

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



**INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION
TECHNOLOGIES**

Published since 2020.
Volume 7. 2 (26). 2026
April–June

**ХАЛЫҚАРАЛЫҚ АҚПАРАТТЫҚ ЖӘНЕ КОММУНИКАЦИЯЛЫҚ
ТЕХНОЛОГИЯЛАР ЖУРНАЛЫ**

2020 жылдан бері шығарылады
Том 7. 2 (26). 2026
Сәуір-Маусым

**МЕЖДУНАРОДНЫЙ ЖУРНАЛ ИНФОРМАЦИОННЫХ И
КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ**

Издается с 2020 г.
Том 7. 2 (26). 2026
Апрель-Июнь

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 Rysbauly — 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)

Nurzhaz Duzbayev — PhD, associate professor, Vice-Rector for Digitalization and Innovation, International Information Technology University (Kazakhstan)

Bakhtgerai 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 Yeskendirowa — 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 Түлегеновна — 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)

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

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

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

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

Синчев Бахтгерей Кусанович — 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 бизнес медиа және басқару факультетінің деканы (Қазақстан)

Абикаликова Замира Тұрсынбаевна — 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 Максұтовна Ескендірова — 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)

Айтмағамбетов 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)

Тадеш 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)

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

Белюшицкая 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)

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

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

Айтмаганбетов 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 Сахбай — кандидат технических наук, профессор, профессор-исследователь кафедры компьютерной инженерии, Международного университета информационных технологий (Казахстан)

Алимсерб 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)

Белошицкая 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

D. Abzhanova, A. Biloshchytskyi

A MODEL AND METHOD FOR MANAGING DATA ON EMISSIONS FROM STATIONARY SOURCES OF POLLUTION IN AN INTELLIGENT ENVIRONMENTAL MONITORING SYSTEM9

A. Slanbekova, M. Rakhimzhanova, A. Zhanibekova, A. Alimagambetova, M. Xudoyberganov

EARLY DETECTION OF HYDROLOGICAL HAZARDS BASED ON SPATIOTEMPORAL ANALYSIS25

INFORMATION TECHNOLOGY

F.N. Abdraimova, A.A. Kereibayeva, D.S. Dyussenova, D.A. Aliyeva, T.Zh. Toktarova

AI TECHNOLOGIES IN LANGUAGE EDUCATION: PRACTICAL ASPECTS AND CHALLENGES OF STUDENT USAGE36

G. Azieva, M. Yessenova, A. Abzhapparova, G. Abdikerimova, P. Schmidt

HYBRID STACKING FRAMEWORK FOR CROP CLASSIFICATION USING UAV DATA50

A.K. Aitim

JOINT MORPHOLOGICAL DISAMBIGUATION AND POS TAGGING FOR AGGLUTINATIVE LANGUAGES62

S.A. Yesniyazova, S.T. Kaimov

PREDICTIVE MAINTENANCE OF HEAVY-DUTY TRUCKS USING EXPLAINABLE MACHINE LEARNING78

T. Imanbekova, Zh. Ibrayeva, G. Jakanova, G. Askanbay

DATA COMPRESSION ALGORITHM BASED ON WAVELET TRANSFORMER; ANALYSIS AND IMPLEMENTATION IN MATLAB92

B.Z. Kenzhegulov, Zh.T. Bilyalova, K.N. Uteuliyeva, L. Nurgaliyeva, Sh.S. Nurzhanova

A MATHEMATICAL AND ALGORITHMIC APPROACH TO THE DEVELOPMENT OF AN INTELLIGENT TEXT-TO-SQL SYSTEM BASED ON LARGE LANGUAGE MODELS110

N.Sh. Maxutova, J.A. Tussupov, A.A. Shekerbek, Zh.E. Kenzhebayeva, Q.O. Rakhimov

MACHINE LEARNING FOR COMPREHENSIVE EVALUATION OF CARDIOVASCULAR DISEASE RISK AND BIOCHEMICAL ALTERATIONS: FOCUS ON ASPARTATE AMINOTRANSFERASE131

O.S. Salykova, V.A. Madin, B.R. Salykov, D.N. Komarov, N.V. Manuilov

INTEGRATION OF MEMS ACCELEROMETER SENSOR MODULES IN INDUSTRIAL MONITORING SYSTEMS146

R. Taberkhan, M.A. Sambetbayeva, G. Kalman

KAZCAUSAL: THE FIRST CORPUS-BASED ANNOTATION OF CAUSAL RELATIONSHIPS IN THE KAZAKH LANGUAGE160

S.Tynymbayev, S.E. Mamanova, R. Berdybayev, Zh.E. Temirbekova, T. Chinibayeva

DIVIDING DEVICES WITH PRELIMINARY PREPARATION OF MULTIPLES OF THE DIVISOR172

K.N. Uteuliyeva, B.Z. Kenzhegulov, T.A. Karazhigitova, H.İ. Bülbül, Z.Zh. Zhanuzakova

MATHEMATICAL AND ALGORITHMIC APPROACHES TO THE DEVELOPMENT OF A COLLABORATIVE FILTERING-BASED RECOMMENDER SYSTEM188

S. Sharmukhanbet, G. Turmukhanova, O. Findik, V. Makhatova, L. Kurmangazyieva

HIGH-PRECISION ROBOTIC ASSEMBLY UNDER VARIABLE ILLUMINATION: A ROBUST MECHATRONIC ARCHITECTURE FOR VISUAL SERVOING209

INFORMATION SECURITY AND COMMUNICATION TECHNOLOGIES

A. Amirbay, Z. Amanbaikyzy, K. Maxutova, A. Mukhanova, M. Kassim

MACHINE LEARNING ALGORITHM FOR EARLY DETECTION OF AUTISM SPECTRUM DISORDERS IN CHILDREN BASED ON MULTIMODAL ANALYSIS OF EYE MOVEMENTS AND FACIAL EXPRESSIONS227

K. Baisylbayeva, Sh. Mussiraliyeva, Zh. Yeltay

DETECTION OF EXTREMIST IDEOLOGY IN THE KAZAKH LANGUAGE: ANNOTATION CHALLENGES AND DEEP LEARNING APPROACHES242

M.A. Bolatbek, A.M. Usmanova, K.B. Bagitova, G.B. Baispay

DEVELOPMENT AND RESEARCH OF A METHOD FOR ANALYZING NETWORK TRAFFIC TO IDENTIFY A CYBER THREAT	261
D.I. Prokopovych-Tkachenko, N.K. Zhumagalieva, D.N. Shchytov, N.F. Mormul, D.A. Cherkaskyi	
FUZZY MODEL FOR EVALUATING INFORMATION SECURITY PARAMETERS OF INFORMATION SYSTEMS UNDER INCOMPLETE AND QUALITATIVE DATA: CONSTRUCTION METHODOLOGY, RULE BASE TUNING, AND DEMONSTRATION CASE FOR ORGANIZATIONS	279
E.A. Pustovoy, O.A. Pustovaya, A.N. Raushanova, I.S. Zaurbekov	
EVALUATION OF THE EFFECTIVENESS OF SYNTHESIS OF STOCHASTIC MODELS WITH CONTROLLED PROPERTIES	305
Y. Serzhan, T. Umarov, A. Abilbayeva	
FRAUD DETECTION IN CREDIT CARD TRANSACTIONS USING MACHINE LEARNING: A COMPARATIVE ANALYSIS	321
T. Babenko, Ye. Bakhtiyarova, D. Yeskendirova, A. Sysoev, Sh. Makilenov	
FLEXIBLE IDPS BASED ON MACHINE LEARNING ALGORITHMS FOR DIPTYCHS AND IOT EDGE DEVICE PROTECTION	333

МАЗМҰНЫ

ӘЛЕУМЕТТІК-ЭКОНОМИКАЛЫҚ ЖҮЙЕЛЕРДІ ДАМУДАҒЫ ЦИФРЛЫҚ ТЕХНОЛОГИЯЛАР

Д.Е. Абжанов, А.А. Белошицкий	
ЭКОЛОГИЯЛЫҚ МОНИТОРИНГТІҢ ЗИЯТКЕРЛІК ЖҮЙЕСІНДЕГІ СТАЦИОНАРЛЫҚ ЛАСТАНУ КӨЗ-ДЕРІНІҢ ШЫҒАРЫНДЫЛАРЫ ТУРАЛЫ ДЕРЕКТЕРДІ БАСҚАРУДЫҢ МОДЕЛІ МЕН ӘДІСІ	9
А.Е. Сланбекова, М.Б. Рахимжанова, А.И. Жанибекова, А.З. Алимагамбетова, М. Худойбергенов	
КЕҢІСТІКТІК-УАҚЫТТЫҚ (SPATIOTEMPORAL) ТАЛДАУ НЕГІЗІНДЕ ГИДРОЛОГИЯЛЫҚ ҚАУІП-ҚАТЕРДІ ЕРТЕ АНЫҚТАУ	25

АҚПАРАТТЫҚ ТЕХНОЛОГИЯЛАР

Ф.Н. Абдраимова, А.А. Керейбаева, Д.С. Дюсенова, Д.А. Алиева, Т.Ж. Токтарова	
ТІЛ БІЛІМІНДЕ ЖАСАНДЫ ИНТЕЛЛЕКТ ТЕХНОЛОГИЯЛАРЫ: СТУДЕНТТЕР ҚОЛДАНУЫНЫҢ ПРАКТИКАЛЫҚ АСПЕКТІЛЕРІ МЕН МӘСЕЛЕЛЕРІ	36
Г.Т. Азиева, М.Б. Есенова, А.К. Абжаппарова, Г.Б. Абдикеримова, P. Schmidt	
UAV ДЕРЕКТЕРІ НЕГІЗІНДЕ АУЫЛ ШАРУАШЫЛЫҒЫ ДАҚЫЛДАРЫН ЖІКТЕУГЕ АРНАЛҒАН ГИБРИДТІ СТЕКИНГ МОДЕЛІ	50
Ә.Қ. Әйтiм	
АГГЛЮТИНАТИВТІ ТІЛДЕРГЕ АРНАЛҒАН МОРФОЛОГИЯЛЫҚ ДИЗАМБИГУАЦИЯ МЕН POS-ТАҢ-БАЛАУДЫ БІРЛЕСІП МОДЕЛЬДЕУ	62
С.А. Есниязова, С.Т. Каимов	
ТҮСІНДІРІЛЕТІН МАШИНАЛЫҚ ОҚЫТУДЫ ҚОЛДАНА ОТЫРЫП АУЫР ЖҮК КӨЛІКТЕРІНЕ БОЛЖАМДЫ ТЕХНИКАЛЫҚ ҚЫЗМЕТ КӨРСЕТУ	78
Т.Д. Иманбекова, Ж.Б. Ибраева, Г.Т. Джаканова, Г.Т. Асқанбай	
МӘЛІМЕТТЕРДІ ВЕЙВЛЕТ-ТҮРЛЕНДІРГІШТІҢ НЕГІЗІНДЕ ҚЫСУ АЛГОРИТМІ; MATLAB ОРТАСЫНДА ТАЛДАУ ЖӘНЕ ІСКЕ АСЫРУ	92
Б.З. Кенжегулов, Ж.Т. Билялова, К.Н. Утеулиева, Л. Нургалиева, Ш.С. Нуржанова	
ҮЛКЕН ТІЛДІК МОДЕЛЬДЕР НЕГІЗІНДЕ ИНТЕЛЛЕКТУАЛДЫ TEXT-TO-SQL ЖҮЙЕСІН ӨЗІРЛЕУДІҢ МАТЕМАТИКАЛЫҚ-АЛГОРИТМДІК ТӘСІЛІ	110
Н.Ш. Максұтова, Ж.А. Тусупов, А.Ә. Шекербек, Ж.Е. Кенжебаева, К.О. Рахимов	
ЖҮРЕК-ҚАН ТАМЫРЛАРЫ АУРУЛАРЫНЫҢ ҚАУІП-ҚАТЕРІН ЖӘНЕ БИОХИМИЯЛЫҚ ӨЗГЕРІСТЕРДІ КЕШЕНДІ БАҚАЛАУ ҮШІН МАШИНАЛЫҚ ОҚЫТУ: АСПАРТАМИНОТРАНСФЕРАЗАҒА ЕРЕКШЕ НАЗАР	131
О.С. Салыкова, В.А. Мадин, Б.Р. Салыков, Д.Н. Комаров, Н.В. Манұйлов	
ӨНЕРКӘСІПТІК МОНИТОРИНГ ЖҮЙЕЛЕРІНДЕГІ MEMS-АКСЕЛЕРОМЕТРЛЕРДІҢ СЕНСОРЛЫҚ МОДУЛЬДЕРІН ИНТЕГРАЦИЯЛАУ	146
Р. Таберхан, М.А. Самбетбаева, Г. Қалман	
КАЗСАUSAL: ҚАЗАҚ ТІЛІНДЕГІ СЕБЕП-САЛДАРЛЫҚ ҚАТЫНАСТАРДЫҢ АЛҒАШҚЫ КОРПУСТЫҚ АННОТАЦИЯСЫ	160



С. Тынымбаев, С.Е. Маманова, Р. Бердібаев, Ж.Е. Темірбекова, Т. Чинибаева БӨЛГІШТІҢ ЕСЕЛІ МӘНДЕРІН АЛДЫН АЛА ДАЙЫНДАУМЕН ЖҮЗЕГЕ АСЫРЫЛАТЫН БӨЛУ ҚҰРЫЛҒЫЛАРЫ	172
К.Н. Утеулиева, Б.З. Кенжегулов, Т.А. Каражигитова, Х. Булбул, З.Ж. Жанузакова КОЛЛАБОРАТИВТІК СҮЗГІЛЕУ НЕГІЗІНДЕГІ ҰСЫНЫМДЫҚ ЖҮЙЕНІ ӨЗІРЛЕУДІҢ МАТЕМАТИКАЛЫҚ-АЛГОРИТМДІК ТӘСІЛДЕРІ	188
С. Шармұханбет, Г. Тұрмұханова, О. Финдик, В. Махатова, Л. Курмангазиева АЙНЫМАЛЫ ЖАРЫҚ ЖАҒДАЙЫНДАҒЫ ЖОҒАРЫ ДӘЛДІКТІ РОБОТТЫҚ ҚҰРАСТЫРУ: ВИЗУАЛДЫ СЕРВОТЕЖЕУДІҢ ТӨЗІМДІ МЕХАТРОНИКАЛЫҚ АРХИТЕКТУРАСЫ	209

АҚПАРАТТЫҚ ҚАУІПСІЗДІК ЖӘНЕ КОММУНИКАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАРҒА АРНАЛҒАН

А. Амирбай, З. Аманбайқызы, К. Максұтова, А. Мұханова, М. Kassim КӨЗ ҚОЗҒАЛЫСТАРЫ МЕН БЕТ МИМИКА БЕЛГІЛЕРІН МУЛЬТИМОДАЛЬДЫ ТАЛДАУҒА НЕГІЗ- ДЕЛГЕН БАЛАЛАРДАҒЫ АУТИЗМ СПЕКТРІНІҢ БҰЗЫЛЫСТАРЫН ЕРТЕ АНЫҚТАУҒА АРНАЛҒАН МАШИНАЛЫҚ ОҚЫТУ АЛГОРИТМІ	227
К.Д. Байсылбаева, Ш.Ж. Мусиралиева, Ж. Елтай ҚАЗАҚ ТІЛІНДЕГІ ЭКСТРЕМИСТІК ИДЕОЛОГИЯНЫ АНЫҚТАУ: АННОТАЦИЯЛАУ МӘСЕЛЕЛЕРІ ЖӘНЕ ТЕРЕҢ ОҚЫТУ ТӘСІЛДЕРІ	242
М.А. Болатбек, А.М. Усманова, Қ.Б. Бағитова, Г.Б. Байспай КИБЕР ҚАУІПТІ АНЫҚТАУ ҮШІН ЖЕЛІЛІК ТРАФИКТІ ТАЛДАУ ӘДІСІН ӨЗІРЛЕУ ЖӘНЕ ЗЕРТТЕУ	261
Д.И. Прокопович-Ткаченко, Н.К. Жумағалиева, Д.Н. Щитов, Н.Ф. Мормуль, Д.А. Черкасский ТОЛЫҚ ЕМЕС ЖӘНЕ САПАЛЫҚ ДЕРЕКТЕР ЖАҒДАЙЫНДА АҚПАРАТТЫҚ ЖҮЙЕЛЕРДІҢ АҚПА- РАТТЫҚ ҚАУІПСІЗДІК ПАРАМЕТРЛЕРІН БАҒАЛАУДЫҢ БҰЛЫҢҒЫР МОДЕЛІ: ҚҰРУ ӘДІСТЕМЕСІ, ЕРЕЖЕЛЕР БАЗАСЫН БАПТАУ ЖӘНЕ ҰЙЫМДАРҒА АРНАЛҒАН ДЕМОСТРАЦИЯЛЫҚ КЕЙС	279
Е.А. Пустовой, О.А. Пустовая, А.Н. Раушанова, И.С. Заурбеков БАСҚАРЫЛАТЫН ҚАСИЕТТЕРІ БАР СТОХАСТИКАЛЫҚ МОДЕЛЬДЕРДІ СИНТЕЗДЕУДІҢ ТИІМДІЛІГІН БАҒАЛАУ	305
Е. Сержан, Т. Умаров, А. Әбілбаева МАШИНАЛЫҚ ОҚУ ӘДІСІ АРҚЫЛЫ КРЕДИТ КАРТА ОПЕРАЦИЯЛАРЫНДАҒЫ АЛАЯҚТЫҚТЫ АНЫҚТАУ: САЛЫСТЫРМАЛЫ ТАЛДАУ	321
Т.В. Бабенко, Е.А. Бахтиярова, Д.М. Ескендірова, А. Сысоев, Ш.Н. Макиленов ДИПТИХ ЖӘНЕ ІОТ ШЕТКІ ҚҰРЫЛҒЫЛАРЫН ҚОРҒАУҒА АРНАЛҒАН МАШИНАЛЫҚ ОҚЫТУ АЛГОРИТМДЕРІНЕ НЕГІЗДЕЛГЕН ІКЕМДІ IDPS	333

СОДЕРЖАНИЕ ЦИФРОВЫЕ ТЕХНОЛОГИИ В РАЗВИТИИ СОЦИО-ЭКОНОМИЧЕСКИХ СИСТЕМ

Д.Е. Абжанова, А.А. Белошицкий МОДЕЛЬ И МЕТОД УПРАВЛЕНИЯ ДАННЫМИ О ВЫБРОСАХ СТАЦИОНАРНЫХ ИСТОЧНИКОВ ЗАГРЯЗНЕНИЯ В ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЕ ЭКОЛОГИЧЕСКОГО МОНИТОРИНГА	9
А.Е. Сланбекова, М.Б. Рахимжанова, А.И. Жанибекова, А.З. Алимагамбетова, М. Худойбергенов РАННЕЕ ВЫЯВЛЕНИЕ ГИДРОЛОГИЧЕСКИХ ОПАСНОСТЕЙ НА ОСНОВЕ ПРОСТРАНСТВЕННО- ВРЕМЕННОГО (SPATIOTEMPORAL) АНАЛИЗА	25

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Ф.Н. Абдраимова, А.А. Керейбаева, Д.С. Дюсенова, Д.А. Алиева, Т.Ж. Токтарова ТЕХНОЛОГИИ ИИ В ЯЗЫКОВОМ ОБРАЗОВАНИИ: ПРАКТИЧЕСКИЕ АСПЕКТЫ И ПРОБЛЕМЫ ПРИМЕНЕНИЯ СТУДЕНТАМИ	36
Г.Т. Азиева, М.Б. Есенова, А.К. Абжаппарова, Г.Б. Абдикеримова, Р. Schmidt ГИБРИДНАЯ МОДЕЛЬ СТЕКИНГА ДЛЯ КЛАССИФИКАЦИИ СЕЛЬСКОХОЗЯЙСТВЕННЫХ КУЛЬТУР ПО ДАННЫМ UAV	50
Ә.Қ. Әйтім	

СОВМЕСТНАЯ МОРФОЛОГИЧЕСКАЯ ДИЗАМБИГУАЦИЯ И POS-РАЗМЕТКА ДЛЯ АГГЛЮТИНАТИВНЫХ ЯЗЫКОВ	62
С.А. Есниязова, С.Т. Каимов	
ПРЕДИКТИВНОЕ ТЕХНИЧЕСКОЕ ОБСЛУЖИВАНИЕ ТЯЖЁЛЫХ ГРУЗОВИКОВ С ИСПОЛЬЗОВАНИЕМ ОБЪЕСНИМОГО МАШИННОГО ОБУЧЕНИЯ	78
Т.Д. Иманбекова, Ж.Б. Ибраева, Г.Т. Джаканова, Г.Т. Асканбай	
АЛГОРИТМ СЖАТИЯ ДАННЫХ НА ОСНОВЕ ВЕЙВЛЕТ-ПРЕОБРАЗОВАТЕЛЯ: АНАЛИЗ И РЕАЛИЗАЦИЯ В МАТЛАВ	92
Б.З. Кенжегулов, Ж.Т. Билялова, К.Н. Утеулиева, Л. Нургалиева, Ш.С. Нуржанова	
МАТЕМАТИКО-АЛГОРИТМИЧЕСКИЙ ПОДХОД К РАЗРАБОТКЕ ИНТЕЛЛЕКТУАЛЬНОЙ TEXT-TO-SQL СИСТЕМЫ НА ОСНОВЕ БОЛЬШИХ ЯЗЫКОВЫХ МОДЕЛЕЙ	110
Н.Ш. МаксUTOва, Д.А. Тусупов, А.А. Шекербек, Ж.Е. Кенжебаева, К.О. Рахимов	
МАШИННОЕ ОБУЧЕНИЕ ДЛЯ КОМПЛЕКСНОЙ ОЦЕНКИ РИСКА СЕРДЕЧНО-СОСУДИСТЫХ ЗАБОЛЕВАНИЙ И БИОХИМИЧЕСКИХ ИЗМЕНЕНИЙ: АКЦЕНТ НА АСПАРТАТАМИНОТРАНСФЕРАЗЕ ...	131
О.С. Салыкова, В.А. Мадин, Б.Р. Салыков, Д.Н. Комаров, Н.В. Мануйлов	
ИНТЕГРАЦИЯ СЕНСОРНЫХ МОДУЛЕЙ MEMS-АКСЕЛЕРОМЕТРОВ В СИСТЕМАХ ПРОМЫШЛЕННОГО МОНИТОРИНГА	146
Р. Таберхан, М.А. Самбетбаева, Г. Калман	
КАЗСАUSAL: ПЕРВАЯ КОРПУСНАЯ АННОТАЦИЯ ПРИЧИННО-СЛЕДСТВЕННЫХ СВЯЗЕЙ НА КАЗАХСКОМ ЯЗЫКЕ	160
С. Тынымбаев, С.Е. Маманова, Р. Бердибаев, Ж.Е. Темирбекова, Т. Чинибаева	
УСТРОЙСТВА ДЕЛЕНИЯ ЧИСЕЛ С ПРЕДВАРИТЕЛЬНОЙ ПОДГОТОВКОЙ КРАТНЫХ ДЕЛИТЕЛЮ	172
К.Н. Утеулиева, Б.З. Кенжегулов, Т.А. Каражигитова, Х.Бюльбюль, З.Ж. Жанузакова	
МАТЕМАТИКО-АЛГОРИТМИЧЕСКИЕ ПОДХОДЫ К РАЗРАБОТКЕ РЕКОМЕНДАТЕЛЬНОЙ СИСТЕМЫ НА ОСНОВЕ КОЛЛАБОРАТИВНОЙ ФИЛЬТРАЦИИ	188
С. Шармуханбет, Г. Турмуханова, О.Финдик, В.Махатова, Л. Курмангазиева	
ВЫСОКОТОЧНАЯ РОБОТИЗИРОВАННАЯ СБОРКА ПРИ ПЕРЕМЕННОЙ ОСВЕЩЁННОСТИ: РОБАСТНАЯ МЕХАТРОННАЯ АРХИТЕКТУРА ВИЗУАЛЬНОГО СЕРВОУПРАВЛЕНИЯ	209

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ

А. Амирбай, З. Аманбайкызы, К. МаксUTOва, А. Муханова, М. Kassim	
АЛГОРИТМ МАШИННОГО ОБУЧЕНИЯ ДЛЯ РАННЕГО ВЫЯВЛЕНИЯ РАССТРОЙСТВ АУТИСТИЧЕСКОГО СПЕКТРА У ДЕТЕЙ НА ОСНОВЕ МУЛЬТМОДАЛЬНОГО АНАЛИЗА ДАННЫХ ДВИЖЕНИЯ ГЛАЗ И МИМИЧЕСКИХ СИГНАЛОВ	227
К.Д. Байсылбаева, Ш.Ж. Мусиралиева, Ж.Елтай	
ОБНАРУЖЕНИЕ ЭКСТРЕМИСТСКОЙ ИДЕОЛОГИИ НА КАЗАХСКОМ ЯЗЫКЕ: ПРОБЛЕМЫ АННОТИРОВАНИЯ И МЕТОДЫ ГЛУБОКОГО ОБУЧЕНИЯ	242
М.А. Болатбек, А.М. Усманова, К.Б. Багитова, Г.Б. Байспай	
РАЗРАБОТКА И ИССЛЕДОВАНИЕ МЕТОДА АНАЛИЗА СЕТЕВОГО ТРАФИКА ДЛЯ ВЫЯВЛЕНИЯ КИБЕРУГРОЗЫ	261
Д.И. Прокопович-Ткаченко, Н.К. Жумагалиева, Д.Н. Щитов, Н.Ф. Мормуль, Д.А. Черкасский	
НЕЧЕТКАЯ МОДЕЛЬ ОЦЕНИВАНИЯ ПАРАМЕТРОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ В УСЛОВИЯХ НЕПОЛНЫХ И КАЧЕСТВЕННЫХ ДАННЫХ: МЕТОДИКА ПОСТРОЕНИЯ, НАСТРОЙКА БАЗЫ ПРАВИЛ И ДЕМОСТРАЦИОННЫЙ КЕЙС ДЛЯ ОРГАНИЗАЦИЙ	279
Е.А. Пустовой, О.А. Пустовая, А.Н. Раушанова, И.С. Заурбеков	
ОЦЕНКА ЭФФЕКТИВНОСТИ СИНТЕЗА СТОХАСТИЧЕСКИХ МОДЕЛЕЙ С УПРАВЛЯЕМЫМИ СВОЙСТВАМИ	305
Е. Сержан, Т. Умаров, А. Абилябаева	
ВЫЯВЛЕНИЕ МОШЕННИЧЕСТВА С ИСПОЛЬЗОВАНИЕМ МАШИННОГО ОБУЧЕНИЯ ПРИ ОПЕРАЦИЯХ С КРЕДИТНЫМИ КАРТАМИ: СРАВНИТЕЛЬНЫЙ АНАЛИЗ	321
Т. Бабенко, Е. Бахтирова, Д. Ескендинова, А. Сысоев, Ш. Макиленов	
ГИБКАЯ IDPS НА ОСНОВЕ АЛГОРИТМОВ МАШИННОГО ОБУЧЕНИЯ ДЛЯ МОНИТОРИНГА И ЗАЩИТЫ ПЕРИФЕРИЙНЫХ IoT-УСТРОЙСТВ	333



INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES

ISSN 2708–2032 (print)

ISSN 2708–2040 (online)

Vol. 7. Is.2. Number 26 (2026). Pp. 333–348

Journal homepage: <https://journal.iitu.edu.kz><https://doi.org/10.54309/IJICT.2026.26.2.021>

УДК 004.056.5

FLEXIBLE IDPS BASED ON MACHINE LEARNING ALGORITHMS FOR DIPTYCHS AND IOT EDGE DEVICE PROTECTION

T. Babenko, Ye. Bakhtiyarova*, D. Yeskendiroya, A. Sysoev, Sh. Makilenov

International Information Technology University, Almaty, Kazakhstan.

E-mail: y.bakhtiyarova@iitu.edu.kz

Tatiana Babenko — Doctor of Technical Sciences, Professor, Department of Cybersecurity, International University of Information Technologies, Almaty, Kazakhstan

<https://orcid.org/0000-0003-1184-9483>;

Yelena Bakhtiyarova — Candidate of Technical Sciences, Associate Professor, Head of the Department of Radio Engineering, Electronics, and Telecommunications, International University of Information Technologies, Almaty, Kazakhstan

E-mail: y.bakhtiyarova@iitu.edu.kz, <https://orcid.org/0000-0001-8735-7683>;

Damelya Yeskendiroya — Candidate of Technical Sciences, Head of the Department of Cybersecurity, International University of Information Technologies, Almaty, Kazakhstan

<https://orcid.org/0000-0003-4270-1908>;

Askar Sysoev — PhD, Senior Lecturer, Department of Cybersecurity, International Information Technology University, Almaty, Kazakhstan

<https://orcid.org/0009-0002-5842-1847>;

Shakirt Makilenov — doctoral student at the International University of Information Technology, Almaty, Kazakhstan

<https://orcid.org/0000-0002-5330-4716>.

© T. Babenko, Ye. Bakhtiyarova, D. Yeskendiroya, A. Sysoev, Sh. Makilenov

Abstract. The growing number of edge IoT devices in smart city infrastructures poses new challenges related to a fragmented attack surface and the limitations of traditional intrusion detection tools. Existing IDS systems typically operate in isolation, generate redundant alerts, and are unable to adapt to distributed environments. This paper proposes the architecture of a flexible IDS that leverages machine learning algorithms to improve the monitoring and protection of edge devices. The architecture includes modules for normalization, deduplication, correlation, and ML analysis, with the ability to provide feedback between the monitoring center and edge nodes. The architectural description of the monitoring environment is based on a hierarchical representation consistent with the Purdue model, allowing for the distinction between edge, local, and centralized levels of



protection. Experimental evaluation on the BoT-IoT and TON_IoT datasets demonstrated a reduction in event correlation latency by approximately 62% and a decrease in the false positive rate by 29–31% compared to baseline approaches. The obtained results confirm the potential of the proposed architecture for smart city infrastructures.

Keywords: intrusion detection and prevention system, Internet of Things, machine learning, smart city, edge devices, alert normalization, event correlation, edge computing, Purdue model

For citation: T. Babenko, Ye. Bakhtiyarova, D. Yeskendirova, A. Sysoyev, Sh. Makilenov (2026). Flexible idps based on machine learning algorithms for diptychs and iot edge device protection // International journal of information and communication technologies. Vol. 7. No. 26. Pp. 333–348. <https://doi.org/10.54309/IJICT.2026.26.2.021>. (In Russ.).

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

Acknowledgment: *This study was supported by the Science Committee of the Ministry of Science and Higher Education of the Republic of Kazakhstan under IRN AP26104787, «Development of AI-based Solutions for Protecting the IoT Infrastructure of Smart Cities in Kazakhstan.»*

ДИПТИХ ЖӘНЕ ИОТ ШЕТКІ ҚҰРЫЛҒЫЛАРЫН ҚОРҒАУҒА АРНАЛҒАН МАШИНАЛЫҚ ОҚЫТУ АЛГОРИТМДЕРІНЕ НЕГІЗДЕЛГЕН ИКЕМДІ IDPS

**Т.В. Бабенко, Е.А. Бахтиярова*, Д.М. Ескендірова, А. Сысоев,
Ш.Н. Макиленов**

Халықаралық ақпараттық технологиялар университеті, Алматы, Қазақстан.

E-mail: y.bakhtiyarova@iitu.edu.kz

Бабенко Татьяна Василевна — т.ғ.д., «Киберқауіпсіздік» кафедрасының профессоры Халықаралық ақпараттық технологиялар университеті, Алматы, Қазақстан
<https://orcid.org/0000-0003-1184-9483>;

Бахтиярова Елена Ажибековна — т.ғ.к, қауымдастырылған профессор «Радиотехника, электроника және телекоммуникациялар» кафедрасының меңгерушісі, Халықаралық ақпараттық технологиялар университеті, Алматы, Қазақстан
E-mail: y.bakhtiyarova@iitu.edu.kz, <https://orcid.org/0000-0001-8735-7683>;

Ескендірова Дамеля Максutowна — т.ғ.к, «Киберқауіпсіздік» кафедрасының меңгерушісі Халықаралық ақпараттық технологиялар университеті, Алматы, Қазақстан
<https://orcid.org/0000-0003-4270-1908>;

Сысоев Аскар — PhD, киберқауіпсіздік кафедрасының аға оқытушысы, Халықаралық ақпараттық технологиялар университеті, Алматы, Қазақстан
<https://orcid.org/0009-0002-5842-1847>;

Макиленов Шакирт Нурлубекулы — докторант, Халықаралық ақпараттық технологиялар университеті, Алматы, Қазақстан
<https://orcid.org/0000-0002-5330-4716>.

© Т.В. Бабенко, Е.А. Бахтиярова, Д.М. Ескендинова, А. Сысоев, Ш.Н. Макиленов

Аннотация. Ақылды қала инфрақұрылымдарындағы шеткі IoT құрылғыларының санының артуы фрагменттелген шабуыл бетіне және дәстүрлі басып кіруді анықтау құралдарының шектеулеріне байланысты жаңа қиындықтар туғызады. Қолданыстағы IDS жүйелері әдетте оқшауланған күйде жұмыс істейді, артық ескертулер жасайды және таратылған ортаға бейімделе алмайды. Бұл мақалада шеткі құрылғыларды бақылау мен қорғауды жақсарту үшін машиналық оқыту алгоритмдерін пайдаланатын икемді IDS архитектурасы ұсынылады. Архитектураға бақылау орталығы мен шеткі түйіндер арасында кері байланыс беру мүмкіндігімен қалыпқа келтіру, қайталауды алып тастау, корреляция және ML талдау модульдері кіреді. Мониторинг ортасының архитектуралық сипаттамасы Purdue моделіне сәйкес иерархиялық көрініске негізделген, бұл шеткі, жергілікті және орталықтандырылған қорғау деңгейлерін ажыратуға мүмкіндік береді. VoT-IoT және TON_IoT деректер жиынтықтары бойынша эксперименттік бағалау бастапқы тәсілдермен салыстырғанда оқиға корреляциясының кідірісінің шамамен 62%-ға және жалған оң нәтижелер көрсеткішінің 29-31%-ға төмендегенін көрсетті. Алынған нәтижелер ақылды қала инфрақұрылымдары үшін ұсынылған архитектураның әлеуетін растайды.

Түйінді сөздер: енуді анықтау және алдын алу жүйесі, Заттар интернеті, машиналық оқыту, ақылды қала, шеткі құрылғылар, дабылдарды қалыпқа келтіру, оқиғалар корреляциясы, шеткі есептеулер, Purdue моделі

Дәйексөздер үшін: Т.В. Бабенко, Е.А. Бахтиярова, Д.М. Ескендинова, А. Сысоев, Ш.Н. Макиленов (2026). Диптих және iot шеткі құрылғыларын қорғауға арналған машиналық оқыту алгоритмдеріне негізделген икемді IDPS // Халықаралық ақпараттық және коммуникалық технологиялар журналы. Т. 7. No. 26. Б.333–348. <https://doi.org/10.54309/IJICT.2026.26.2.021>. (Орыс. тіл.).

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

Алғыс: Бұл мақала Қазақстан Республикасы Ғылым және жоғары білім министрлігі Ғылым комитетінің қаржылық қолдауымен, AP26104787 «Жасанды интеллект негізінде Қазақстанның ақылды қалаларының IoT-инфрақұрылымын қорғау шешімдерін әзірлеу» атты жобасы аясында орындалды.

ГИБКАЯ IDPS НА ОСНОВЕ АЛГОРИТМОВ МАШИННОГО ОБУЧЕНИЯ ДЛЯ МОНИТОРИНГА И ЗАЩИТЫ ПЕРИФЕРИЙНЫХ IoT-УСТРОЙСТВ

Т. Бабенко, Е. Бахтиярова*, Д. Ескендинова, А. Сысоев, Ш. Макиленов

Международный университет информационных технологий, Алматы, Казахстан.

E-mail: y.bakhtiyarova@iitu.edu.kz

Бабенко Татьяна Василевна — д.т.н., профессор кафедры «Кибербезопасность», Международный университет информационных технологий, Алматы, Казахстан



<https://orcid.org/0000-0003-1184-9483>;

Бахтиярова Елена Ажибековна — к.т.н., ассоциированный профессор, заведующий кафедрой «Радиотехника, электроника и телекоммуникации», Международный университет информационных технологий, Алматы, Казахстан

E-mail: y.bakhtiyarova@iitu.edu.kz, <https://orcid.org/0000-0001-8735-7683>;

Ескендирова Дамеля Максutowна — к.т.н., заведующий кафедрой «Кибербезопасность», Международный университет информационных технологий, Алматы, Казахстан

<https://orcid.org/0000-0003-4270-1908>;

Аскар Сысоев — PhD, старший преподаватель кафедры кибербезопасности, Международный университет информационных технологий, Алматы, Казахстан

<https://orcid.org/0009-0002-5842-1847>;

Макиленов Шакирт Нурлубекулы — докторант, Международного университета информационных технологий, Алматы, Казахстан

<https://orcid.org/0000-0002-5330-4716>.

© Т. Бабенко, Е. Бахтиярова, Д. Ескендирова, А. Сысоев, Ш. Макиленов

Аннотация. Рост числа периферийных IoT-устройств в инфраструктуре умных городов порождает новые вызовы, связанные с фрагментированной поверхностью атак и ограниченностью традиционных средств обнаружения вторжений. Существующие системы IDPS, как правило, работают изолированно, генерируют избыточные алерты и не способны адаптироваться к условиям распределённой среды. В данной статье предлагается архитектура гибкой IDPS, использующей алгоритмы машинного обучения для повышения качества мониторинга и защиты периферийных устройств. Архитектура включает модули нормализации, дедупликации, корреляции и ML-анализа с возможностью обратной связи между центром мониторинга и edge-узлами. Архитектурное описание среды мониторинга опирается на иерархическое представление, согласующееся с моделью Purdue, что позволяет разграничить периферийный, локальный и централизованный уровни защиты. Экспериментальная оценка на датасетах VoT-IoT и TON_IoT показала сокращение задержки корреляции событий примерно на 62% и снижение доли ложных срабатываний на 29–31% по сравнению с базовыми подходами. Полученные результаты подтверждают перспективность предложенной архитектуры для инфраструктур умного города.

Ключевые слова: система обнаружения и предотвращения вторжений, Интернет вещей, машинное обучение, умный город, периферийные устройства, нормализация алертов, корреляция событий, edge-вычисления, модель Purdue

Для цитирования: Т. Бабенко, Е. Бахтиярова, Д. Ескендирова, К. Сансызбай, Ш. Макиленов (2026). Гибкая idps на основе алгоритмов машинного обучения для мониторинга и защиты периферийных iot-устройств // Международный журнал информационных и коммуникационных технологий. Т. 7. No. 26. Стр. 333–348. <https://doi.org/10.54309/IJICT.2026.26.2.021>. (На русс.).

Конфликт интересов: авторы заявляют об отсутствии конфликта интересов.

Благодарность: Статья выполнена при финансовой поддержке Комитета науки Министерства науки и высшего образования Республики Казахстан в рамках проекта ИРН AP26104787 «Разработка решений для защиты IoT-инфраструктуры умных городов Казахстана на основе искусственного интеллекта».

Введение.

Городская среда меняется быстрее, чем успевают перестраиваться модели её защиты. Умные города внедряют тысячи подключённых устройств, от датчиков качества воздуха до контроллеров критической инфраструктуры (Jo et al., 2019; Elvas et al., 2021). По оценкам, к 2030 году их число может достичь нескольких миллиардов (Du et al., 2019) и каждое из них выступает не только источником данных, но и потенциальной точкой проникновения для злоумышленника (Almeida, 2023). При этом значительная часть таких устройств располагается на периферии сети, то есть на тех уровнях, где вычислительные ресурсы ограничены, а каналы связи нестабильны (Shi et al., 2016).

Модели кибербезопасности, сложившиеся вокруг централизованных сетевых периметров, оказываются в этих условиях недостаточно эффективными. Центры мониторинга безопасности (SOC), исторически служившие ядром оперативного реагирования (Bhatt et al., 2014), рассчитаны на относительно стабильные топологии с хорошо определёнными границами (Kotenko et al., 2012). Сети умного города, однако, простираются на обширные территории и включают устройства различных производителей, работающие по разнородным протоколам (Sisinni et al., 2018). Атаки на IoT-устройства нередко развиваются стремительно, эксплуатируя уязвимости ресурсоограниченных узлов до того, как централизованные механизмы обнаружения смогут сопоставить разрозненные сигналы в целостную картину (Liu et al., 2020).

Системы обнаружения и предотвращения вторжений (IDPS) призваны мониторить сетевой трафик на предмет вредоносных паттернов (Zarpeão et al., 2017; Walling et al., 2025). Платформы вроде Suricata и Zeek обладают развитыми возможностями анализа пакетов и сигнатурного обнаружения (Raxson, 1998). Тем не менее, в условиях распределённой IoT-среды они страдают от фундаментального дефицита интеграции (Aktar et al., 2024). Большинство установок работают как изолированные сенсоры, генерирующие алерты в несогласованных форматах без координации с централизованной платформой оркестрации (La et al., 2021). Это создаёт информационные силосы, в которых фрагменты многостадийных атак теряют контекст (Wardana et al., 2024).

Здесь важно заметить, что сами по себе алгоритмы машинного обучения, при всей их перспективности для выявления аномалий, не решают проблему изолированности и негибкости IDPS. Применение ML в задачах обнаружения вторжений описано в ряде обзорных работ (Zarpeão et al., 2017; Walling et al., 2025; Mitchell et al., 2014), однако вопрос о том, как встроить такие модели в гибкую, модульную архитектуру, адаптированную к условиям периферийной IoT-среды, остаётся открытым. Стандарты обмена информацией об угрозах, такие как STIX и TAXII (Iqbal et

al., 2018; Sauerwein et al., 2017), предоставляют полезные строительные блоки, но их внедрение в реальных развёртываниях умных городов пока фрагментарно (Najafi et al., 2021).

Целью данной статьи является разработка архитектуры гибкой IDPS на основе алгоритмов машинного обучения для мониторинга и защиты периферийных IoT-устройств. Под гибкостью здесь понимается способность системы адаптироваться к различным типам устройств, модульно встраивать и заменять аналитические компоненты, а также обеспечивать двунаправленную связь между центром мониторинга и периферийными сенсорами. Научная новизна состоит в предложении архитектуры, которая объединяет нормализацию, дедупликацию, ML-анализ и приоритизацию событий в единый конвейер, адаптированный для периферийного уровня IoT-инфраструктуры. Практическая значимость определяется возможностью использования подхода при построении систем безопасности для национальной инфраструктуры умных городов.

Материалы и методы.

Анализ существующих подходов

Особенности защиты периферийных IoT-устройств

Периферийные IoT-устройства принципиально отличаются от традиционных конечных точек корпоративной сети. Прежде всего, речь идёт об ограниченных вычислительных ресурсах: многие датчики работают на микроконтроллерах с объёмом памяти в десятки килобайт, что делает невозможным развёртывание полноценного агентского ПО безопасности (Shi et al., 2016). Разнообразие протоколов (MQTT, CoAP, Zigbee, BLE) создаёт гетерогенную среду, в которой единые правила обнаружения вторжений теряют универсальность (Sisinni et al., 2018; Hernández-Ramos et al., 2018). Устройства нередко эксплуатируются в удалённых точках, что усложняет обновление прошивок (Du et al., 2019).

Распределённость добавляет ещё один критический фактор. В инфраструктуре умного города периферийные устройства могут находиться на значительных расстояниях от центра обработки данных, а сетевая связь между ними бывает ограничена по пропускной способности (Shi et al., 2016). Это означает, что часть аналитической работы должна выполняться непосредственно на периферии, до передачи результатов на более высокие уровни. Если воспользоваться логикой иерархического представления, близкого к модели Purdue (Williams, 1994), периферийные IoT-устройства располагаются на нижних уровнях (сенсоры, актуаторы, полевые устройства), где задержка критична, а централизованная защита запаздывает. Этим объясняется необходимость локальных механизмов предварительного анализа и фильтрации.

Традиционные IDPS и их ограничения

Классические системы обнаружения вторжений развивались в условиях относительно гомогенных корпоративных сетей. Платформы вроде Snort, Suricata и Zeek обеспечивали сигнатурный анализ трафика и некоторые возможности поведенческого обнаружения (Rahson, 1998). Однако при перенесении этих инструментов в распределённую IoT-среду обнаруживаются существенные недостатки.

Первый из них связан с локальностью обнаружения: каждый сенсор видит лишь свой сегмент трафика и не располагает информацией о событиях на других участках (Aktar et al., 2024). Для многостадийных атак это означает неизбежную потерю контекста (Wardana et al., 2024). Второй недостаток заключается в слабой координации: когда несколько IDPS работают параллельно, каждая генерирует свой поток алертов в собственном формате без согласования метаданных (La et al., 2021). Третий касается шума: в типичной IoT-среде число ложных срабатываний достигает 30 и более процентов от общего объёма, что приводит к усталости аналитиков (Almeida, 2023; Aktar et al., 2024).

Применение алгоритмов машинного обучения в IDPS

Методы машинного обучения всё чаще рассматриваются как средство повышения качества обнаружения. Обзорные работы (Zarpelão et al., 2017; Walling et al., 2025) показывают, что модели классификации и детекции аномалий способны выявлять паттерны в сетевом трафике, которые трудно описать вручную через сигнатурные правила. Это особенно актуально в IoT-среде, поскольку поведение устройств существенно варьируется (Yasaei et al., 2020).

При этом применение ML сопряжено с рядом сложностей. Concept drift, то есть изменение характеристик трафика во времени, приводит к деградации моделей, обученных на исторических данных (Mitchell et al., 2014). Объяснимость решений остаётся проблемой, поскольку оператору SOC важно понимать основания для квалификации активности как угрозы (Najafi et al., 2020). Наконец, даже высокоточные модели генерируют заметное число ложноположительных алертов при работе с реальным трафиком в условиях дисбаланса классов (Aktar et al., 2024). Отдельно стоит отметить работу (Moustafa et al., 2019), в которой исследованы механизмы выявления аномалий в распределённой среде с использованием статистических методов, что подтверждает актуальность данного направления.

Недостаточно решённые вопросы

Проведённый анализ позволяет зафиксировать несколько пробелов. Отсутствует достаточно гибкая архитектура IDPS, адаптированная именно для периферийного уровня IoT-инфраструктуры и допускающая модульную замену компонентов без перестройки всей системы. Недостаточно проработана интеграция ML-мониторинга с механизмами защиты периферийных узлов, включая вопрос о размещении моделей в конвейере обработки событий. Существующие решения, как правило, ограничиваются обнаружением, не обеспечивая структурирование и ранжирование событий перед передачей оператору (Bhatt et al., 2014; Najafi et al., 2021). Таким образом, требуется система, способная не только обнаруживать, но и структурировать, приоритизировать и адаптивно обрабатывать события безопасности на периферии IoT-среды.

Постановка задачи

Объектом исследования являются процессы мониторинга и защиты периферийных IoT-устройств в инфраструктуре умного города. Предметом исследования выступают методы построения гибкой IDPS на основе алгоритмов машинного обу-

чения.

Архитектурное описание среды мониторинга опирается на иерархическое представление инфраструктуры, близкое к модели Purdue (Williams, 1994), что позволяет разграничить периферийный, локальный и централизованный уровни защиты. Нижние уровни (сенсоры, актуаторы, полевые устройства) характеризуются минимальными ресурсами и требуют лёгких механизмов предварительного анализа. Средний уровень (edge-шлюзы, агрегаторы) позволяет размещать нормализацию, дедупликацию и локальный ML-анализ. Верхний уровень (SOC, централизованная корреляция) обеспечивает глобальное видение и управление инцидентами (Bhatt et al., 2014; Kotenko et al., 2012). Данные и алерты поднимаются от нижнего уровня к верхнему с последовательным обогащением контекстом, что соответствует логике иерархической эшелонированной защиты (Knapp et al., 2015).

Требования к системе формулируются следующим образом: работа в распределённой среде с поддержкой периферийных устройств; уменьшение избыточных алертов через дедупликацию; снижение ложных срабатываний с помощью ML-анализа; адаптация к изменяющимся условиям; обеспечение обратной связи с центром мониторинга; совместимость со стандартами обмена данными об угрозах (Iqbal et al., 2018; Sauerwein et al., 2017; ISO/IEC, 2022). Задержка обработки событий (от обнаружения до доступности в SOC) не должна превышать одной секунды (Liu et al., 2020), а пропускная способность должна составлять не менее 5000 событий в секунду (Du et al., 2019).

Предлагаемая архитектура гибкой IDPS

Общая архитектура системы

Предлагаемая архитектура включает девять функциональных компонентов, организованных в три уровня в соответствии с иерархическим представлением инфраструктуры. На рис. 1 представлена общая схема системы, показывающая направление потоков данных и обратной связи.

На первом этапе edge IDPS (Suricata или Zeek) генерирует необработанные алерты на основе сигнатурных правил и, при наличии ресурсов, лёгких поведенческих моделей (Paxson, 1998; Suricata User Guide). Далее алерты проходят предварительную фильтрацию, отсекающую заведомо нерелевантные события по заранее определённым критериям. Нормализация приводит разнородные форматы к единому JSON-представлению, совместимому со STIX 2.1 (Iqbal et al., 2018; Yasaei et al., 2020). Модуль дедупликации устраняет повторяющиеся алерты, порождённые одним и тем же инцидентом, но зарегистрированные на нескольких сенсорах. После этого события поступают в ML-модуль для дополнительного анализа и в корреляционный движок, который сопоставляет разрозненные сигналы и формирует оценку риска. На финальном этапе приоритизированные алерты передаются в SOC для визуализации и реагирования (Bhatt et al., 2014; Aktar et al., 2024).

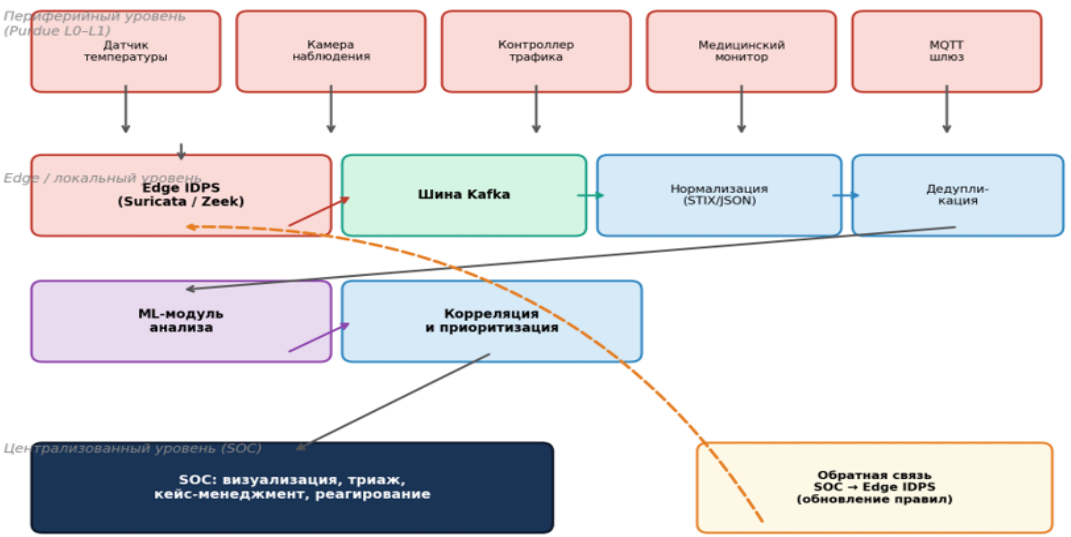


Рис. 1. Общая архитектура гибкой IDPS: от периферийных IoT-устройств через edge-уровень к централизованному SOC с обратной связью

Таблица 1 – Функциональные компоненты архитектуры гибкой IDPS

Компонент	Уровень	Назначение
Периферийные IoT-устройства	Нижний (Purdue L0-L1)	Источники телеметрии и событий
Edge IDPS (Suricata/Zeek)	Периферийный	Сигнатурное и поведенческое обнаружение
Модуль сбора событий	Периферийный	Агрегация событий от нескольких сенсоров
Шина сообщений (Kafka)	Транспортный	Потоковая доставка с гарантированной персистентностью
Модуль нормализации	Edge/локальный	Преобразование алертов в STIX/JSON формат
Модуль дедупликации	Локальный	Устранение дублирующих и избыточных алертов
ML-модуль анализа	Локальный	Детекция аномалий, классификация, снижение FP
Модуль корреляции и приоритизации	Локальный/SOC	Скоринг, ранжирование, передача в SOC
Интерфейс SOC + обратная связь	Централизованный	Визуализация, триаж, обновление правил IDPS

Транспортный уровень реализован на базе Apache Kafka (Apache Kafka Documentation), выбранной за высокую пропускную способность и возможность горизонтального масштабирования. Нормализация выполняется микросервисом на Python, преобразующим алерты от различных IDPS-платформ в единый формат STIX 2.1 (Iqbal et al., 2018). Спецификация API событий описана в формате OpenAPI 3.1 (OpenAPI Specification), что обеспечивает машинночитаемые контракты для валидации.

Логика обработки событий

Обработка событий в системе следует конвейерной логике, представленной на рис. 2. Каждое событие проходит последовательность этапов, от генерации на пе-

риферийном сенсоре до появления в интерфейсе SOC в виде приоритизированного алерта.



Рис. 2. Конвейер обработки событий: сбор → фильтрация → нормализация → дедупликация → ML-анализ → корреляция → скоринг → триаж

Гибкость системы

Термин «гибкая» в названии архитектуры обусловлен несколькими конструктивными особенностями. Во-первых, модульность: каждый компонент конвейера реализован как независимый микросервис, развёрнутый в Docker-контейнере (Kubernetes Documentation), что позволяет заменять, масштабировать или обновлять отдельные модули без остановки всей системы. Во-вторых, адаптация под разные типы IoT-узлов: конфигурация edge IDPS параметризована по типу устройства, протоколу и ожидаемому профилю трафика (Suricata User Guide). В-третьих, возможность замены ML-модели: аналитический модуль принимает стандартизированные входные данные и может работать с различными алгоритмами без модификации остальных компонентов. В-четвёртых, настраиваемость правил обработки и приоритизации: пороги скоринга, критерии дедупликации и политики корреляции задаются через конфигурационные файлы. Наконец, архитектура предусматривает путь расширения до SOAR (Security Orchestration, Automation and Response), что позволит в дальнейшем автоматизировать не только обнаружение, но и реагирование (Wardana et al., 2024; Shabad et al., 2021).

Использование алгоритмов машинного обучения

Роль ML в системе

ML-модуль занимает определённое место в общем конвейере обработки: он размещается после нормализации и дедупликации, но перед корреляционным движком. Его роль состоит в дополнительном анализе нормализованных событий с целью повышения точности обнаружения и снижения числа ложных срабатываний. В отличие от подходов, где ML-модель заменяет весь процесс обнаружения, в предлагаемой архитектуре машинное обучение используется как один из аналитических инструментов внутри модульного конвейера.

Конкретные задачи ML-модуля включают анализ сетевого трафика для выявления отклонений от нормального профиля устройства, классификацию событий по

степени вероятности вредоносности и снижение доли ложноположительных срабатываний путём кросс-валидации с алертами от других сенсоров (Zarpeão et al., 2017; Moustafa et al., 2019). Результаты работы модуля используются корреляционным движком при формировании итоговой оценки риска.

Используемые признаки и типы данных

На вход ML-модуля поступают нормализованные события в формате STIX JSON, из которых извлекаются четыре группы признаков. Сетевые характеристики включают IP-адреса источника и назначения, порты, протокол, размер пакетов и флаги. Временные признаки отражают межпакетные интервалы, длительность потока и частоту событий в скользящем окне. Поведенческие признаки описывают отклонение текущей активности от ранее наблюдаемого профиля для данного типа устройства (Yasaei et al., 2020). Агрегированные события обобщают показатели по группе устройств в пределах одного сетевого сегмента.

Логика принятия решений

ML-модуль формирует для каждого события вероятностную оценку вредоносности. Пусть x обозначает вектор признаков нормализованного события, а $f(x)$ — выход ML-модели, интерпретируемый как вероятность того, что событие связано с вредоносной активностью. Тогда оценка аномальности события определяется как:

$$A(x) = f(x) \cdot w_{dev(x)} \quad (1)$$

где $w_{dev(x)}$ представляет собой весовой коэффициент, отражающий степень отклонения вектора признаков от базового профиля устройства. Чем сильнее отклонение от усреднённого поведения, тем больший вес получает событие.

Далее оценка аномальности интегрируется в общую формулу риска, учитывающую контекстуальные факторы:

$$R(x) = A(x) \cdot C_{asset} \cdot \alpha(t) \cdot \beta(conn) \quad (2)$$

где C_{asset} обозначает критичность актива (определяемую на основе его роли в инфраструктуре (Hnatiienko et al., 2024)), $\alpha(t)$ отражает длительность аномального поведения (чем дольше сохраняется аномалия, тем выше вклад временного фактора), а $\beta(conn)$ учитывает сетевую связность устройства (высоко связанные узлы представляют бóльший риск распространения угрозы).

Пороговая логика используется для преобразования непрерывной оценки риска в категориальное решение о приоритете. Определяются три уровня:

$$P(x) = \left\{ \begin{array}{l} \text{низкий, если } R(x) < \theta_{low}; \\ \text{средний, если } \theta_{low} \leq R(x) < \theta_{high}; \\ \text{высокий, если } R(x) \geq \theta_{high} \end{array} \right\} \quad (3)$$

где пороги θ_{low} и θ_{high} настраиваются в процессе калибровки на валидационном наборе данных. Важно отметить, что в текущей реализации ML-модуль не претендует на полную замену экспертного анализа. Его задача состоит в предварительном ранжировании событий, что позволяет оператору SOC сосредоточиться на наиболее вероятных угрозах (Bhatt et al., 2014; Najafi et al., 2021).

Экспериментальная оценка

Условия эксперимента

Экспериментальная оценка проводилась на двух публичных датасетах, содержащих реалистичный IoT-трафик с размеченными атаками. BoT-IoT и TON_IoT были выбраны как представительные наборы, включающие DDoS, разведку и атаки на уровне протоколов MQTT и CoAP (Moustafa et al., 2019). Характеристики датасетов представлены в таблице 2.

Таблица 2 – Характеристики экспериментальных датасетов

Параметр	BoT-IoT	TON_IoT
Типы атак	DDoS, DoS, разведка, кража данных	DDoS, ransomware, backdoor, injection, XSS
Протоколы	MQTT, HTTP, TCP/UDP	MQTT, CoAP, HTTP, DNS
Число записей	~73 млн (подвыборка)	~460 тыс.
Метки классов	Бинарные + мультиклассовые	Бинарные + мультиклассовые

Прототип развёрнут на базе Suricata 7.0 и Zeek 6.0 в качестве edge IDPS, Apache Kafka 3.6 как шины сообщений, Python 3.11 для нормализации и корреляции, а также Elasticsearch 8.11 для интеграции с SOC (Paxson, 1998; Apache Kafka Documentation; Suricata User Guide). Развёртывание выполнено в Docker-контейнерах (Kubernetes Documentation). Для сравнения использовались два базовых подхода: (а) автономная работа IDPS без централизованной корреляции и (б) наивная пересылка алертов в SOC без нормализации и дедупликации.

Критерии оценки

Оценка производилась по следующим метрикам: задержка корреляции (время от генерации алерта до его доступности в SOC), доля ложных срабатываний (FP rate), объём алертов (число событий, поступающих аналитику после обработки), надёжность доставки сообщений и пропускная способность системы. Дополнительно оценивалась точность нормализации путём ручной проверки случайной выборки из 500 алертов по каждому датасету.

Полученные результаты

Результаты экспериментальной оценки представлены в таблице 3 и на рис. 3. Средняя задержка корреляции составила 687 мс ($\sigma = 143$ мс), с 95-м перцентилем 921 мс и 99-м перцентилем 1247 мс. По сравнению с наивной пересылкой, основанной на

файловом обмене (типичная задержка 1,5–2,8 с) (Najafi et al., 2020), предлагаемая архитектура снизила задержку примерно на 62%.

Таблица 3 – Результаты оценки производительности

Метрика	Только IDPS	Наивная пересылка	Предлагаемый подход
Задержка корреляции	Нет корреляции	~1,8 с	~0,69 с
FP rate (Suricata)	30,1%	30,1%	21,4% (–29%)
FP rate (Zeek)	41,2%	41,2%	28,6% (–31%)
Объём алертов	100%	100%	~60% (–40%)
Надёжность доставки	Н/Д	~95%	99,97%
Пропускная способ- ность	Н/Д	~2000 соб./с	>8200 соб./с
Точность нормализации	Н/Д	Н/Д	96,8%

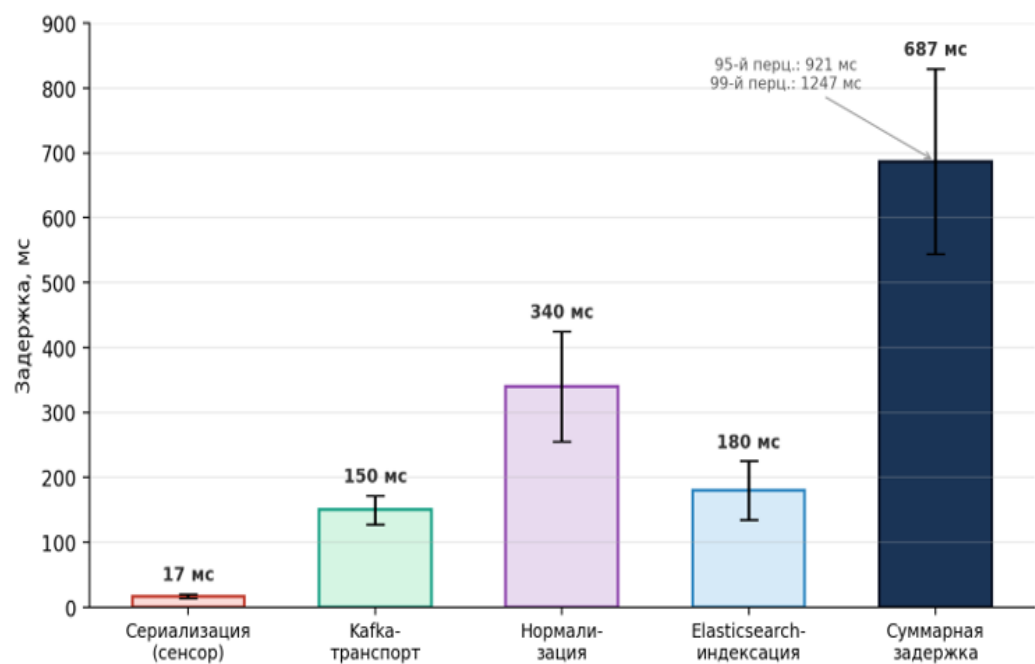


Рис. 3. Распределение задержки по этапам конвейера для 10 000 алертов (нормализация, Kafka-транспорт, Elasticsearch-индексация)

Ложные срабатывания снизились на 29% для Suricata и на 31% для Zeek благодаря корреляции алертов между сенсорами: изолированные алерты, не подтверждённые временной или межсенсорной корробрацией, подавлялись (Almeida, 2023; Zarpelão et al., 2017). Объём алертов, поступающих аналитику, сократился примерно на 40% за счёт дедупликации и подавления шума. Точность нормализации составила 96,8%, что превышает установленный порог в 95%. Ошибки нормализации (3,2%) были связаны с некорректными временными метками и пустыми обязательными полями (Yasaei et al., 2020).

Декомпозиция задержки показала, что основной вклад вносит нормализа-

ция (~340 мс), за ней следуют Elasticsearch-индексация (~180 мс) и Kafka-транспорт (~150 мс). Сериализация на стороне сенсора занимает примерно 17 мс. Пропускная способность оставалась стабильной до 8200 событий в секунду при одном экземпляре нормализатора; при горизонтальном масштабировании до трёх экземпляров система обрабатывала до 18 500 событий в секунду (Apache Kafka Documentation).

Двунаправленный механизм обратной связи обеспечил распространение обновлённых правил обнаружения от SOC ко всем edge-сенсорам в среднем за 2,3 секунды (Suricata User Guide), что позволяет адаптировать конфигурацию IDPS без необходимости ручной перенастройки каждого узла.

Результаты и обсуждение.

Полученные результаты позволяют утверждать, что архитектура на основе потоковой шины сообщений эффективно решает проблему интеграции разнородных IDPS-сенсоров в распределённой IoT-среде. В отличие от статических схем с файловой пересылкой алертов (Najafi et al., 2020), потоковая архитектура на базе Kafka устраняет задержки поллинга и обеспечивает непрерывную доставку событий. Снижение ложных срабатываний на 29–31% через кросс-сенсорную корреляцию непосредственно повышает эффективность работы аналитиков и снижает нагрузку на SOC (Almeida, 2023; Aktar et al., 2024).

Архитектура разработана с учётом принципов ISO/IEC 27001 (ISO, 2022) и GDPR (GDPR, 2016) в части шифрования каналов (TLS 1.3), аутентификации событий (HMAC-SHA256) и настраиваемых политик хранения телеметрии. Нормализация в формат STIX 2.1 (Iqbal et al., 2018) обеспечивает вендор-нейтральность, что принципиально важно для муниципальных инфраструктур, где оборудование закупается у различных поставщиков (Aktar et al., 2024).

Предложенный подход особенно релевантен для периферийных IoT-устройств, поскольку он позволяет размещать часть аналитических функций непосредственно на edge-уровне, снижая зависимость от централизованного канала связи. Иерархическая структура, согласующаяся с моделью Purdue (Williams, 1994), делает архитектуру понятной для специалистов промышленной автоматизации и облегчает её позиционирование в рамках существующих фреймворков безопасности (Knapp et al., 2015).

Вместе с тем необходимо указать на ограничения. Загрузка CPU edge-сенсоров достигала 85% при пиковых нагрузках (Paxson, 1998), что оставляет мало резерва для дополнительных аналитических задач. Нормализация является основным узким местом по задержке (~340 мс), и её оптимизация через компилируемые парсеры представляет практический интерес (Yasaei et al., 2020). Зависимость от качества входных данных остаётся критичной: при некорректных метках или пропущенных полях качество ML-анализа снижается. Необходимость периодического дообучения моделей для противодействия concept drift (Mitchell et al., 2014) требует операционных ресурсов. Наконец, проверка проведена на бенчмарк-датасетах, и подтверждение работоспособности в реальных условиях масштабного развёртывания остаётся задачей будущих исследований.

Перспективы развития

Архитектура предусматривает несколько направлений расширения. Первое из них связано с полной SOAR-автоматизацией, позволяющей перейти от ручного триажа к автоматизированным сценариям реагирования, включая изоляцию скомпрометированных устройств и перенастройку сетевых политик (Wardana et al., 2024; Shabad et al., 2021). Второе направление касается внедрения online learning, то есть механизмов адаптивного обучения, корректирующих ML-модели на основе обратной связи от аналитиков SOC без полного переобучения на исторических данных. Третье направление предполагает мультиклассовую классификацию инцидентов, что позволит различать типы атак (DDoS, разведка, эксплуатация уязвимостей) и применять дифференцированные стратегии реагирования. Наконец, ключевым практическим шагом является пилотное развёртывание в реальной инфраструктуре умного города Казахстана, что позволит проверить работоспособность подхода при масштабах и условиях, не воспроизводимых в лабораторных экспериментах.

Заключение.

В статье предложена архитектура гибкой IDPS на основе алгоритмов машинного обучения для мониторинга и защиты периферийных IoT-устройств. В отличие от традиционных изолированных схем, предложенный подход обеспечивает модульную обработку событий через конвейер нормализации, дедупликации, ML-анализа, корреляции и приоритизации. Архитектурное описание среды опирается на иерархическое представление, согласующееся с моделью Purdue, что позволяет чётко разграничить периферийный, локальный и централизованный уровни защиты.

Экспериментальная оценка на датасетах BoT-IoT и TON_IoT показала сокращение задержки корреляции событий примерно на 62% по сравнению с базовыми подходами, снижение доли ложных срабатываний на 29–31% и уменьшение объёма алертов, поступающих аналитику, на 40%. Точность нормализации составила 96,8%, пропускная способность превысила 8200 событий в секунду, а механизм обратной связи обеспечил обновление правил обнаружения на всех edge-сенсорах за 2,3 секунды.

Полученные результаты подтверждают перспективность использования предложенной архитектуры при построении систем мониторинга IoT-инфраструктуры умных городов. Модульность, адаптивность и вендор-нейтральность системы создают основу для дальнейшего расширения средствами SOAR, online learning и мультиклассовой классификации. Планируется пилотное развёртывание в рамках инфраструктуры умного города Казахстана.

REFERENCES

- Almeida F.A. (2023). Prospects of cybersecurity in smart cities // *Future Internet*. — Vol. 15. — No. 9. Art. 285.
- Aktar M.N. et al. (2024). Enhancing false positive alert detection in SIEM using RNN // *Proc. 27th ICCIT*. Pp. 1–6.
- Apache Kafka Documentation. Version 3.6 // URL: <https://kafka.apache.org/documentation/>
- Babenko T., Kolesnikova K. et al. (2026). Hybrid GNN-LSTM architecture for probabilistic IoT botnet detection // *Computers*. — Vol. 15. — No. 1. Art. 26.
- Bhatt S., Manadhata P.K., Zomlot L. (2014). The operational role of security information and event management

systems // IEEE Secur. Priv. — Vol. 12. — No. 5. Pp. 35–41.

Du R., Santi P., Xiao M. et al. (2019). The sensible city: A survey on the deployment and management for smart city monitoring // IEEE Commun. Surv. Tutor. — Vol. 21. — No. 2. Pp. 1533–1560.

Elvas L., Mataloto B., Martins A., Ferreira J.C. (2021). Disaster management in smart cities // Smart Cities. — Vol. 4. — No. 2. Pp. 819–839.

Gerhards R. (2009). The syslog protocol // RFC 5424, IETF.

General Data Protection Regulation (GDPR). (2016). Regulation (EU) 2016/679 // Official J. EU. L 119. Pp. 1–88.

Hnatiienko H., Hnatiienko V., Zulunov R., Babenko T. et al. (2024). Method for determining the level of criticality elements // CEUR Workshop Proc.

Hernández-Ramos S. et al. (2018). MQTT security: A novel fuzzing approach // Wirel. Commun. Mob. Comput. Art. 8261746.

Jo J., Sharma P., Sicato J.C.S., Park J.H. (2019). Emerging technologies for sustainable smart city network security // J. Inf. Process. Syst. — Vol. 15. — No. 4. Pp. 765–784.

Iqbal Z., Anwar Z., Mumtaz R. (2018). STIXGEN: A novel framework for automatic generation of structured cyber threat information // Proc. FIT. Pp. 271–276.

ISO/IEC 27001 (2022). Information security management systems. Geneva: ISO.

Kubernetes Documentation // URL: <https://kubernetes.io/docs/>

Knap E.D., Langill J.T. (2015). Industrial Network Security. 2nd ed. Waltham: Syngress.

Kotenko I., Chechulin A., Novikova E. (2012). Attack modelling and security evaluation for SIEM // Proc. SECRIPT. Rome. Pp. 391–394.

Liu Y., Ma M., Liu X. et al. (2020). Design and analysis of probing route to defense sink-hole attacks for IoT security // IEEE Trans. Netw. Sci. Eng. — Vol. 7. — No. 1. Pp. 356–372.

La V.H., Montes de Oca E., Mallouli W., Cavalli A. (2021). A framework for security monitoring of real IoT testbeds // Proc. ICSoft. Pp. 1–12.

Moustafa N., Choo K.-K.R., Radwan I., Camtepe S. (2019). Outlier Dirichlet mixture mechanism: Adversarial statistical learning for anomaly detection in the fog // IEEE Trans. Inf. Forensics Secur. — Vol. 14. — No. 8. Pp. 1975–1987.

Mitchell R., Chen I.-R. (2014). A survey of intrusion detection techniques for cyber-physical systems // ACM Comput. Surv. — Vol. 46. — No. 4. Art. 55.

Najafi P., Cheng F., Meinel C. (2021). SIEMA: Bringing advanced analytics to legacy SIEM // SecureComm 2020. LNCS. 2021. — Vol. 357. — Pp. 21–39.

OpenAPI Specification v3.1.0 // URL: <https://spec.openapis.org/oas/v3.1.0>

Paxson V. (1998). Bro: A system for detecting network intruders in real-time // Proc. 7th USENIX Secur. Symp.

Palko D., Babenko T. et al. (2023). Cyber security risk modeling in distributed information systems // Appl. Sci. — Vol. 13. — No. 4. Art. 2393.

Shi W., Cao J., Zhang Q. et al. (2016). Edge computing: Vision and challenges // IEEE Internet Things J. — Vol. 3. — No. 5. Pp. 637–646.

Sisinni E., Saifullah A., Han S. et al. (2018). Industrial Internet of Things: Challenges, opportunities, and directions // IEEE Trans. Ind. Informat. — Vol. 14. — No. 11. Pp. 4724–4734.

Suricata User Guide. Version 7.0 // URL: <https://docs.suricata.io/en/latest/>

Shabad P.K.R., Alrashide A., Mohammed O. (2021). Anomaly detection in smart grids using ML // Proc. IECON. Pp. 1–6.

Sauerwein C. et al. (2017). Threat intelligence sharing platforms // Proc. 13th WI. Pp. 837–851.

Walling S., Lodh S. (2025). An extensive review of ML and DL techniques on network intrusion detection for IoT // Trans. Emerg. Telecommun. Technol. DOI: 10.1002/ett.70064.

Wardana A.A., Sukarno P. (2024). Taxonomy and survey of collaborative IDS using federated learning // ACM Comput. Surv. — Vol. 56. — No. 7. Pp. 1–37.

Yasaei R., Hernandez F., Faruque M.A. (2020). IoT-CAD: Context-aware adaptive anomaly detection in IoT // Proc. ICCAD. Pp. 1–9.

Williams T.J. (1994). The Purdue enterprise reference architecture // Comput. Ind. — Vol. 24. — No. 2–3. Pp. 141–158.

Zarpelão B.B., Miani R.S., Kawakani C.T. et al. (2017). A survey of intrusion detection in IoT // J. Netw. Comput. Appl. — Vol. 84. — Pp. 25–37.

**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 30.06.2026.

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