

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. 1 (25). 2026
January–March

**ХАЛЫҚАРАЛЫҚ АҚПАРАТТЫҚ ЖӘНЕ КОММУНИКАЦИЯЛЫҚ
ТЕХНОЛОГИЯЛАР ЖУРНАЛЫ**

2020 жылдан бері шығарылады
Том 7. 1 (25). 2026
Қаңтар-Наурыз

**МЕЖДУНАРОДНЫЙ ЖУРНАЛ ИНФОРМАЦИОННЫХ И
КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ**

Издается с 2020 г.
Том 7. 1 (25). 2026
Январь-Март

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)

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

Bakhtgerci 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)
Луччо 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)
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 Токсулжаевич — 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 Абдуллаевна — 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)
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)
Дамелия Максустовна Ескендрова — 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)
Талеуш 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 сулет 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 Токсужаевич — 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)

Дамелия Максугуона Ескендрова — 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)

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

Алимурабаев 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)

Белошницкая 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 социально-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.B. Zhalgas, Y.N. Kalpakov, B.Ye. Amirgaliyev
MACHINE LEARNING-DRIVEN OPTIMIZATION OF LOGISTICS IN SMART CITIES: A CASE STUDY OF ASTANA9

L. Kurmangaziyeva, Sh. Kodanova, M. Urazgaliyeva, O. Findik, S. Iskakova
INTEGRATING FUZZY LOGIC AND ARTIFICIAL INTELLIGENCE IN OPTIMIZING BUSINESS PROCESS AUTOMATION DECISIONS24

Y. Mailybayev, U. Adilbayeva, R. Amanova
ORGANIZATION OF AN ONLINE SURVEY OF PARTICIPANTS IN THE EDUCATIONAL PROCESS AND ANALYSIS OF THE RESULTS BASED ON THE MODIFIED DELPHI METHOD46

V.A. Takizhanov, A.Z. Ibragimov, A. Shalakhmetov
SIMULATION-BASED ROBUSTNESS ASSESSMENT OF ASTANA'S BUS NETWORK UNDER RANDOM AND TARGETED FAILURES61

INFORMATION TECHNOLOGY

M. Zh. Aitimov, G. K. Muratova, Zh. K. Bissenbayeva, I.M. Bapiyev, M. Kassim
SEMANTIC COMPLETENESS IN KAZAKH-LANGUAGE EXTRACTIVE QA THROUGH ONTOLOGY AND RETRIEVAL MECHANISMS76

O.N. Akylbekov, Y.T. Dauletbek, A.N. Moldagulova, G.S. Zakariya, D.A. Gura
MACHINE LEARNING METHODS FOR ANALYSING THREE-DIMENSIONAL SPATIAL DATA IN KAZAKHSTAN'S LAND USE PLANNING.....89

S.Zh. Aliaskarov, R.K. Uskenbayeva, A. Razaque, A.B. Kassymova, A.M. Anartayeva
TOWARDS EFFICIENT BIG DATA ANALYTICS IN REGIONAL SYSTEMS: PRACTICAL INSIGHTS FROM HYBRID ARCHITECTURE DEPLOYMENT.....109

A. Ismailova, G. Yessenbayeva, K. Kadyrkulov, R. Moldasheva, A. Amangeldi
DEVELOPMENT OF A HYBRID DEEP LEARNING MODEL FOR MULTICLASS CLASSIFICATION OF MICROSCOPIC IMAGES OF BACTERIA128

G. Kalman, J. Kultan, A.N. Ismukamova, N.M. Ausilova, Y.V. Makhatova
A DOMAIN-KNOWLEDGE-BASED MODEL FOR REFERENCE RESOLUTION IN LOW-RESOURCE LANGUAGES141

Y. Kamen, Zh. Yessendauletova, L. Fazylova, M. Rakhimzhanova, A.M. Nedzved
USING NEURAL NETWORKS FOR OBJECTIVE ASSESSMENT OF ATTENTION IN CHILDREN BASED ON EEG DATA158

A.Ye. Kulakayeva, Ye.A. Bakhtiyarova, G.T. Jakanova, Sh. Nursultan
COMPARATIVE ANALYSIS OF VARIOUS RADIO WAVE PROPAGATION MODELS FOR MOBILE NETWORK COVERAGE PREDICTION173

M.B. Nurpeissova, Sh.K. Aitkazinova, A.M. Abenov, N.S. Donenbayeva
METHODOLOGY FOR TRANSFORMING SATELLITE COORDINATES INTO A TOPOCENTRIC RECTANGULAR COORDINATE SYSTEM189

A. Ospanov, P. Alonso-Jordá, A. Zhumadillayeva
BLOCKCHAIN-ENABLED ERP WAREHOUSE INTEGRATION WITH IOT DIMENSIONERS AND MACHINE LEARNING-OPTIMIZED DIMENSIONAL WEIGHT RECONCILIATION202

A.A. Sakhipov, R.B. Seitbek
EVENT-DRIVEN MICROSERVICES FOR INCIDENT DETECTION AND RESPONSE IN INTELLIGENT TRAFFIC SYSTEM218

G. Yusupova, K.S. Shadinova, D. Ussipbekova, Zh.Zh. Azhibekova, P. Schmidt
DETERMINATION OF SOIL PROFILE STRATIFICATION AT 0–200 CM DEPTH USING A MULTILEVEL STACKING MODEL231

INFORMATION SECURITY AND COMMUNICATION TECHNOLOGIES

S.A. Adilzhanova, M.Zh. Sakypbekova, L.Sh. Cherikbaeva, G.A. Tyulepberdinova, G.T. Zhubanysheva SYSTEMATIC ANALYSIS OF RISK ASSESSMENT METHODS AND MODELS IN INFORMATION SECURITY.....	244
T. K. Zhukabayeva, D.B. Baumuratova, E. Benkhelifa, N.A. Niyetbayeva EDGE COMPUTING-BASED TECHNIQUE FOR CONSTRUCTION OF ATTACK DETECTION MEANS IN CYBER-PHYSICAL SYSTEMS OF INDUSTRIAL INTERNET-OF-THINGS	270
N.E. Karabayev, S.K. Serikbayeva, Y.M. Mardenov, B. Tassuov, M. Fajkus DETECTION OF CYBER ATTACKS IN TRANSPORT NETWORKS BASED ON MACHINE LEARNING METHODS	292
V.A. Kumalakov, A.O. Dargulova A HYBRID FRAMEWORK FOR RESUME-JOB MATCHING SYSTEM	311
V. Makhatova, B. Dzhugembayeva, A. Gabdulova, L. Nurgaliyeva, A. Abdigaliyeva MATHEMATICAL MODEL FOR OPTIMAL SENSOR SELECTION IN SIEM SYSTEMS USING THE ANALYTIC HIERARCHY PROCESS	326

МАЗМҰНЫ

ӘЛЕУМЕТТІК-ЭКОНОМИКАЛЫҚ ЖҮЙЕЛЕРДІ ДАМУДАҒЫ ЦИФРЛЫҚ ТЕХНОЛОГИЯЛАР

А.Б. Жалғас, Е.Н. Калпаков, Б.Е. Амиргалиев АҚЫЛДЫ ҚАЛАЛАРДАҒЫ ЛОГИСТИКАНЫ МАШИНАЛЫҚ ОҚЫТУҒА НЕГІЗДЕЛГЕН ОҢТАЙЛАНДЫРУ: АСТАНАНЫҢ ЖАҒДАЙЫН ЗЕРТТЕУ.....	9
Л.Курманғазиева, Ш. Қоданова, М. Уразғалиева, О. Findik, С. Искакова ЖАСАНДЫ ИНТЕЛЛЕКТ ПЕН АЙҚЫН ЕМЕС ЛОГИКАНЫ БІРІКТІРУ АРҚЫЛЫ БИЗНЕС-ПРОЦЕСТЕРДІ АВТОМАТТАНДЫРУ ШЕШІМДЕРІН ОҢТАЙЛАНДЫРУ	24
Е. Майлыбаев, У. Адилбаева, Р. Аманова ҰЙЫМДАСТЫРЫЛҒАН ОНЛАЙН САУАЛНАМА АРҚЫЛЫ БІЛІМ БЕРУ ПРОЦЕСІНЕ ҚАТЫСУШЫЛАРДЫҢ ПІКІРЛЕРІН ЖИНАУ ЖӘНЕ НӘТИЖЕЛЕРІН МОДИФИКАЦИЯЛАНҒАН ДЕЛЬФИ ӘДІСІ НЕГІЗІНДЕ ТАЛДАУ	46
В.А. Такижанов, А.Ж. Ибрагимов, А. Шалахметов МОДЕЛЬДЕУ НЕГІЗІНДЕ АСТАНАНЫҢ АВТОБУС ЖЕЛІСІНІҢ ТҮРАҚТЫЛЫҒЫН БАҒАЛАУ: КЕЗДЕЙСОҚ ЖӘНЕ МАҚСАТТЫ ІСТЕН ШЫҒУЛАР ЖАҒДАЙЫНДА	61

АҚПАРАТТЫҚ ТЕХНОЛОГИЯЛАР

М.Ж. Айтимов, Г.К. Муратова, Ж.К. Бисенбаева, И.М. Бапиев, М. Кассим ОНТОЛОГИЯ ЖӘНЕ ІЗДЕУ МЕХАНИЗМДЕРІ АРҚЫЛЫ ҚАЗАҚ ТІЛІНДЕГІ ЭКСТРАКЦИЯЛЫҚ ҚАДАҒЫ СЕМАНТИКАЛЫҚ ТОЛЫҚТЫҚ	76
О.Н. Ақылбеков, Е.Т. Даулетбек, А.Н. Молдагулова, Г.С. Закария, Д.А. Гура ҚАЗАҚСТАННЫҢ АУМАҚТЫҚ ЖОСПАРЛАУЫНДАҒЫ ҮШ ӨЛШЕМДІ КЕҢІСТІКТІК МӨЛІМЕТТЕРДІ ТАЛДАУ ҮШІН МАШИНАЛЫҚ ОҚЫТУ ӘДІСТЕРІ	89
С.Ж. Алиасқаров, Р.К. Ускенбаева, А. Разак, А.Б. Қасымов, А.М. Анартаева АЙМАҚТЫҚ ЖҮЙЕЛЕРДЕГІ ҮЛКЕН ДЕРЕКТЕРДІ ТИІМДІ ТАЛДАУҒА ҚАРАЙ: ГИБРИДТІ АРХИТЕКТУРАНЫ ЕНГІЗУДІҢ ПРАКТИКАЛЫҚ ТҮСІНІКТЕР.....	109
А.А. Исмаилова, Г.Р. Есенбаева, Қ.К. Кадиркулов, Р.Н. Молдашева, А. Амангелді РОСКОПИЯЛЫҚ БЕЙНЕЛЕРІН КӨПКЛАССТЫ ЖІКТЕУГЕ АРНАЛҒАН ГИБРИДТІ ТЕРЕҢ ОҚЫТУ МОДЕЛІН ӘЗІРЛЕУ	128
Г. Қалман, К. Ярослав, А.Н. Исмуқанова, Н.М. Аусилова, В.Е. Махатова ПӨНДІК САЛА БІЛІМ НЕГІЗІНДЕ РЕУСРСТАРЫ АЗ ТІЛДЕРДЕГІ РЕФЕРЕНЦИЯНЫ ШЕШУДІҢ МОДЕЛІ.....	141
Е.Г. Кәмен, Ж.Т. Есендаулетова, Л.С. Фазылова, М.Б. Рахимжанова, А.М. Недзьведь ЭЭГ ДЕРЕКТЕРІ БОЙЫНША БАЛАЛАРДЫҢ ЗЕЙІНІН ОБЪЕКТИВТІ БАҒАЛАУ ҮШІН НЕЙРОНДЫҚ ЖЕЛІЛЕРДІ ҚОЛДАНУ	158
А.Е. Кулакаева, Е.А. Бахтиярова, Г.Т. Джаканова, Ш. Нурсултан ҰЯЛЫ БАЙЛАНЫС ЖЕЛІЛЕРІНІҢ ҚАМТУ АЙМАҒЫН БОЛЖАУҒА АРНАЛҒАН ӨРТҮРЛІ РАДИОТОЛҚЫН ТАРАЛУ МОДЕЛЬДЕРІНІҢ САЛЫСТЫРМАЛЫ ТАЛДАУЫ	173

М.Б. Нұрпейісова, Ш.Қ. Айтқазынова, А.М. Абенов, Н.С. Дөненбаева
СПУТНИКТИК КООРДИНАТТАРДЫ ТОПОЦЕНТРЛІК ТІК БҰРЫШТЫ КООРДИНАТТАР ЖҮЙЕСІНЕ ТҮРЛЕНДІРУДІҢ ӘДІСТЕМЕСІ189

А. Оспанов, П. Алонсо-Хорда, А. Жұмаділлаева
БЛОКЧЕЙН-ТЕХНОЛОГИЯСЫМЕН ЫҚПАЛДАС ERP ҚОЙМА ЖҮЙЕСІН ІОТ ДИМЕНСИОНЕРЛЕР ЖӘНЕ МАШИНАЛЫҚ ОҚЫТУ АРҚЫЛЫ ОПТИМИЗАЦИЯЛАНҒАН ӨЛШЕМДІ САЛМАҚ ЕСЕПТЕУМЕН ИНТЕГРАЦИЯЛАУ202

А.А. Сахипов, Р.Б. Сейітбек
ОҚИҒАҒА БАҒДАРЛАНҒАН МИКРОҚЫЗМЕТТЕР ЖҮЙЕСІ АРҚЫЛЫ АҚЫЛДЫ ТРАФИК ЖҮЙЕЛЕРІНДЕ ОҚИҒАЛАРДЫ АНЫҚТАУ ЖӘНЕ ШАРАЛАР ҚОЛДАНУ218

Г.М. Юсупова, К.С. Шадинова, Д.И. Усипбекова, Ж.Ж. Ажибекова, Р. Schmidt
ТОПЫРАҚ ПРОФИЛІНІҢ 0–200 СМ ТЕРЕҢДІКТЕГІ СТРАТИФИКАЦИЯСЫН КӨПДЕҢГЕЙЛІ СТЕКИНГ-МОДЕЛІМЕН АНЫҚТАУ.....231

АҚПАРАТТЫҚ ҚАУІПСІЗДІК ЖӘНЕ КОММУНИКАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАРҒА АРНАЛҒАН

С.А. Адилжанова, М.Ж. Сақыпбекова, Л.Ш. Черикбаева, Г.А. Тюлепбердинова, Г.Т. Жубанышева
АҚПАРАТТЫҚ ҚАУІПСІЗДІКТЕ ТӘУЕКЕЛДЕРДІ БАҒАЛАУ ӘДІСТЕРІ МЕН МОДЕЛЬДЕРІН ЖҮЙЕЛІ ТАЛДАУ.....244

Т.К. Жукабаева, Д. Б. Баумуратова, Е. Бенкхелифа, Н.А. Ниегбаева
ШЕКАРАЛЫҚ ЕСЕПТЕУЛЕРДІ ҚОЛДАНА ОТЫРЫП, ЗАТТАРДЫҢ ӨНЕРКӘСІПТІК ИНТЕРНЕТІНІҢ КИБЕРФИЗИКАЛЫҚ ЖҮЙЕЛЕРІНДЕГІ ШАБУЫЛДАРДЫ АНЫҚТАУ ҚҰРАЛДАРЫН ҚҰРУ ӘДІСТЕМЕСІ.....270

Н.Е. Қарабаев, С.К. Серикбаева, Е.М. Марденов, Б. Тасуов, М. Файкус
МАШИНАЛЫҚ ОҚЫТУ ӘДІСТЕРІНЕ НЕГІЗДЕЛГЕН КӨЛІК ЖЕЛІЛЕРІНДЕГІ КИБЕРШАБУЫЛДАРДЫ АНЫҚТАУ292

Б.А. Кумалаков, А.О. Даргулова
ТҮЙІНДЕМЕЛЕР МЕН ВАКАНСИЯЛАРДЫ АВТОМАТТАНДЫРЫЛҒАН СӘЙКЕСТЕНДІРУГЕ НЕГІЗДЕЛГЕН ГИБРИДТІ ҮМІТКЕРЛЕРДІ ІРІКТЕУ ЖҮЙЕСІ311

В. Махатова, Б. Джугембаева, А. Габдулова, Л. Нурғалиева, А. Абдигалиева
ИЕРАРХИЯЛАРДЫ ТАЛДАУ ӘДІСІ НЕГІЗІНДЕ SIEM ЖҮЙЕЛЕРІНДЕ ОҢТАЙЛЫ СЕНСОРДЫ ТАҢДАУДЫҢ МАТЕМАТИКАЛЫҚ МОДЕЛІ326

СОДЕРЖАНИЕ

ЦИФРОВЫЕ ТЕХНОЛОГИИ В РАЗВИТИИ СОЦИО-ЭКОНОМИЧЕСКИХ СИСТЕМ

А.Б. Жалғас, Е.Н. Калпаков, Б.Е. Амиргалиев
ОПТИМИЗАЦИЯ ЛОГИСТИКИ В УМНЫХ ГОРОДАХ НА ОСНОВЕ МАШИННОГО ОБУЧЕНИЯ: НА ПРИМЕРЕ АСТАНЫ9

Л. Курмангазиева, Ш. Коданова, М. Уразғалиева, О. Финдик, С. Исакова
ИНТЕГРАЦИЯ НЕЧЕТКОЙ ЛОГИКИ И ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ПРИ ОПТИМИЗАЦИИ РЕШЕНИЙ ПО АВТОМАТИЗАЦИИ БИЗНЕС-ПРОЦЕССОВ24

Е. Майлыбаев, У. Адилбаева, Р. Аманова
СБОР МНЕНИЙ УЧАСТНИКОВ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПОСРЕДСТВОМ ОРГАНИЗОВАННОГО ОНЛАЙН-АНКЕТИРОВАНИЯ И АНАЛИЗ РЕЗУЛЬТАТОВ НА ОСНОВЕ МОДИФИЦИРОВАННОГО МЕТОДА ДЕЛЬФИ46

В.А. Такижанов, А.Ж. Ибрагимов, А. Шалахметов
ОЦЕНКА УСТОЙЧИВОСТИ АВТОБУСНОЙ СЕТИ АСТАНЫ НА ОСНОВЕ МОДЕЛИРОВАНИЯ ПРИ СЛУЧАЙНЫХ И ЦЕЛЕНАПРАВЛЕННЫХ ОТКАЗАХ61

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

М.Ж. Айтимов, Г.К. Муратова, Ж.К. Бисенбаева, И.М. Бапиев, М. Кассим
СЕМАНТИЧЕСКАЯ ПОЛНОТА В КАЗАХСКОЯЗЫЧНОМ EXTRACTIVE QA ЧЕРЕЗ ОНТОЛОГИЮ И RETRIEVAL-МЕХАНИЗМЫ76

О.Н. Акылбеков, Е.Т. Даулетбек, А.Н. Молдагулова, Г.С. Закария, Д.А. Гура МЕТОДЫ МАШИННОГО ОБУЧЕНИЯ ДЛЯ АНАЛИЗА ТРЁХМЕРНЫХ ПРОСТРАНСТВЕННЫХ ДАННЫХ В ТЕРРИТОРИАЛЬНОМ ПЛАНИРОВАНИИ КАЗАХСТАНА	89
С.Ж. Алиаскаров, Р.К. Ускенбаева, А. Разак, А.Б. Касымова, А.М. Анартаева НА ПУТИ К ЭФФЕКТИВНОЙ АНАЛИТИКЕ БОЛЬШИХ ДАННЫХ В РЕГИОНАЛЬНЫХ СИСТЕМАХ: ПРАКТИЧЕСКИЕ ВЫВОДЫ ИЗ ВНЕДРЕНИЯ ГИБРИДНОЙ АРХИТЕКТУРЫ	109
А.А. Исмаилова, Г.Р. Есенбаева, К.К. Кадиркулов, Р.Н. Молдашева, А. Амангелды РАЗРАБОТКА ГИБРИДНОЙ МОДЕЛИ ГЛУБОКОГО ОБУЧЕНИЯ ДЛЯ МНОГОКЛАССОВОЙ КЛАССИФИКАЦИИ МИКРОСКОПИЧЕСКИХ ИЗОБРАЖЕНИЙ БАКТЕРИЙ	128
Г. Калман, К. Ярослав, А.Н. Исмуканова, Н.М. Аусилова, В.Е. Махатова МОДЕЛЬ НА ОСНОВЕ ЗНАНИЙ ПРЕДМЕТНОЙ ОБЛАСТИ ДЛЯ РАЗРЕШЕНИЯ КОРЕФЕРЕНЦИИ В МАЛОРЕСУРСНЫХ ЯЗЫКАХ	141
Е.Г. Камен, Ж.Т. Есендаулетова, Л.С. Фазылова, М.Б. Рахимжанова, А.М. Недзьведь ИСПОЛЬЗОВАНИЕ НЕЙРОННЫХ СЕТЕЙ ДЛЯ ОБЪЕКТИВНОЙ ОЦЕНКИ ВНИМАНИЯ У ДЕТЕЙ ПО ДАННЫМ ЭЭГ	158
А.Е. Кулакаева, Е.А. Бахтиярова, Г.Т. Джаканова, Ш. Нурсултан СРАВНИТЕЛЬНЫЙ АНАЛИЗ РАЗЛИЧНЫХ МОДЕЛЕЙ РАСПРОСТРАНЕНИЯ РАДИОВОЛН ДЛЯ ПРОГНОЗИРОВАНИЯ ПОКРЫТИЯ СЕТЕЙ МОБИЛЬНОЙ СВЯЗИ	173
М.Б. Нурпенсова, Ш.К. Айтказинова, А.М. Абеннов, Н.С. Доненбаева МЕТОДИКА ПРЕОБРАЗОВАНИЯ СПУТНИКОВЫХ КООРДИНАТ В ТОПОЦЕНТРИЧЕСКУЮ ПРЯМОУГОЛЬНУЮ СИСТЕМУ КООРДИНАТ	189
А. Оспанов, П. Алонсо-Хорда, А. Жумадиллаева ИНТЕГРАЦИЯ СКЛАДСКИХ МОДУЛЕЙ ERP-СИСТЕМ С ИСПОЛЬЗОВАНИЕМ БЛОКЧЕЙНА, IOT-ДИМЕНСИОНЕРОВ И ОПТИМИЗИРОВАННОГО МАШИНЫМ ОБУЧЕНИЕМ РАСЧЁТА ГАБАРИТНО-ГО ВЕСА	202
А.А. Сахипов, Р.Б. Сейитбек СОБЫТИЯ-ОРИЕНТИРОВАННЫЕ МИКРОСЕРВИСЫ ДЛЯ ОБНАРУЖЕНИЯ И РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ В ИНТЕЛЛЕКТУАЛЬНЫХ ТРАНСПОРТНЫХ СИСТЕМАХ	218
Г.М. Юсупова, К.С. Шадинова, Д.И. Усипбекова, Ж.Ж. Ажибекова, П. Шмидт ОПРЕДЕЛЕНИЕ СТРАТИФИКАЦИИ ПОЧВЕННОГО ПРОФИЛЯ НА ГЛУБИНЕ 0–200 СМ С ИСПОЛЬЗОВАНИЕМ МОДЕЛИ МНОГОУРОВНЕВОГО НАЛОЖЕНИЯ	231
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ	
С.А. Адилжанова, М.Ж. Сакыпбекова, Л.Ш. Черикбаева, Г.А. Тюлепбердинова, Г.Т. Жубанышева СИСТЕМАТИЧЕСКИЙ АНАЛИЗ МЕТОДОВ И МОДЕЛЕЙ ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	244
Т.К. Жукабаева, Д.Б. Баумуратова, Е. Бенкхелифа, Н.А. Ниетбаева МЕТОДИКА ПОСТРОЕНИЯ СРЕДСТВ ОБНАРУЖЕНИЯ АТАК В КИБЕРФИЗИЧЕСКИХ СИСТЕМАХ ПРОМЫШЛЕННОГО ИНТЕРНЕТА ВЕЩЕЙ С ИСПОЛЬЗОВАНИЕМ ГРАНИЧНЫХ ВЫЧИСЛЕНИЙ	270
Н.Е. Карабаев, С.К. Серикбаева, Е.М. Марденов, Б. Тасуов, М. Файкус ОБНАРУЖЕНИЕ КИБЕРАТАК В ТРАНСПОРТНЫХ СЕТЯХ НА ОСНОВЕ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ	292
Б.А. Кумалаков, А.О. Даргулова ГИБРИДНЫЙ ПОДХОД К АВТОМАТИЗИРОВАННОМУ ПОДБОРУ КАНДИДАТОВ НА ОСНОВЕ СОПОСТАВЛЕНИЯ РЕЗЮМЕ И ВАКАНСИЙ	311
В. Махатова, Б. Джугембаева, А. Габдулова, Л. Нургалиева, А. Абдигалиева МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ВЫБОРА ОПТИМАЛЬНОГО СЕНСОРА В SIEM-СИСТЕМАХ СРЕДСТВАМИ МЕТОДА АНАЛИЗА ИЕРАРХИЙ	326

INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES

ISSN 2708–2032 (print)

ISSN 2708–2040 (online)

Vol. 7. Is.1. Number 25 (2026). Pp. 326–349

Journal homepage: <https://journal.iitu.edu.kz>

<https://doi.org/10.54309/IJICT.2026.25.1.020>

UDC 004.032.26

MATHEMATICAL MODEL FOR OPTIMAL SENSOR SELECTION IN SIEM SYSTEMS USING THE ANALYTIC HIERARCHY PROCESS

*V. Makhatova*¹, *B. Dzhugembayeva*^{1*}, *A. Gabdulova*¹, *L. Nurgaliyeva*², *A. Abdigaliyeva*³

¹Kh.Dosmukhamedov Atyrau University, Atyrau, Kazakhstan;

²Saidot Ltd., Helsinki, Finland;

³Safi Utebayev Atyrau Oil and Gas University, Atyrau, Kazakhstan.

E-mail: asbaku@mail.ru

Valentina Makhatova — Candidate of Technical Sciences, Professor of the Department of Software Engineering, Kh.Dosmukhamedov Atyrau University, Atyrau, Kazakhstan
<https://orcid.org/0000000240829193>;

Bakhytgul Dzhugembayeva — Ms.Sc., Senior Lecturer Kh. Dosmukhamedov Atyrau University, Atyrau, Kazakhstan

E-mail: asbaku@mail.ru, <https://orcid.org/0000-0002-2697-5194>;

Aigul Gabdulova — Ms.Sc., Senior Lecturer, Department of Software Engineering, Kh.Dosmukhamedov Atyrau University, Atyrau, Kazakhstan

<https://orcid.org/0000-0002-6589-854>;

Lunara Nurgaliyeva — Ms.Sc., AI Safety ML/LLM Engineering, Saidot Ltd. Helsinki, Finland

<https://orcid.org/0009-0005-5252-9525>;

Akmaral Abdigaliyeva — Ms.Sc., Senior Lecturer, Faculty of Information Technology, Safi Utebayev Atyrau Oil and Gas University, Atyrau, Kazakhstan

<https://orcid.org/0009-0003-7907-6875>.

© V. Makhatova, B. Dzhugembayeva, A. Gabdulova, L. Nurgaliyeva, A. Abdigaliyeva

Abstract. This paper presents a mathematical model for the optimal selection of sensors in Security Information and Event Management (SIEM) systems using the Analytic Hierarchy Process (AHP). The growing complexity of modern information infrastructures and the increasing number of cyber threats require reliable and efficient monitoring mechanisms. Since the effectiveness of a SIEM system significantly depends on the performance and configuration of its sensors, the problem of selecting the most suitable sensor under multi-criteria conditions becomes a relevant scientific and practical task. The proposed approach formalizes the sensor selection process as a three-level hierarchical structure that includes the main objective, a system of evaluation criteria,



and alternative sensor configurations. The criteria considered in the study include system load, reaction time, working time, efficiency, implementation cost, labor intensity, universality, implementation quality, and prevalence. Pairwise comparisons were performed according to the Saaty scale, and weighting coefficients were calculated using eigenvalue-based methods. The consistency index and consistency ratio were evaluated to ensure the reliability of expert judgments. Based on the developed model, a software tool was implemented in C++ using the MySQL database management system. The system automates the formation of comparison matrices, calculation of priority vectors, and ranking of alternatives. Experimental results demonstrate that the application of AHP improves the objectivity and transparency of decision-making, reduces configuration time, and increases the reliability of SIEM sensor deployment. The proposed model is scalable and can be adapted to various information security infrastructures, contributing to the advancement of multi-criteria optimization methods in cybersecurity.

Keywords: information security, SIEM, sensor, Analytic Hierarchy Process (AHP), decision-making

For citation: V. Makhatova, B. Dzhugembayeva, A. Gabdulova, L. Nurgaliyeva A. Abdigaliyeva (2026). Mathematical model for optimal sensor selection in siem systems using the analytic hierarchy process // International journal of information and communication technologies. Vol. 7. No. 25. Pp. 326–349. <https://doi.org/10.54309/IJICT.2026.25.1.020>. (In Eng.).

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

ИЕРАРХИЯЛАРДЫ ТАЛДАУ ӘДІСІ НЕГІЗІНДЕ SIEM ЖҮЙЕЛЕРІНДЕ ОҢТАЙЛЫ СЕНСОРДЫ ТАҢДАУДЫҢ МАТЕМАТИКАЛЫҚ МОДЕЛІ

В. Махатова¹, Б. Джугембаева¹, А. Габдулова^{1}, Л. Нурғалиева²,
А. Абдигалиева³*

¹ Х. Досмұхамедов атындағы Атырау университеті, Атырау, Қазақстан;

² Saidot Ltd. Хельсинки, Финляндия;

³ С.Өтебаев атындағы Атырау мұнай және газ университеті, Атырау, Қазақстан.

E-mail: asbaku@mail.ru

Валентина Махатова — техника ғылымдарының кандидаты, Х. Досмұхамедов атындағы Атырау университетінің «Бағдарламалық инженерия» кафедрасының профессоры, Атырау, Қазақстан

<https://orcid.org/0000000240829193>;

Бакытгул Джугембаева — сеньор лектор, Х. Досмұхамедов атындағы Атырау университетінің «Физика және техникалық пәндер» кафедрасы, Атырау, Қазақстан

E-mail: asbaku@mail.ru, <https://orcid.org/0000-0002-2697-5194>;

Айгул Габдулова — сеньор лектор, Х. Досмұхамедов атындағы Атырау университетінің «Бағдарламалық инженерия» кафедрасы, Атырау, Қазақстан

<https://orcid.org/0000-0002-6589-854X>;

Лунара Нургалиева — магистр, AI Safety ML/LLM Engineering, Saidot Ltd. Helsinki, Finland

<https://orcid.org/0009-0005-5252-9525>;

Ақмарал Абдигалиева — магистр, Ақпараттық технологиялар факультеті, Сафи Өтебаев атындағы Атырау мұнай және газ университеті, Атырау, Қазақстан.

<https://orcid.org/0009-0003-7907-6875>.

© В. Махатова, Б. Джугембаева, А. Габдулова, Л. Нургалиева, А. Абдигалиева

Аннотация. Бұл мақалада SIEM класты ақпараттық қауіпсіздікті басқару жүйелерінде оңтайлы сенсорды таңдау үшін иерархияларды талдау әдісі (ИТӨ) негізінде математикалық модель ұсынылады. Заманауи ақпараттық инфрақұрылымдардың күрделенуі және киберқауіптердің артуы сенімді әрі тиімді мониторинг тетіктерін қажет етеді. SIEM жүйесінің тиімділігі көбінесе қолданылатын сенсорлардың сипаттамалары мен конфигурациясына тәуелді болғандықтан, көпкритерийлі ортада ең қолайлы сенсорды таңдау ғылыми әрі практикалық тұрғыдан өзекті мәселе болып табылады. Ұсынылған тәсіл сенсорды таңдау үдерісін үш деңгейлі иерархиялық құрылым түрінде формалдайды: негізгі мақсат, бағалау критерийлері және баламалы сенсорлар. Зерттеуде келесі критерийлер ескерілді: жүйеге түсетін жүктеме, жауап беру уақыты, жұмыс уақыты, тиімділік, енгізу құны, енгізудің еңбек сыйымдылығы, әмбебаптық, жүзеге асыру сапасы және таралу деңгейі. Жұптық салыстырулар Саати шкаласы бойынша жүргізіліп, салмақ коэффициенттері меншікті мәндер әдісі арқылы есептелді. Сараптамалық бағалардың дұрыстығын тексеру үшін келісімділік индексі және келісімділік қатынасы анықталды. Өзірленген модель негізінде C++ бағдарламалау тілінде және MySQL деректер қорын басқару жүйесін қолдана отырып бағдарламалық құрал жасалды. Жүйе жұптық салыстыру матрицаларын құруды, басымдық векторларын есептеуді және баламаларды ранжирлеуді автоматтандырады. Эксперименттік нәтижелер иерархияларды талдау әдісін қолдану шешім қабылдау үдерісінің объективтілігі мен айқындығын арттыратынын, жүйені баптау уақытын қысқартатынын және SIEM инфрақұрылымында сенсорды таңдаудың сенімділігін жоғарылататынын көрсетті. Ұсынылған модель масштабталатын болып табылады және әртүрлі ақпараттық қауіпсіздік жүйелеріне бейімделе алады, бұл киберқауіпсіздік саласындағы көпкритерийлі оңтайландыру әдістерін дамытуға ықпал етеді.

Түйін сөздер: ақпараттық қауіпсіздік; SIEM; сенсор; иерархияларды талдау әдісі; шешім қабылдау

Дәйексөздер үшін: В. Махатова, Б. Джугембаева, А. Габдулова, Л. Нургалиева А. Абдигалиева (2026). Иерархияларды талдау әдісі негізінде siem жүйелерінде оңтайлы сенсорды таңдаудың математикалық моделі // Халықаралық ақпараттық және коммуникалық технологиялар журналы. Т. 7. № 25. Б. 326–349. <https://doi.org/10.54309/IJICT.2026.25.1.020>. (Ағыл. тіл.).

Мүдделер қақтығысы: Авторлар осы мақалада мүдделер қақтығысы жоқ



деп мәлімдейді.

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ВЫБОРА ОПТИМАЛЬНОГО СЕНСОРА В SIEM-СИСТЕМАХ СРЕДСТВАМИ МЕТОДА АНАЛИЗА ИЕРАРХИЙ

В. Махатова¹, Б. Джугембаева¹, А. Габдулова^{1}, Л. Нургалиева²,
А. Абдигалиева³*

¹Атырауский университет имени Х. Досмухамедова, Атырау, Казахстан;

²Saidot Ltd. Хельсинки, Финляндия;

³Атырауский университет нефти и газа имени С.Утебаева, Атырау, Казахстан.

E-mail: asbaku@mail.ru

Валентина Махатова — кандидат технических наук, профессор кафедры «Программная инженерия» Атырауского университета имени Х. Досмухамедова, Атырау, Казахстан

<https://orcid.org/0000-0002-4082-9193>;

Бакытгуль Джугембаева — магистр, старший преподаватель Атырауского университета имени Х. Досмухамедова, Атырау, Казахстан

E-mail: asbaku@mail.ru, <https://orcid.org/0000-0002-2697-5194>;

Айгуль Габдулова — магистр, старший преподаватель кафедры «Программная инженерия» Атырауского университета имени Х. Досмухамедова, Атырау, Казахстан

<https://orcid.org/0000-0002-6589-854X>;

Лунара Нургалиева — магистр, инженер по безопасности ИИ и машинного обучения/больших языковых моделей (AI Safety ML/LLM Engineering), компания Saidot Ltd. Хельсинки, Финляндия

<https://orcid.org/0009-0005-5252-9525>;

Акмарал Абдигалиева — магистр, старший преподаватель факультета информационных технологий Атырауского университета нефти и газа имени Сафи Утебаева, Атырау, Казахстан

<https://orcid.org/0009-0003-7907-6875>.

© В. Махатова, Б. Джугембаева, А. Габдулова, Л. Нургалиева, А. Абдигалиева

Аннотация. В данной статье представлена математическая модель выбора оптимального сенсора в системах управления информационной безопасностью класса SIEM на основе метода анализа иерархий (МАИ). Возрастающая сложность современных информационных инфраструктур и увеличение количества киберугроз требуют надежных и эффективных механизмов мониторинга. Поскольку эффективность функционирования SIEM-системы во многом зависит от характеристик и конфигурации используемых сенсоров, задача выбора наиболее подходящего сенсора в условиях многокритериальности является актуальной на-

учной и практической проблемой. Предложенный подход формализует процесс выбора сенсора в виде трехуровневой иерархической структуры, включающей целевую функцию, систему критериев оценки и альтернативные варианты сенсоров. В исследовании учитываются следующие критерии: нагрузка на систему, время реакции, рабочее время, эффективность, стоимость реализации, трудоёмкость внедрения, универсальность, качество реализации и распространённость. Парные сравнения проводились по шкале Саати, а весовые коэффициенты рассчитывались на основе методов определения собственных значений. Для проверки корректности экспертных оценок были вычислены индекс согласованности и отношение согласованности. На основе разработанной модели реализовано программное обеспечение на языке C++ с использованием СУБД MySQL. Система автоматизирует формирование матриц парных сравнений, расчет векторов приоритетов и ранжирование альтернатив. Результаты экспериментов показывают, что применение метода анализа иерархий повышает объективность и прозрачность принятия решений, сокращает время настройки системы и увеличивает надежность выбора сенсоров для SIEM-инфраструктуры. Предложенная модель является масштабируемой и может быть адаптирована к различным системам информационной безопасности, способствуя развитию методов многокритериальной оптимизации в сфере кибербезопасности.

Ключевые слова: информационная безопасность; SIEM; сенсор; метод анализа иерархий; принятие решений

Для цитирования: В. Махатова, Б. Джугембаева, А. Габдулова, Л. Нургалиева А. Абдигалиева (2026). Математическая модель выбора оптимального сенсора в siem-системах средствами метода анализа иерархий. // Международный журнал информационных и коммуникационных технологий. Т. 7. №. 25. Стр. 326–349. <https://doi.org/10.54309/IJICT.2026.25.1.020>. (На англ.).

Конфликт интересов: авторы заявляют об отсутствии конфликта интересов.

Introduction.

Modern information systems are an integral part of the infrastructure of enterprises, government agencies, and commercial organizations. As data volumes and levels of automation grow, the number of information security threats increases significantly, requiring continuous improvement of protection and monitoring methods. One of the most effective tools is a security information and event management system (SIEM), which collects, correlates, and analyzes data on events occurring within the protected network.

The effectiveness of a SIEM system depends on the proper operation of its sensors—the components that collect, filter, and transmit security event data. An incorrectly selected or improperly configured sensor can lead to the loss of critical data, false alarms, or increased system load. Therefore, the problem of selecting the optimal sensor that balances performance, reliability, and cost is a pressing scientific and practical is-

sue.

Traditional sensor selection methods rely primarily on expert assessments and empirical data, which do not always account for the multi-criteria nature and mutual influence of system parameters. Therefore, it is advisable to apply formalized mathematical methods of multi-criteria analysis, capable of considering both quantitative and qualitative characteristics. One of the most universal approaches is the Analytic Hierarchy Process (AHP), proposed by T. Saaty, which is widely used in optimization and decision support problems.

Using the Analytic Hierarchy Process (AHP) allows us to represent the sensor selection process as a hierarchical structure: from the primary goal—improving the effectiveness of the security system—to subordinate levels of criteria and alternatives. This model enables us to objectively assess the importance of each criterion, determine the weights of alternatives, and formulate a quantitative justification for the selection.

The objective of this study is to develop a mathematical model and software tool that enable rational selection of the optimal sensor for a SIEM system using the Analytic Hierarchy Processing (AHP) method. To achieve this goal, the following tasks are addressed:

- An analysis of existing approaches to the construction and configuration of SIEM systems was conducted;
- a hierarchical structure of sensor selection criteria has been formed;
- an algorithm for calculating weights and consistency indices has been implemented;
- a software module was developed in C++ using the MySQL DBMS;
- An experimental verification of the correctness and effectiveness of the proposed model was carried out.

The results of the study are aimed at improving the efficiency of SIEM system setup and operation, reducing the risk of information incidents, and ensuring a higher level of information infrastructure security.

Materials and Methods

SIEM Systems.

Security Information Event Management (SIEM) is the general name for software products previously used separately from each other, categories SIM (Security Information Management) and SEM (Security Event Management).

A typical SIEM system faces the following tasks.

Consolidation and storage of event logs from various sources – network devices, applications, OS logs, security tools. Sometimes an incident is detected late, and the events have long since been deleted, or the event logs are inaccessible for some reason, making it impossible to identify the cause of the incident. Furthermore, connecting to each source and viewing events is time-consuming.

Providing tools for event analysis and incident resolution. Event formats vary across various sources. Text-based formats can be cumbersome when dealing with large volumes and reduce the likelihood of incident detection. Some SIEM products standard-

ize events and make them more readable, while the interface visualizes only valuable information events, highlights them, and allows filtering out non-critical events.

Correlation and rule-based processing. A single event doesn't always indicate an incident. The simplest example is "login failed": one instance is insignificant, but three or more such events involving the same account may indicate brute-force attacks. In the simplest case, rules in SIEM are represented in RBR (RuleBasedReasoning) format and contain a set of conditions, triggers, counters, and action scripts.

Automatic notification and incident management.

The primary goal of a SIEM is not simply to collect events, but to automate the process of incident detection, documenting them in its own log or an external HelpDesk system, and providing timely notification of events. A SIEM can detect:

network attacks on internal and external perimeters;

viral epidemics or individual viral infections, unremoved viruses, backdoors and Trojans;

attempts to gain unauthorized access to confidential information;

errors and failures in the operation of information systems;

vulnerabilities;

Configuration errors in security tools and information systems.

A SIEM system is versatile thanks to its logic. But to accomplish its intended tasks, useful sources and correlation rules are necessary. Any event (for example, a door opening in a specific room) can be fed to the SIEM input and used.

Sources are selected based on the following factors:

criticality of the system (value, risks) and information (processed and stored);

reliability and informativeness of the source of events;

coverage of information transmission channels (not only the external but also the internal perimeter of the network must be considered);

solving a range of IT and information security problems (ensuring continuity, incident investigation, policy compliance, preventing information leaks, etc.).

Main sources of SIEM

AccessControl, Authentication – for monitoring access control to information systems and the use of privileges.

Server and workstation event logs – for access control, ensuring continuity, and compliance with information security policies.

Network active equipment (change and access control, network traffic counters).

IDS/IPS. Events about network attacks, configuration changes, and device access.

Antivirus protection. Events about software performance, databases, configuration and policy changes, and malware.

Vulnerability scanners. Inventorying assets, services, software, and vulnerabilities, providing inventory data and topology structure.

GRC systems for risk accounting, threat criticality, and incident prioritization.

Other systems for protecting and monitoring information security policies: DLP, anti-fraud, device control, etc.

Inventory and asset management systems. To monitor infrastructure assets and identify new ones.

Netflow and traffic accounting systems.

A SIEM solution typically includes several components (Figure 1):

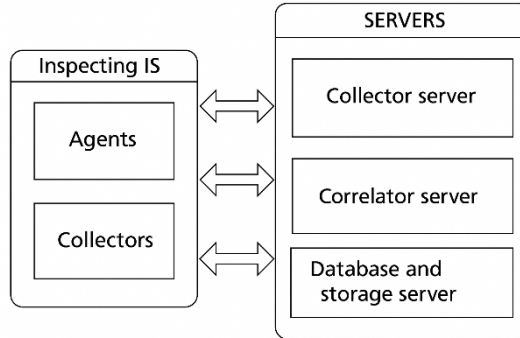


Fig. 1. SIEM structure.

Agents installed on the information system in question (relevant for OS; an agent is a separate program (service) that locally checks all event services and sends statistics to the server);

Agent collectors, otherwise known as modules for understanding a separate log of all system events;

Collector server, required for initial collection of events from various sources;

Correlator server, required for collecting data from collectors and agents and studying the received data using algorithms and rules of mutual intersection.

Database server and storage, which are responsible for storing all data.

Often, a SIEM system is presented in an agent architecture - a place for storing information - a program server installed on top of the protected IT structure (Zhumabekov, 2021)

Agents implement the collection of security events, their rapid analysis and filtering by type.

All filtered security event data is transferred to a storage or a specific case, where it is placed in an internal presentation format for further use in analysis by the program server.

This server supports basic ZI functionality. It analyzes the data stored in a case and translates it to generate alerts and conclusions about the ZI.

As a result, 3 levels of construction are often distinguished in a SIEM system: the data collection level; the data control level; and the data study level (Zhang et al., 2019).

At the first level, data is collected from several types of sources. These include file servers, database servers, Windows servers, firewalls, workstations, intrusion pre-

vention systems (IPS), antivirus programs, and so on.

The second level manages security event data stored in the repository.

Data stored in the repository is retrieved in response to queries from data analysis models.

The results of information processing in the SIEM system, obtained at the third level, are reports in predefined and arbitrary forms, operational (online) correlation of event data, as well as alerts generated online and/or transmitted via email. (Gorelik et al., 2020)

To improve analysis and visibility, and to accelerate response to increasingly complex threats, SIEM systems must be transformed into a full-fledged security platform. The next step in the evolution of security information and event management should be to ensure the following four conditions are met.

Comprehensive view

Security analysis platforms must support full replay of any activity so that security operations center analysts have access to all the information they need to determine the best way to address potential issues.

Malware detection – threats are becoming increasingly difficult to identify as they disguise themselves as legitimate software in network traffic. Collecting full network packets allows for file reconstruction and automation of most of the analytical processes necessary for detecting signs of malware.

Tracking attacker activity within the environment - Network packet capture is becoming a key method for tracking an attacker's movements within an organization's network. Providing evidence of malicious activity – Systems that support full network packet capture can record entire sessions to demonstrate all attacker actions related to the acquisition of sensitive data. Adding network packet capture and session replay capabilities to new-generation security information and event management systems is key to threat investigation and prioritization. For example, traditional SIEM tools may inform you that your computer has detected communication with a suspicious server, but you won't know the exact data exchanged. Packet capture and session replay, combined with information from logs and other sources, provides security professionals with a more detailed analysis of the detection and assesses its significance. Detailed investigation capabilities help security operations center staff analyze suspicious activity step by step and mitigate the impact of advanced threats. (Khraisat et al., 2019)

Deeper analytics and faster investigations

Security analysis systems must have the means to examine disparate data and identify signs of advanced threats. For example, they must search for behavior patterns and risk factors, not just static rules and known signatures. Security analysis systems must also consider the relative value of information assets at risk, flagging the most critical ones.

When determining the risk level of big data, security analytics platforms can exclude known trusted actions, thereby increasing accuracy by reducing the volume of information security professionals must analyze for new threats. In-depth automated

analysis provides events of interest with a frequency profile. Thus, security analytics systems triage events for analysts, highlighting those that require more detailed investigation. (Aldwairi et al., 2020)

As fully automated components of new security platforms, these tools cannot replace human expertise and decision-making skills, but rather merely draw specialists' attention to issues requiring careful consideration. Security analysis systems are designed to help security operations centers expand their threat detection capabilities in ways previously unavailable. This allows analysts to promptly investigate incidents and compare the impact of increasingly complex threats (Ring et al., 2019)

Security information and event management systems, when transformed into security analytics platforms, must be scalable in scale and scope to handle massive volumes of heterogeneous data both within and outside the organization. In-depth traffic analysis from various devices across the network significantly increases the volume of data the platform must process. Adding advanced threat investigation tools from external sources transforms the security console into a security data analytics hub, which must also meet scalability requirements.

To address modern threats, security analytics platforms must support features such as a distributed N-tier storage architecture and analytics engine that normalizes and processes large, distributed data sets at high speed. The analytics platform must scale in parallel with the storage system. (Gupta et al., 2021)

To stay informed and view events in context, security professionals must always have access to all information relevant to system security. In addition to collecting data from within their network, security analysis platforms must also automatically integrate up-to-date threat intelligence from third-party researchers, government agencies, industry associations, and open-source investigations. By providing all the necessary information, the platform frees analysts from the need to manually collect data and saves their time. Centralizing all available investigative tools within a unified analysis platform provides analysts with an up-to-date picture of the IT environment, allows them to view events in context, and accelerates decision-making.

Models of SIEM Systems

A SIEM system incorporates the functions of two third-party systems related to information security management systems-SIM and SEM. Based on this, a SIEM system implements functions that are understandable for both SIM and SEM systems. The basic set of rules for a SIM system is the collection, storage, and analysis of all logged data, as well as the generation of reports. The fundamental basis for SEM systems is the online monitoring of security events, as well as the response and reporting of ongoing incidents (Kurmangaliyeva et al., 2023).

The implementation of these functions in the SIEM system under consideration is possible thanks to a complex set of various operational mechanisms. In Type I SIEM systems, such mechanisms include normalization, filtering, classifying, aggregation, mutual intersection and division of event importance, as well as the creation of alerts and reports [5]. Modern SIEM systems also include analysis of events occurring during

incidents and their consequences, as well as a solution implementation mechanism and visual presentation.

Let us describe the core principles of a SIEM system's operation. Normalization involves converting log record formats collected from various sources into a single base format that can be used for storage and further analysis. Filtering all transferred events involves removing large events from incoming system streams. Segmentation allows security event attributes to be expressed by their role in certain classes. Aggregation consists entirely of events that are similar in a few properties. Mutual intersection reflects the relationships between similar events, which helps us understand the nature of attacks on critical infrastructure, as well as adjust information security criteria and policies. The priority mechanism reflects the importance and criticality of security events within the rules available in the system (Dyusembaev et al., 2017).

Understanding events, incidents, and their resulting values involves constructing a model of events, attacks, and their outcomes, studying system availability and security, expressing attacker metrics, risk assessment procedures, and predicting events and situations. Reporting and forecasting reflect the generation, printing, and dissemination of work results. Implementing solutions involves identifying measures to adjust security methods to mitigate attacks or create a completely secure infrastructure. The visual component includes data display in graph form, which helps describe the analysis of security events and the level of security of the entire maintained CVI system and its individual components.

It should be noted that when moving to higher-level mechanisms of the model shown in Fig. 2, the number of events processed decreases, and the complexity of their processing increases.

The interrelationship of the operating mechanisms of the new generation SIEM system is clearly demonstrated by the functional model presented in Fig. 2.

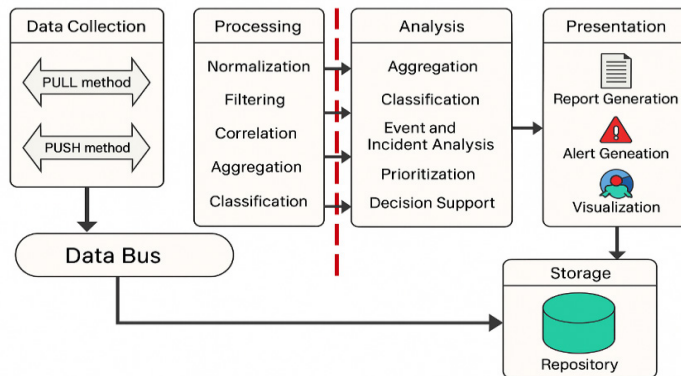


Fig. 2. Interrelation of the SIEM system functioning mechanisms.

As can be seen from Fig. 2, the SIEM system can be divided into five main func-

tional subsystems: (1) data collection; (2) processing; (3) storage; (4) analysis; (5) presentation. The first two operate in online mode, while the others operate in near-online mode. Let us briefly describe these subsystems.

Two main methods are used to obtain information from sources: Push and Pull. With Push, the source sends its log data to the SIEM system. With Pull, the system automatically retrieves the log data.

Data is collected from diverse types of sources.

Processing subsystem. Information processing includes normalization, filtering, correlation, aggregation, and classification.

Storage subsystem. Filtered data in normalized form is stored in a repository. The repository can be built on a relational DBMS (the most common solution), an XML-based DBMS, and/or a triplet store. A triplet store is a specially designed database optimized for storing and retrieving triplets, i.e., statements of the “subject-predicate-object” type.

Analysis subsystem. Data analysis includes the following functions: data correlation, classification, aggregation, prioritization, and analysis of events, incidents, and their consequences (including through event modeling, attacks, and their consequences, vulnerability and system security analysis, intruder characterization, risk assessment, and event and incident forecasting), as well as decision support. Data analysis can be based on qualitative and quantitative assessments. Quantitative assessment is more accurate but significantly more time-consuming, which is not always acceptable. Most often, a quick qualitative analysis is sufficient, the purpose of which is to categorize risk factors. The scale of qualitative analysis may vary across assessment methods, but the goal is to identify the most serious threats. (Ring et al., 2019)

Presentation subsystem. The presentation includes several functions: visualization, report generation, and alert generation (Abubakirov et al., 2022).

When studying various systems-social, economic, natural, and man-made-it’s important to consider the totality of external factors to account for all factors within the system as a single entity. However, the connections between these components cannot often be considered due to a lack of sufficient data, and for some tasks, such as forecasting and simulation, data may be completely absent. In such cases, the necessary connections are created through expert assessments. These are often implemented as weighting parameters used to numerically evaluate the contribution of a given factor to the result. (Saaty et al., 1980)

Accounting for weight parameters. Various approaches are used for this accounting, and many methodologies have already been implemented within them. Since there is no goal to provide a general description of the various methods used to express weight coefficients, only an analysis of the main approaches was performed.

Direct weighting. Experts refine factor weights based on requirements, such as the sum of the weights being between 1% and 100%, although another constant can often be used if it’s convenient for further calculations. This process is often confusing factors specific values on an explicit numerical scale, but in this case, it’s better to call



such factors “significance indicators” rather than “weights,” as they are then assessed comparatively rather than by their overall impact. Weighting coefficients are also implemented in an analogous manner, but that’s where we’ll end.

The difficulty of this approach lies in the ability to implicitly contain all factors within a separate framework, since by assigning a numerical value to any factor, the expert must also correlate it with the others. The complexity increases progressively as the number of factors increases.

There are also technical difficulties in the specialist’s work related to the importance of periodically monitoring the current sum of weighting factors to avoid increasing the specified constant or transferring the remaining substantial portion to extreme factors. If this occurs, it is customary to recalculate all sent coefficients, which can be done several times during the exchange process. The number of operations increases as the number of factors increases.

Factor ranking. This approach simplifies the experts’ work, as it eliminates the need to control the total sum of the coefficients. In this case, experts are required to rank, i.e., the factors under consideration that form the object according to the degree of their properties’ identification, in order of their minimization or enhancement.

$$\left. \begin{matrix} R_{11}, R_{21}, \dots, R_{i1} \\ R_{12}, R_{22}, \dots, R_{i2} \\ \dots \dots \dots \dots \dots \dots \dots \\ R_{1j}, R_{2j}, \dots, R_{ij} \end{matrix} \right\}, \tag{1}$$

Where R_{ij} is the rank (place) assigned to factor O_{ij} by the j th expert in a series of n -studied objects, based on the degree of expression of the analyzed property. Two or more factors may have the same rank, but then the rank is a fraction. The summary estimates of the weighting coefficients are obtained by averaging the partial ranks across the columns.

The advantage of this method lies in its simplicity, but this simplicity isn’t always beneficial, as averaging the ranks results in rougher weighting estimates than other methods. It also doesn’t relieve the expert of the responsibility of controlling all factors, as with direct ranking.

Transferring coefficients to factors. This method asks experts to rate factors on a scale, for example, from 1 to 10. The result is:

$$\left. \begin{matrix} y_{11}, y_{21}, \dots, y_{i1} \\ y_{12}, y_{22}, \dots, y_{i2} \\ \dots \dots \dots \dots \dots \dots \dots \\ y_{1j}, y_{2j}, \dots, y_{ij} \end{matrix} \right\}, \tag{2}$$

where y_{ij} is the factor score transmitted from the j -th expert, n is the sum of factors, m is the number of experts.

Summary estimates of the weighting coefficients are often found by selecting an

appropriate regression model. The average estimate w_i of the factor weighting coefficients is obtained using trivial formulas:

$$w_i = \frac{\sum_{j=1}^m w_{ij}}{\sum_{i=1}^n \sum_{j=1}^m w_{ij}}, \quad (3)$$

where w_{ij} is the weight of the i -th object, based on the assessments of all experts;

$$w_{ij} = \frac{x_{ij}}{\sum_{i=1}^n x_{ij}}, \quad (4)$$

where x_{ij} is the assessment of factor i given by expert j ;
 n is the number of factors, m is the number of experts.

This method weakens the dependence of the assessment of an individual factor on the others, but does not eliminate it, since it is necessary to compare the factors, otherwise it will not be possible to correctly assign the significance coefficients.

The Analytical Hierarchy Processing (AHP) method, created by T. Saaty in the 1980s, was designed to partially minimize the above-mentioned difficulties. The essence of the method is as follows. (Saaty et al., 1993; Saaty et al., 1980)

Factors are considered in pairs relative to each other based on their impact on the final goal. The influence of other factors is not considered. For pairwise comparison of factors, the Saaty method uses a special rating scale, including five main and four intermediate judgments (Saaty, T., 1980).

In it, the experts' arguments were highlighted as follows (Table 1):

Table 1 – Specifics of expert comparisons of the ratio of factors.

Judgment	Explanation
1. Equal importance	Equal contribution of factors to the final goal
2. ...	Additional expression
3. A slight advantage	Judgment and experience give slight superiority to one factor over the others
4. ...	Additional expression
5. Tangible superiority	Sensitive dominance of one factor over the others
6. ...	Additional expression
7. Increased superiority	There is a significant predominance of one factor over the others
8. ...	Additional expression
9. Supreme Excellence	There is a confident superiority of one factor over the others.

The results of such pairwise comparisons are presented as a square matrix $A = (a_{ij})$ with a diagonal equal to 1 (comparing a factor to itself equals 1). Here, "a" becomes the ratio of the ratings of specific elements; the indices i and j range from one to a value equal to the sum of the factors. Since, when sequentially searching through all available pairs, the factors are related to each other twice (a_{ij} with a_{ji} , then vice versa), the "reverse symmetry" condition must be true when preparing the matrix: . It follows that it is sufficient to fill only one part of the matrix—the one located above or

below the diagonal—which has no specific significance due to the simple recalculation of mutually inverse parameters. If n factors are studied, then a total of $a_{ji} = \frac{1}{a_{ij}} \cdot 100$ meaningful combinations will be available. $\frac{n^2-n}{2}$

In MAI, the number of a specific row of Table 2 is used for coding. Any of the specified judgments is coded in the range of numbers from 1/9 to 9.

Weights are calculated in several ways. One available method for approximating the weight vector is to calculate a separate vector of the pairwise comparison matrix, usually corresponding to the larger eigenvalue. Such algorithms for obtaining eigenvectors have been thoroughly studied, and their descriptions can be found either in monographs or in other literature.

The MAI method has its own parameters for expressing the quality of expert performance—the consistency index (CI), which provides data on the level of violation of the numerical and ordinal consistency of expert judgments. Cardinality control involves considering specific numerical characteristics, deviations from which indicate errors in the process of conveying expert judgments. Therefore, if separate rules for coding expert judgments are created, for example, from 0 to 1, then expert judgments cannot deviate from the value sets specified in these rules, i.e., be greater than one or negative. The ordering helps understand the logic of the expert’s reasoning. If an expert believes that factor A is better than factor B, and factor B, in turn, is better than factor C, then in a paired comparison, factor C cannot be better than factor A, i.e., the inequality $A > B > C$ is satisfied. Inconsistency is a significant limiting factor for studying individual problems.

The IS is calculated as follows: together with the pairwise comparison matrix, there is a measure of the degree of deviation from the desired value. The IS in each matrix for each hierarchy is estimated using the formula:

$$ИС = \frac{\lambda - n}{n - 1}, \tag{5}$$

where λ is the eigenvalue,
 n – the number of factors being compared.

The IS is compared with the value obtained from a random selection of quantitative variables, which is treated as the average. The average consistency (MC) for random matrices of different orders is given in Table 2, where n is the number of factors.

Table 2 – Average consistency (MC) for random matrices of different orders

n	1	2	3	4	5	6	7	8	9	10
SS	0	0	0.58	0.90	1.12	1.24	1.32	1.41	1.45	1.49

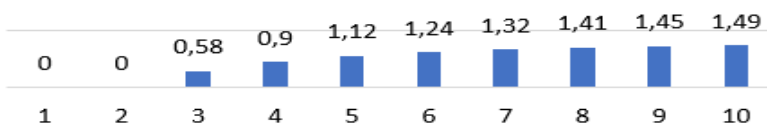


Fig. 3. Average consistency (MC) for random matrices of different orders

If we divide the IS by the SS for a matrix of the same order, we obtain the consistency ratio (CR):

$$OC = \frac{HC}{CC} * 100\%, \quad (6)$$

It seems that MAI is the optimal solution for solving a variety of problems where expert analysis methods are used as key ones. This is true, and we will outline the main reasons for this.

Pairwise comparisons. Pairwise comparisons of things can also be found in human nature. Minimizing the need to always consider all factors, or, for example, some of them, allows the expert to focus more on a specific issue: how factor A_j is ahead of factor B_j or behind it. This allows for more accurate results.

Complementarity of the initial matrix. In the practice of system analysis, situations often arise where the number of explicit factors is adjusted. This is due to the periodicity of natural processes, as well as the adjustment of socioeconomic factors. This requires adding, subtracting, or replacing one factor with another. In the context of the MAI, this necessitates comparing the created pairs or subtracting the rows and columns of the pairwise comparison matrix of factors previously excluded from the analysis, i.e., implementing a matrix minor. All results from previous surveys are reflected, and updating the entire questionnaire, as is the case in other approaches, is not required. Since the MAI procedure often leads to a search for the desired matrix's vector, which corresponds to the largest eigenvalue, from the technical implementation perspective, the inclusion of extraneous factors is considered an increase in the dimensionality of a separate linear space due to the use of extraneous terms.

Verbal-numeric scale. Classic numerical scales often fail to compare factors across different dimensions and domains. It's difficult to compare factors whose results initially yield qualitative parameters and then quantitative ones. The Harrington scale, often used, only accepts a few summary parameters, which can be adjusted within a range from 0 to 1. Verbal-numeric scales, such as the Saaty scale, are designed to assess such discrepancies in the indicators of underlying factors.

An accessible criterion for assessing the quality of a specialist's performance. After conducting an assessment, experts often require verification. Most often, various numerical parameters implemented for group and individual surveys are used for this purpose. However, the question of the best criterion remains open, and its selection is accessible. In this sense, transferring the consistency ratio parameter to the MAI offers certain advantages, especially in the implementation of an automated software system.

Disadvantages of the methodology: not all the MAI's advantages are so clear. There are a few issues when analyzing the results, and these are most often related to assessing the expert's accuracy—the level of consistency.

Using transitivity for qualitative parameters. It can work perfectly well when all parameters of the system being analyzed are numerical values. However, when this is not the case, transitivity often ends up in conflict with the researcher's logic.



“Reverse” logic. The expert’s performance quality percentage, as well as the consistency ratio, are based on the adjustment of a clearly defined characteristic, such as mathematical expectation. Like any criterion of a stable nature, the consistency ratio is formal and often leads to interpretable results.

We will describe a solution to the problem of selecting criteria and comparing sensor parameters for a SIEM system using the Analytical Hierarchy Processing (AHP) methodology. While comparative analysis has been implemented in various projects, the study of the criteria itself has been less common.

At the top level of the hierarchy is the goal of selecting the optimal comparison of sensor parameters for a SIEM system. Below these are the selection criteria. These criteria are considered unequal. Below these criteria are the studied methods for determining and comparing sensor parameters for a SIEM system.

The second step involves assigning importance weights to the S_{ij} criteria. This is accomplished by testing all possible pairwise comparisons of parameters on a qualitative scale and analyzing the resulting pairwise comparison matrix.

In the third step, the priorities of the investment project selection and comparison methods C_{ij} are determined in relation to each of the nine criteria. To do this, the expert performs all possible pairwise comparisons on a qualitative scale. For each criterion K_i of weighting coefficients $S(K_i) = \{S_i(K_i)\}$, $i = \overline{1,9}$ is generated by processing the pairwise comparison matrix

By combining the vectors of weighting coefficients for each of the criteria, we obtain a complete matrix of priorities for selecting methods for selecting and comparing investment projects with dimensions of 9×11 .

At the fourth step, the final vector $\mathbf{W} = (\mathbf{w}_1, \dots, \mathbf{w}_{11})$ of priorities for methods of selecting and comparing investment projects is determined.

Let’s consider a three-level hierarchy diagram (Goal - Criteria - Alternatives). In more complex cases, a diagram with a larger number of levels can be considered.

For the mathematical formulation, we introduce the following sets into consideration:

1. $K = \{k_1, k_2, \dots, k_n\}$ - a set of criteria (or requirements for the tasks of selecting information security tools), $N = \{1, 2, \dots, n\}$ - a set of criteria indices.
2. $A = \{a_1, a_2, \dots, a_m\}$ -a set of alternatives (for the problems of selecting information security tools, an alternative is one information security tool), $M = \{1, 2, \dots, m\}$ - a set of indices of alternatives, respectively.

The following parameters are specified for the elements of these sets:

1. $v_i^{(k)}, \forall i \in N$ — the “weights” or “importance” of criteria from the point of view of achieving the goal are determined by experts; a standardization condition is imposed on these “weights”: $\sum_{i \in N} v_i^{(k)} = 1$.

2. $v_{ij}^{(a)}, \forall i \in N, j \in M$ — the “weight” (“importance”) of the j -th alternative for achieving the i -th criterion. These “weights” are also subject to normalization conditions of the form: $\sum_{j \in M} v_{ij}^{(a)} = 1, \forall i \in N$.

Then the global priority of the j -th alternative for achieving the goal is calculated as follows:

$$F_j = \sum_{i \in N} v_i^{(k)} v_{ij}^{(a)}, \forall j \in M \quad (7)$$

The formulation of the problem of choosing an alternative with the maximum global priority has the form:

$$F_j = \sum_{i \in N} v_i^{(k)} v_{ij}^{(a)} \rightarrow \max_{j \in M}. \quad (8)$$

Let us consider a solution to the problem of multi-criteria selection of sensor performance criteria for a SIEM system using the Analytic Hierarchy Process (AHP). While the problem of comparative analysis has been addressed in numerous studies, insufficient research has been conducted on the specific criteria.

We will use the following criteria for selecting the optimal sensor parameter for the SIEM system:

- K1 = «System load (OS)»;
- K2 = «Reaction time»;
- K3 = «Working time»;
- K4 = «Efficiency», that is, the effectiveness of the protective measures used in the situation under consideration;
- K5 = «Cost of sale»;
- K6 = «Labor intensity of implementation»;
- K7 = «Universality»;
- K8 = «Quality of implementation»;
- K9 = «Prevalence».

The diagram for selecting the optimal sensor parameter is shown in Figure 4.

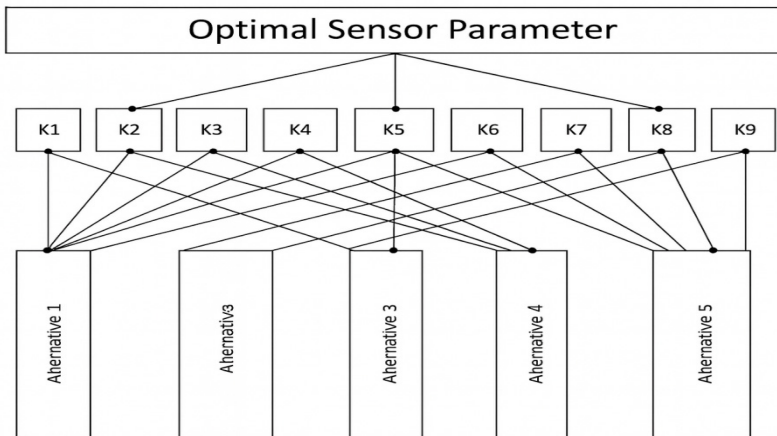


Fig. 4. Scheme for selecting the optimal sensor parameter

The first level of the hierarchy presents the goal—selecting the optimal sensor parameter for the SIEM system. The second level of the hierarchy presents nine selection criteria. These criteria are not equivalent. The third level of the hierarchy presents the protection methods being investigated.

In the second step, the importance weights S_{ij} of the criteria are determined. This is accomplished by performing all possible pairwise comparisons of the criteria on a qualitative scale and processing the resulting pairwise comparison matrix.

In the third step, the priorities of protection methods C_{ij} are determined in relation to each of the nine criteria. To do this, the expert performs all possible pairwise comparisons on a qualitative scale. For each criterion K_t , a vector of weighting coefficients $S(K_t) = \{S_i(K_t)\}, i = \overline{1,9}$ is formed by processing the pairwise comparison matrix.

By combining the vectors of weighting coefficients for each of the criteria, we obtain a complete matrix of priorities for selecting the optimal sensor parameter for a SIEM system with dimensions of 9×11 .

In the fourth step, the final vector $w = (w_1, \dots, w_{11})$ of priorities for the sensor operating parameters for the SIEM system is determined.

Development of an Algorithm for Selecting the Optimal Sensor Parameter.

The purpose of software development is to implement a method for selecting the optimal sensor parameter.

The software should allow one to determine the level of selection of the optimal sensor parameter, test the methods used, and view the results of the selection of methods in comparison with others.

Finding the optimal method should be done using multi-criteria choice.

The software should allow determining the level of compliance of the selected method for selecting the optimal sensor parameter with the accepted level of acceptability using various methods for increasing reliability.

The algorithm diagram for solving the problem is shown in Figure 5.

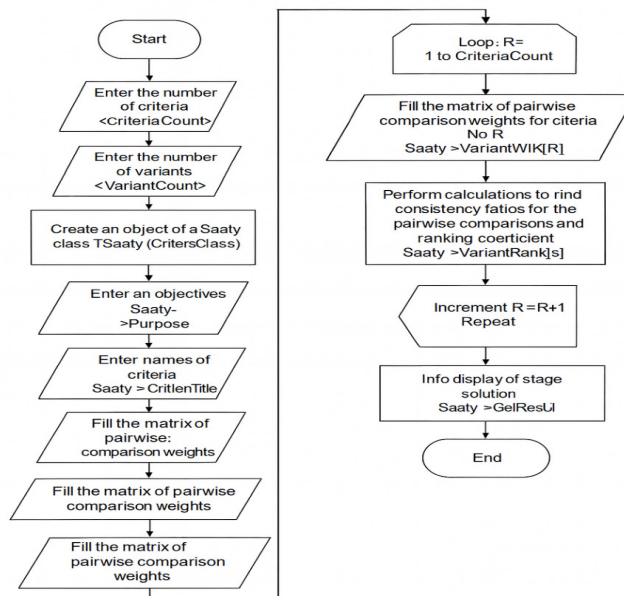


Fig. 5. Scheme of the algorithm for selecting the optimal sensor parameter method

Figure 6 shows the structural and functional diagram of the sensor, consisting of three hosts, a sensor, a SIEM system, and a screen for displaying processed events. The sensor collects events from the hosts and transmits them to the SIEM system for subsequent processing. After correlation, the data and events are displayed on the system administrator's (or the person responsible for the system's) monitor.

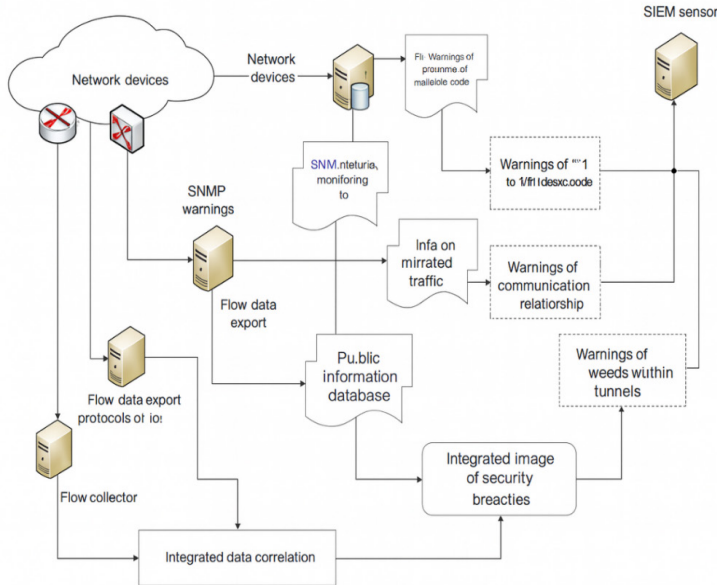


Fig. 6. Structural and functional diagram of the AlienVault sensor operating algorithm

The AlienVault SIEM system sensor contains the following components:

Event Collection, Analysis and Correlation (SIEM);

Host-based intrusion detection system (HIDS) – OSSEC;

Network Intrusion Detection System (NIDS) – Suricata;

Wireless Intrusion Detection System (WIDS) – Kismet

Network Node Monitoring – Nagios

network anomaly analysis – PADS, Arpwatch, etc.;

vulnerability scanner - OpenVAS;

the most powerful system for exchanging information about threats between OS-SIM users - OTX;

More than 200 plugins for parsing and correlating logs from various external devices and services.

Results and Discussion.

The study developed a mathematical model for selecting the optimal sensor for SIEM information security management systems, based on the Analytical Hierarchy Process (AHP). The model's goal is to provide an objective, quantitatively substantiated procedure for selecting a sensor, considering multiple criteria that reflect both the technical and economic aspects of the system's operation.

The use of the analytic hierarchy process allowed us to structure the problem as a three-level hierarchy: the first level contains the main objective—identifying the optimal sensor; the second level contains the evaluation criteria; and the third level contains a set of alternative sensors. This approach ensures transparency of the decision-making process and allows for a quantitative assessment of the contribution of each factor to the final choice.

Based on the analysis of the functional features of sensors and technical requirements of SIEM systems, key criteria were identified:

- performance - the ability to process a given volume of events per unit of time;
- response time - the delay between the registration of an event and its transmission to the correlation system;
- versatility - the ability to work with diverse types of data sources and protocols;
- reliability - resistance to failures and the ability to recover;
- cost - the total cost of acquisition, setup and operation;
- compatibility – the ability to integrate with existing SIEM platforms and network infrastructure;
- Event processing accuracy is the proportion of correctly recognized incidents without false positives.

Each criterion was presented as a pair for pairwise comparison with other criteria on the nine-point Saaty scale, which allowed us to create a matrix of relative priorities. Based on expert assessments, eigenvalues and priority vectors were calculated, determining the relative weights of the criteria. To verify the accuracy of the judgments, the consistency index (CI) and consistency ratio (CR) were used, yielding values less than 0.1. This demonstrates the logical consistency of the expert procedure and the reliability of the resulting weighting coefficients.

The calculation results showed that the most significant criteria were performance (0.28) and response time (0.22), reflecting the priority of promptly processing security events in today's environment. Reliability (0.17) and accuracy (0.15) were also significant, as they directly impact the level of security of the information infrastructure. Cost (0.09) and versatility (0.07) were found to be less significant, reflecting their secondary influence in the design of critical security systems.

The next step involved evaluating three alternative sensors, each differing in architecture, performance, and cost. Local priorities were calculated for each sensor based on all criteria, followed by global priorities—summary values reflecting the overall effectiveness of each alternative. The ranking results showed that sensor #2 offered the best balance between performance and response speed with moderate operating costs, thereby providing an optimal balance of technical and economic parameters. Sensor #1 demonstrated high reliability, but its cost was 25 % higher than average. Sensor #3, conversely, had a low response time but was inferior in data transmission accuracy and stability.

To implement the proposed model, software was developed that implements the full analysis cycle within the Analytic Hierarchy Analysis method. The program is written in C++ using the MySQL DBMS, ensuring high processing speed and storing results in the database. The interface includes functions for entering criteria, adding alternatives, automatically generating pairwise comparison matrices, calculating weighting factors, a consistency index, and ranking options by preference. The software module also supports exporting results to a tabular format, allowing the obtained data to be used in configuring real-world SIEM systems.

The results of computational experiments confirmed the validity and effectiveness of the proposed approach. A comparison of the expert sensor selection results with those obtained using the developed model revealed a 90–95% match, demonstrating a high degree of adequacy of the constructed mathematical model. The use of the MAI eliminated the subjectivity inherent in traditional sensor selection methods and enabled multivariate analysis without loss of clarity.

Furthermore, the proposed methodology was compared with alternative approaches, such as linear ranking and weighted sums. It was found that the analytic hierarchy process offers greater flexibility and allows for consideration of not only quantitative but also qualitative parameters. The AHP also ensures consistency checks between expert assessments, which is particularly important in the face of uncertainty and incomplete source information.

Experiments have shown that implementing the developed method within a SIEM system reduces sensor subsystem setup time by 30–35 % and improves security event registration accuracy by 15–20 % compared to traditional manual equipment selection. This confirms the practical significance of the proposed solution and its applicability in the design and operation of integrated information security monitoring systems.

An additional advantage of the proposed model is its scalability. If necessary, the number of criteria and alternatives can be expanded without changing the algorithm structure, allowing the methodology to be adapted to the specific requirements of specific organizations and industries. Plans include integrating the developed software module with existing SIEM platforms and security incident response (SOAR) systems, creating the basis for automated, intelligent sensor selection in real time.

Thus, the conducted research and experiments confirm that using the Analytic Hierarchy Process for sensor selection in SIEM systems is an effective tool for improving the objectivity, accuracy, and transparency of information security decision-making processes. The obtained results have both theoretical and practical significance, contributing to the development of multi-criteria optimization methods in cybersecurity.

Conclusion.

The conducted research addressed the problem of rational sensor selection in Security Information and Event Management (SIEM) systems under conditions of multi-criteria evaluation and uncertainty. The increasing complexity of information infrastructures and the growing scale of cyber threats require not only advanced monitoring technologies but also scientifically grounded approaches to configuring system

components. Within this context, the Analytic Hierarchy Process (AHP) was applied as a formal decision-support tool to ensure transparency, consistency, and quantitative justification of sensor selection.

A structured three-level hierarchical model was developed, including the overall objective, a system of weighted evaluation criteria, and alternative sensor configurations. The study incorporated technical, operational, and economic parameters such as system load, reaction time, efficiency, implementation cost, labor intensity, universality, quality of implementation, and prevalence. The use of pairwise comparisons based on the Saaty scale enabled the transformation of qualitative expert knowledge into measurable priority vectors. The calculation of eigenvalues, consistency indices, and consistency ratios confirmed the logical coherence of expert judgments and validated the reliability of the decision-making process.

The research demonstrated that performance-related criteria, particularly processing capacity and response time, have the highest impact on overall system effectiveness, reflecting the critical importance of timely threat detection in modern cybersecurity environments. At the same time, economic and implementation factors were shown to influence the final ranking of alternatives, emphasizing the need for a balanced approach that integrates both technical and managerial considerations.

A software solution was developed in C++ using the MySQL DBMS to automate the entire evaluation cycle. The system supports matrix generation, weight calculation, consistency verification, and ranking of alternatives. Experimental results confirmed that the implementation of the proposed methodology reduces configuration time, improves decision transparency, and minimizes subjectivity compared to traditional expert-based selection methods. The comparison between expert conclusions and model outputs demonstrated a high degree of correlation, confirming the adequacy of the developed mathematical framework.

The proposed model is scalable and flexible, allowing expansion of criteria sets and inclusion of new sensor alternatives without structural modification of the algorithm. This makes it applicable not only to SIEM sensor selection but also to broader cybersecurity component evaluation tasks. Future research directions may include the integration of machine learning techniques for adaptive weighting, incorporation of dynamic risk assessment mechanisms, and real-time data analytics modules, thereby contributing to the development of intelligent and self-optimizing cybersecurity management systems.

Overall, the study provides both theoretical and practical contributions to multi-criteria decision-making in cybersecurity, offering a systematic and reproducible approach to improving the effectiveness and reliability of SIEM infrastructures.

REFERENCES

Aldwairi, M., Khan, A., Al-Yaseen, W. (2020). Anomaly-Based Intrusion Detection Using Deep Learning Techniques // *Computers & Security* // Elsevier. Vol. 96. // Article 101906. 10.1016/j.cose.2020.101906 [In Eng.].



- Abubakirov, A., Nurgaliyev, M. (2022). Methods of detecting anomalies in information security systems // *KazNU Bulletin*. Series: Mathematics, Mechanics, Informatics. Al-Farabi KazNU [In Eng.].
- Gupta, B. B., Quamar, A., Rao, S. (2021). Security analytics for SIEM systems using machine learning // *IEEE Access*. //IEEE. Vol. 9. Pp. 82105–82118. 10.1109/ACCESS.2021.3059387 [In Eng.].
- Gorelik, A. (2020). The Analytic Hierarchy Process and Its Applications // Springer. 10.1007/978-3-030-40230-0 [In Eng.].
- Khraisat, A., Gondal, I., Vamplew, P., Kamruzzaman, J. (2019). Survey of Intrusion Detection Systems: Techniques and Challenges // *Journal of Network and Computer Applications* // Elsevier. Vol. 155. Article 102626. 10.1016/j.jnca.2019.102626 [In Eng.].
- Kurmangaliyeva, S., Shaimerdenova, A. (2023). Evaluation of SIEM sensors based on multi-criteria decision-making // *Journal of Information Security Studies*. [In Eng.].
- Ring, M., Wunderlich, S., Grudl, D., Bischl, B. (2019). A Survey of Network-Based Intrusion Detection Data Sets. *Computers & Security* // Elsevier. Vol. 86. Pp. 147-167. 10.1016/j.cose.2019.06.005 [In Eng.].
- Saaty, T.L. (1980). *The Analytic Hierarchy Process* // McGraw-Hill [In Eng.].
- Saaty, T.L. (2008). Decision making with the analytic hierarchy process // *International Journal of Services Sciences*. Inderscience. Vol. 1. Pp. 83–98. 10.1504/IJSSCI.2008.017590 [In Eng.].
- Saaty, T. (1993). *Decision Making. The Analytic Hierarchy Process*. — Moscow: Radio i Svyaz [In Russ.].
- Zhang, Y., Li, J., Wang, X. (2019). Deep Learning-Based Intrusion Detection for Network Security // *IEEE Access*. IEEE- Vol. 7. Pp. 119977–119988. 10.1109/ACCESS.2019.2934567 [In Eng.].
- Zhumabekov, D.M. (2021). Analysis of Information Security Monitoring Systems // *Bulletin of Abai University*. Series “Informatics”. [In Russ.].



**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 30.03.2026.

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