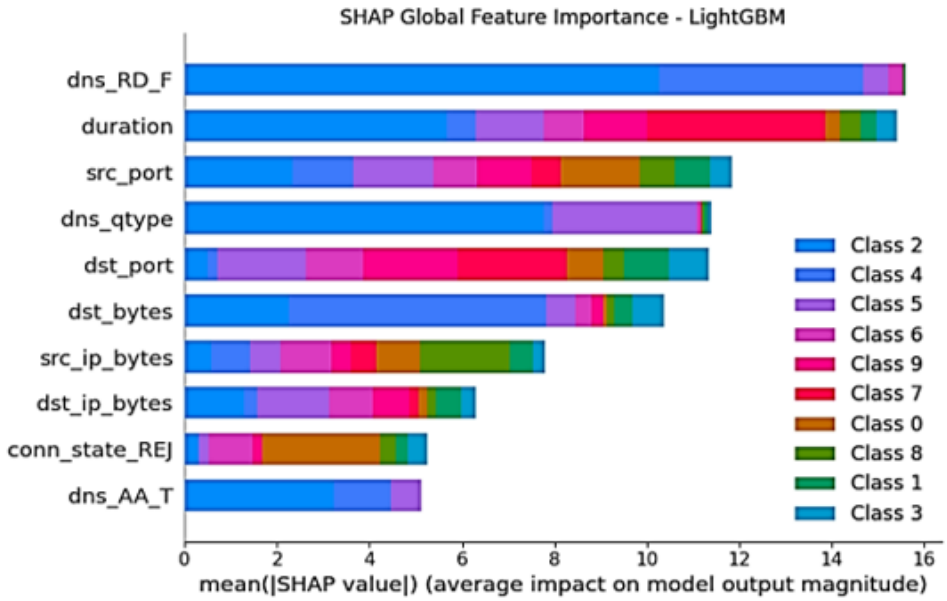


Рис. 11. SHAP summary plot дляLightGBM

GaussianNoise и FGSM оказывают принципиально разный эффект: случайный шум снижает качество постепенно и относительно равномерно, тогда как направленные adversarial возмущения способны резко обрушить точность классификации даже при небольших значениях ε. Это подчёркивает важность явной оценки adversarialrobustness при разработке ML-based систем обнаружения вторжений — стандартного тестирования на чистых данных для этого недостаточно.

Применение PCA снижает размерность и незначительно улучшает устойчивость к случайному шуму, однако не является надёжной защитой от направленных атак. Adversarialtraining, напротив, продемонстрировал выраженный положительный эффект для XGBoost и RandomForest: FGSM AccuracyDrop снизился в 3–4 раза без существенной просадки на чистых данных. Это делает adversarialtraining перспективным компонентом при проектировании устойчивых IDS для IoT/IIoT-сетей.

Ограничением настоящей работы является использование transfer-based подхода для генерации FGSM-примеров, что означает лишь приближённую реализацию атаки на недифференцируемые модели. В реальном сценарии black-box атакующий мог бы использовать более совершенную surrogate-модель или итеративные методы (PGD, C&W), что потенциально привело бы к большей деградации качества.

Заключение.

В ходе проведённого исследования была решена актуальная задача оцен-

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

ки adversarialrobustness ансамблевых моделей машинного обучения XGBoost, RandomForest и LightGBM при мультиклассовом обнаружении вторжений в IoT/IIoT-сетях с использованием сетевой части набора данных ToN-IoT. Рост цифровизации и увеличение числа подключённых устройств существенно повышают требования к кибербезопасности бортовых и промышленных сетей, что делает разработку устойчивых IDS-систем особенно востребованной.

Проведена комплексная предобработка данных, включающая удаление нерелевантных признаков, one-hotencoding, стандартизацию и стратифицированное разбиение. Для задачи мультиклассовой классификации применялись модели XGBoost, RandomForest и LightGBM. Для оценки устойчивости реализованы GaussianNoiseAttack ($\sigma \in \{0.01, 0.03, 0.05, 0.10\}$) и FGSM ($\varepsilon \in \{0.01, 0.03, 0.05, 0.10\}$) через surrogateneuralnetwork в transfer-based сценарии.

Результаты экспериментов подтвердили, что все три базовые модели демонстрируют высокую точность классификации на чистых данных (CleanAccuracy и F1 выше 0.988), однако их качество снижается под воздействием adversarial атак и шумовых искажений. Среди рассмотренных моделей RandomForest продемонстрировал наиболее устойчивое поведение по сравнению с XGBoost и LightGBM: FGSM AccuracyDrop 0.6082 против 0.7306–0.7352 у boosting-моделей.

Эксперименты показали, что применение PCA способствует повышению устойчивости моделей к искажениям входных данных: FGSM Drop снизился до 0.4948 для RandomForest_PCA и 0.5883 для XGBoost_PCA. Adversarialtraining позволяет дополнительно снизить влияние FGSM-атак (TrabajoFernández et al., 2020): RandomForest_AT достиг Average FGSM Accuracy 0.8524 при FGSM AccuracyDrop 0.1362 и минимальном снижении baseline. Таким образом, adversarialtraining является наиболее эффективным методом повышения robustness среди рассмотренных подходов.

SHAP-анализ позволил повысить интерпретируемость результатов и выявить наиболее значимые признаки src_bytes, dst_bytes, src_pkts, dst_pkts, duration, service, conn_state влияющие на решения IDS-моделей. Полученные результаты подтверждают перспективность использования ансамблевых методов и adversarialtraining при разработке устойчивых систем обнаружения вторжений для IoT/IIoT-сетей.

Практическая рекомендация: для построения IDS с требованиями к adversarialrobustness рекомендуется RandomForest с adversarialtraining. Перспективными направлениями дальнейших исследований являются: оценка robustness при более мощных атаках; исследование физически реализуемых adversarialperturbations в реальном трафике; применение certifiedrobustness к ансамблевым IDS; онлайн adversarialtraining с учётом дрейфа данных.

REFERENCES

Abdelmoumin, G., Rawat, D. B., & Rahman, A. (2022). On the performance of machine learning models for anomaly-based intelligent intrusion detection systems for IoT // IEEE Internet of Things Journal. — Vol. 9. — No. 6. — Pp. 4280–4290. DOI: https://doi.org/10.1109/JIOT.2021.3103829. [in Eng.].

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

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

Bhagoji, A. N., Cullina, D., & Mittal, P. (2018). Dimensionality reduction as a defense against evasion attacks on machine learning classifiers // arXiv preprint. DOI: https://doi.org/10.48550/arXiv.1704.02654. [in Eng.].

Chen, T., &Guestrin, C. (2016). XGBoost: A scalable tree boosting system // Proceedings of ACM SIGKDD. — Pp. 785–794. DOI: https://doi.org/10.1145/2939672.2939785. [in Eng.].

Chen, H., Zhang, H., Boning, D., & Hsieh, C.-J. (2019). Robust decision trees against adversarial examples // Proceedings of ICML. — Vol. 97. — Pp. 1122–1131. DOI: https://doi.org/10.48550/arXiv.1902.10660. [in Eng.].

Diro, A., &Chilamkurti, N. (2018). Distributed attack detection scheme using deep learning approach for Internet of Things // Future Generation Computer Systems. — Vol. 82. — Pp. 761–768. DOI: https://doi.org/10.1016/j.future.2017.08.043. [in Eng.].

European Parliament. (2024). Regulation (EU) 2024/1689 — Artificial Intelligence Act // Official Journal of the European Union. DOI: https://doi.org/10.32657/10356/178723. [in Eng.].

Goodfellow, I. J., Shlens, J., &Szegedy, C. (2015). Explaining and harnessing adversarial examples // Proceedings of ICLR. DOI: https://doi.org/10.48550/arXiv.1412.6572. [in Eng.].

Hall, M., Frank, E., Holmes, G., Pfahringer, B., Reutemann, P., & Witten, I. H. (2022). The WEKA data mining software: An update // ACM SIGKDD Explorations Newsletter. — Vol. 11. — No. 1. — Pp. 10–18. DOI: https://doi.org/10.1145/1656274.1656278. [in Eng.].

Ke, G., Meng, Q., Finley, T., Wang, T., Chen, W., Ma, W., Ye, Q., & Liu, T.-Y. (2017). LightGBM: A highly efficient gradient boosting decision tree // Advances in Neural Information Processing Systems. — Vol. 30. — Pp. 3146–3154. DOI: https://doi.org/10.48550/arXiv.1811.00934. [in Eng.].

Lundberg, S. M., & Lee, S.-I. (2017). A unified approach to interpreting model predictions // Advances in Neural Information Processing Systems. — Vol. 30. — Pp. 4765–4774. DOI: https://doi.org/10.48550/arXiv.1705.07874. [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.].

Moustafa N., & Slay J. (2015). UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). — In Proc. MilCIS. — Pp. 1–6. IEEE. DOI: 10.1109/MilCIS.2015.7348942. [in Eng.].

Papernot, N., McDaniel, P., Goodfellow, I., Jha, S., Celik, Z. B., & Swami, A. (2017). Practical black-box attacks against machine learning // Proceedings of ACM ASIA CCS. — Pp. 506–519. DOI: https://doi.org/10.1145/3052973.3053009. [in Eng.].

Madry, A., Makelov, A., Schmidt, L., Tsipras, D., & Vladu, A. (2018). Towards deep learning models resistant to adversarial attacks // Proceedings of ICLR. DOI: DOI: https://doi.org/10.48550/arXiv.1706.06083. [in Eng.].

Mirsky, Y., Doitshman, T., Elovici, Y., &Shabtai, A. (2018). Kitsune: An ensemble of autoencoders for online network intrusion detection // Proceedings of NDSS. DOI: https://doi.org/10.14722/ndss.2018.23204. [in Eng.].

Sharafaldin, I., Lashkari, A. H., Hakak, S., &Ghorbani, A. A. (2019). Developing realistic DDoS attack dataset and taxonomy // Proceedings of ICCST. — Pp. 1–8. DOI: https://doi.org/10.1109/CCST.2019.8888419. [in Eng.].

TrabajoFernández, J. C., Palomo-Duarte, M., &Dodero, J. M. (2020). Applying machine learning to intrusion detection: A comparison // Proceedings of ARES. — Pp. 1–9. DOI: https://doi.org/10.1145/3407023.3409231. [in Eng.].

Pierazzi, F., Pendlebury, F., Cortellazzi, J., & Cavallaro, L. (2020). Intriguing properties of adversarial ML attacks in the problem space // Proceedings of the IEEE Symposium on Security and Privacy (SP 2020). — Pp. 1332–1349. DOI: https://doi.org/10.1109/SP40000.2020.00073. [in Eng.].

Wressnegger, C., Schwenk, G., Arp, D., &Rieck, K. (2013). A close look on n-grams in intrusion detection: Anomaly detection vs. classification. Proceedings of AISec. — Pp. 67–76. DOI: https://doi.org/10.1145/2517312.2517316. [in Eng.].

Yang, K., Liu, J., Zhang, C., & Fang, Y. (2018). Adversarial examples against the deep learning based network intrusion detection systems // Proceedings of MILCOM. — Pp. 559–564. DOI: https://doi.org/10.1109/MILCOM.2018.8599935. [in Eng.].

Yen, S. H., Lin, Y. D., Lai, Y. C., Ho, C. H., Yu, C. M., & Pitt, D. (2021). Deployment and verification of multiclass intrusion detection systems in IoT // IEEE Internet of Things Journal. — Vol. 8. — No. 10. — Pp. 8001–8012. DOI: https://doi.org/10.1109/JIOT.2020.3041007. [in Eng.].

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

Zhang, Y., Chen, X., Jin, L., Wang, X., &Guo, D. (2019). Network intrusion detection based on deep hierarchical network and original flow data // IEEE Access. — Vol. 7. — Pp. 37004–37016. DOI: https://doi.org/10.1109/ACCESS.2019.2905041. [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"