MINISTRY OF SCIENCE AND HIGHER EDUCATION OF THE REPUBLIC OF KAZAKHSTAN

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РЕСПУБЛИКИ КАЗАХСТАН

KAZAKHSTAN

ХАЛЫҚАРАЛЫҚ УНИВЕРСИТЕТІ

INTERNATIONAL UNIVERSITY SINCE 2009

МЕЖДУНАРОДНЫЙ УНИВЕРСИТЕТ

INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES

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

ХАЛЫҚАРАЛЫҚ АҚПАРАТТЫҚ ЖӘНЕ КОММУНИКАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАР ЖУРНАЛЫ

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

МЕЖДУНАРОДНЫЙ ЖУРНАЛ ИНФОРМАЦИОННЫХ И КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

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

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

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

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

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

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

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

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

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

РЕДАКЦИЯ

БАС РЕДАКТОР:

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

БАС РЕДАКТОРДЫҢ ОРЫНБАСАРЫ:

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

РЕДАКЦИЯЛЫҚ АЛҚА:

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

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

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

Микеле Пагано — PhD, Пиза Университетінің (Италия) профессоры

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

ЖАУАПТЫ РЕДАКТОР:

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

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

РЕДАКЦИЯ

ГЛАВНЫЙ РЕДАКТОР:

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

ЗАМЕСТИТЕЛЬ ГЛАВНОГО РЕДАКТОРА:

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

РЕДАКЦИОННАЯ КОЛЛЕГИЯ:

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

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

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

Микеле Пагано — PhD, профессор Университета Пизы (Италия)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

ОТВЕТСТВЕННЫЙ РЕДАКТОР:

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

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

CONTENTS

DIGITAL TECHNOLOGIES IN THE DEVELOPMENT OF SOCIO-ECONOMIC SYSTEMS

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

INFORMATION TECHNOLOGY

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

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

INFORMATION SECURITY AND COMMUNICATIONTECHNOLOGIES

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

МАЗМҰНЫ
ӘЛЕУМЕТТІК-ЭКОНОМИКАЛЫҚ ЖҮЙЕЛЕРДІ ДАМЫТУДАҒЫ ЦИФРЛЫҚ ТЕХНОЛОГИЯЛАР

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

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

АҚПАРАТТЫҚ ТЕХНОЛОГИЯЛАР

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

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

АҚПАРАТТЫҚ ҚАУІПСІЗДІК ЖӘНЕ КОММУНИКАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАРҒА АРНАЛҒАН

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

СОДЕРЖАНИЕ
ЦИФРОВЫЕ ТЕХНОЛОГИИ В РАЗВИТИИСОЦИО-ЭКОНОМИЧЕСКИХ СИСТЕМ

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

ИНТЕГРАТИВНАЯ МНОГОМЕРНАЯ МОДЕЛЬ 78

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

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

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

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ

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

INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Vol. 7. Is.3. Number 27 (2026). Pp. 512–528
Journal homepage: https://journal.iitu.edu.kz
https://doi.org/10.54309/IJICT.2026.27.3.028
МРНТИ 20.16.05

INFORMATION SECURITY IN GOVERNMENT CLOUD SERVICES: RISK ASSESSMENT AND PROTECTION STRATEGIES

G. Shangytbayeva[2], A.N. Amanov[3], M.K. Issenova[1], G.E. Berikkhanova[1], K.O. Shakerkhan[1*]
[1]Shakarim University, Semey, Kazakhstan;
[2]Zhubanov Aktobe Regional University, Aktobe, Kazakhstan;
[3]Khoja Akhmet Yassawi International Kazakh–Turkish University, Turkistan, Kazakhstan.
E-mail: q.shakerkhan@shkarim.kz

Gulmira Shangytbayeva — PhD, Associate Professor, Zhubanov Aktobe Regional University, Aktobe, Kazakhstan
https://orcid.org/0000–0003–4615–5756;
Anuarbek Amanov — PhD, Khoja Akhmet Yassawi International Kazakh–Turkish University, Turkestan, Kazakhstan
https://orcid.org/0000–0003–0638–6859;
Madina Isenova — Master of Pedagogical Sciences, Lecturer, Shakarim University, Semey, Kazakhstan
https://orcid.org/0009–0006–8551–5063;
Gulnaz Berikhanova — Doctor of Physical and Mathematical Sciences, Professor, Shakarim University, Semey, Kazakhstan
https://orcid.org/0000–0001–5013–1226;
Kapan Shakerhan — PhD, Shakarim University, Semey, Kazakhstan
E-mail: q.shakerhan@shakarim.kz, https://orcid.org/0000–0001–5013–1226.

© G. Shangytbayeva, A.N. Amanov, M.K. Issenova, G.E. Berikkhanova, K.O. Shakerkhan

Abstract. This article examines information security issues in cloud services of government bodies, risk assessment methods, and protection strategies. The relevance of this topic stems from the dichotomous conflict between economic efficiency and strict regulatory security requirements for government information resources within the three-tier cloud computing model—SaaS (software as a service), PaaS (platform as a service), and IaaS (infrastructure as a service)—as the primary factor determining the scientific and educational value of research. The integration of public sector entities into cloud computing infrastructure is considered a strategic priority for the purpose of optimizing operational costs associated with the use of information and communications

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

technologies and increasing the functional efficiency of e-government institutions. However, this process creates new risks and threats to data confidentiality, integrity, and availability. The study analyzes five main classes of cyber threats in cloud services (traditional attacks, functional attacks, client–side attacks, virtualization threats, complex threats). Modern methods of protecting virtual infrastructure (hypervisor protection, virtual machine migration control, management system protection) are described. Prospective cloud security technologies – self–protected data and trusted monitors – are considered. The relevance of the study is confirmed by the increasing frequency of targeted cyberattacks on cloud infrastructures and the lack of unified risk assessment methodologies for hybrid environments that take into account national specifics. The object of the research is cloud services within the government administration perimeter, and the subject is the methodology for assessing risk factors and approaches to creating a multi–level security architecture. The aim of the work is to develop an adaptive risk assessment model and formulate practical protection strategies for government cloud platforms.

Keywords: cloud computing, information security, public sector, cyber threats, virtualization, Hyper–V, risk assessment

For citation: Shangytbayeva G., Amanov A.N., Issenova M.K., Berikkhanova G.E., Shakerkhan K.O. (2026). Information security in government cloud services: risk assessment and protection strategies // International journal of information and communication technologies. Vol. 7. No. 27. Pp. 512–528. https://doi.org/10.54309/IJICT.2026.27.3.028. (In Kaz.).

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

МЕМЛЕКЕТТІК ОРГАНДАРДЫҢ БҰЛТТЫ СЕРВИСТЕРІНДЕГІ АҚПАРАТТЫҚ ҚАУІПСІЗДІК: ТӘУЕКЕЛДЕРДІ БАҒАЛАУ ЖӘНЕ ҚОРҒАУ СТРАТЕГИЯЛАРЫ

Г.А. Шангытбаева[2], А.Н. Аманов[3], М.К. Исенова[1], Г.Е. Берикханова[1], Қ.О. Шакерхан[1*]

[1]Шәкәрім университеті, Семей, Казақстан;
[2]Қ. Жұбанов атындағы Ақтөбе өңірлік университеті, Ақтөбе, Қазақстан;
[3]Қожа Ахмет Яссауи атын. Халықаралық Қазақ–Түрік Университеті, Түркістан, Қазақстан.
E-mail: q.shakerkhan@shkarim.kz

Шангытбаева Гүлмира — PhD доктор, қауымдастырылған профессор, Қ. Жұбанов атындағы Ақтөбе өңірлік университеті, Ақтөбе, Қазақстан
https://orcid.org/0000–0003–4615–5756;
Аманов Ануарбек — PhD доктор, Қожа Ахмет Яссауи атын. Халықаралық Қазақ–Түрік Университеті, Түркістан, Қазақстан
https://orcid.org/0000–0003–0638–6859;
Исенова Мадина — педагогика ғылымдарының магистрі, оқытушысы, Шәкәрім Университеті, Семей, Қазақстан

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

https://orcid.org/0009–0006–8551–5063;
Берикханова Гүлназ — ф–м.ғ.д., профессор, Шәкәрім Университеті, Семей, Қазақстан
https://orcid.org/ 0000–0001–5013–1226;
Шакерхан Қапан — PhD доктор, Шәкәрім университеті, Семей, Қазақстан
E-mail: q.shakerhan@shakarim.kz, https://orcid.org/0000–0001–5013–1226.

© Г.А. Шангытбаева, А.Н. Аманов, М.К. Исенова, Г.Е. Берикханова, Қ.О. Шакерхан

Аннотация. Бұл мақалада мемлекеттік органдардың бұлтты сервистеріндегі ақпараттық қауіпсіздік мәселелері, тәуекелдерді бағалау әдістері және қорғау стратегиялары қарастырылады. Тақырыптың өзектілігі зерттеу жұмысының ғылыми-танымдық мәнін айқындайтын негізгі фактор ретінде бұлтты есептеу технологияларының үш деңгейлі моделі – SaaS (бағдарламалық қамтамасыз ету қызмет ретінде), PaaS (платформа қызмет ретінде) және IaaS (инфрақұрылым қызмет ретінде) – аясындағы экономикалық тиімділік пен мемлекеттік ақпараттық ресурстарға қойылатын қатаң реттеушілік қауіпсіздік талаптары арасындағы туындайтын дихотомиялық қайшылықтан туындап отыр. Мемлекеттік сектор субъектілерінің бұлтты есептеу инфрақұрылымына интеграциялануы ақпараттық-коммуникациялық технологияларды пайдаланумен байланысты операциялық шығындарды оңтайландыру және электрондық үкімет институтының функционалдық тиімділігін арттыру мақсатындағы стратегиялық басымдық ретінде қарастырылады. Алайда, бұл процесс деректердің құпиялылығына, тұтастығына және қолжетімділігіне байланысты жаңа қауіптер мен тәуекелдерді туғызады. Зерттеу барысында бұлтты сервистердегі киберқауіптердің бес негізгі класы (дәстүрлі атакалар, функционалды атакалар, клиентке атакалар, виртуалдауға атакалар, кешенді атакалар) талданды. Виртуалды инфрақұрылымды қорғаудың заманауи әдістері (гипервизорды қорғау, виртуалды машиналарды көшіруді қадағалау, басқару жүйелерін қорғау) сипатталды. Болашақтың бұлтты қауіпсіздік технологиялары – самозащищенные деректер және сенімді мониторлар қарастырылды. Зерттеудің өзектілігі бұлтты инфрақұрылымдарға бағытталған кибершабуылдар жиілігінің артуымен және ұлттық ерекшелікті ескеретін гибридті орталар үшін тәуекелдерді бағалаудың бірыңғай әдістемелерінің болмауымен расталады. Зерттеу нысаны мемлекеттік басқару контурындағы бұлтты сервистер, пәні – тәуекел факторларын бағалау әдіснамасы және көп деңгейлі қорғау архитектурасын құру тәсілдері болып табылады. Жұмыстың мақсаты – тәуекелдерді бағалаудың адаптивті моделін әзірлеу және мемлекеттік бұлтты платформалар үшін практикалық қорғау стратегияларын тұжырымдау.

Түйінді сөздер: бұлтты есептеулер, ақпараттық қауіпсіздік, мемлекеттік сектор, киберқауіптер, виртуалдау, Hyper–V, тәуекелдерді бағалау

Дәйексөздер үшін: Шангытбаева Г.А., Аманов А.Н., Исенова М.К., Берикханова Г.Е., Шакерхан Қ.О. (2026). Мемлекеттік органдардың бұлтты сервистеріндегі ақпараттық қауіпсіздік: тәуекелдерді бағалау және қорғау

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

стратегиялары // Халықаралық ақпараттық және коммуникациялық технологиялар журналы. Т. 7. No 27. Б. 512–528. https://doi.org/10.54309/IJICT.2026.27.3.028. (Қаз. тіл.).

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

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ОБЛАЧНЫХ СЕРВИСАХ ГОСУДАРСТВЕННЫХ ОРГАНОВ: ОЦЕНКА РИСКОВ И СТРАТЕГИИ ЗАЩИТЫ

Г.А. Шангытбаева[2], А.Н. Аманов[3], М.К. Исенова[1], Г.Е. Берикханова[1], Қ.О. Шакерхан[1*]

[1]Университет Шакарима, Семей, Казахстан;

[2]Актюбинский региональный университет имени К.Жубанова, Актобе, Казахстан;

[3]Международный казахско–турецкий университет им. Ходжа Ахмета Яссауи, Туркестан, Казахстан.

E-mail: q.shakerkhan@shkarim.kz

Шангытбаева Гульмира — доктор PhD, ассоциированный профессор, Актюбинский региональный университет имени К.Жубанова, Актобе, Казахстан https://orcid.org/0000–0003–4615–5756;

Аманов Ануарбек — доктор PhD, Международный казахско–турецкий университет им. Ходжи Ахмета Яссави, Туркестан, Казахстан https://orcid.org/0000–0003–0638–6859;

Исенова Мадина — магистр педагогических наук, преподаватель, Университет Шакарима, Семей, Казахстан https://orcid.org/0009–0006–8551–5063;

Бериханова Гульназ — доктор физико–математических наук, профессор, Университет Шакарима, Семей, Казахстан https://orcid.org/ 0000–0001–5013–1226;

Шакерхан Капан — доктор PhD, Университет Шакарима, Семей, Казахстан E-mail: q.shakerkhan@shkarim.kz, https://orcid.org/0000–0001–5013–1226.

© Г.А. Шангытбаева, А.Н. Аманов, М.К. Исенова, Г.Е. Берикханова, Қ.О. Шакерхан

Аннотация. В данной статье рассматриваются вопросы информационной безопасности в облачных сервисах государственных органов, методы оценки рисков и стратегии защиты. Актуальность темы обусловлена дихотомическим конфликтом, возникающим между экономической эффективностью и строгими требованиями нормативной безопасности государственных информационных ресурсов в рамках трехуровневой модели облачных вычислительных технологий — SaaS (программное обеспечение как услуга), PaaS (платформа как услуга) и

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

IaaS (инфраструктура как услуга) — как основным фактором, определяющим научную и познавательную ценность исследовательской работы. Интеграция субъектов государственного сектора в инфраструктуру облачных вычислений рассматривается как стратегический приоритет с целью оптимизации операционных затрат, связанных с использованием информационно-коммуникационных технологий, и повышения функциональной эффективности института электронного правительства. Однако этот процесс порождает новые риски и угрозы конфиденциальности, целостности и доступности данных. В ходе исследования проанализированы пять основных классов киберугроз в облачных сервисах (традиционные атаки, функциональные атаки, атаки на клиента, угрозы виртуализации, комплексные угрозы). Описаны современные методы защиты виртуальной инфраструктуры (защита гипервизора, контроль миграции виртуальных машин, защита систем управления). Рассмотрены перспективные технологии облачной безопасности – самозащищенные данные и доверенные мониторы. Актуальность исследования подтверждается нарастающей частотой целевых кибератак на облачные инфраструктуры и отсутствием унифицированных методик оценки рисков для гибридных сред с учетом национальной специфики. Объектом исследования являются облачные сервисы в контуре государственного управления, предметом – методология оценки факторов риска и подходы к созданию многоуровневой архитектуры защиты. Цель работы заключается в разработке адаптивной модели оценки рисков и формулировании практических стратегий защиты для государственных облачных платформ.

Ключевые слова: облачные вычисления, информационная безопасность, государственный сектор, киберугрозы, виртуализация, Hyper–V, оценка рисков

Для цитирования: Шангытбаева Г.А., Аманов А.Н., Исенова М.К., Берикханова Г.Е., Шакерхан Қ.О. (2026). Информационная безопасность в облачных сервисах государственных органов: оценка рисков и стратегии защиты // Международный журнал информационных и коммуникационных технологий. Т. 7. No. 27. Стр. 512–528. https://doi.org/10.54309/IJICT.2026.27.3.028. (На каз.).

Конфликт интересов: авторы заявляют об отсутствии конфликта интересов.

Кіріспе.

Қазіргі уақытта IT–индустриясында ақпараттық технологияларды дамытудың төрт негізгі үрдісі бар: бұлтты технологиялар, пайдаланушылардың мобильділігі, үлкен деректер (big data) және әлеуметтік жүйелер. Бұлтты есептеулер ақпараттық жүйелердің эволюциялық дамуындағы сапалық жаңа кезеңді білдіреді. Мемлекеттік органдардың осы технологиялық платформаға көшуі Қазақстан Республикасы Үкіметінің ұзақмерзімді цифрлық трансформация стратегиясындағы басым бағыттардың бірі ретінде айқындалады. Мұндай көшудің тиімділігі электрондық үкімет жүйесінің функционалдық нәтижелігін арттыру, құжат айналымы процестерінің жеделдігін қамтамасыз ету, ақпараттық қауіпсіздік деңгейінің сенімділігін күшейту, сондай-ақ ақпараттық-

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

коммуникациялық инфрақұрылымды ұстауға кететін шығындарды елеулі төмендету арқылы жүзеге асырылады.

Дегенмен, мемлекеттік секторда бұлттық сервистерді енгізу процесі жаңа сын-қатерлер мен тәуекелдік факторлардың туындауына себеп болмақ. Атап айтқанда, ақпараттық қауіпсіздікті қамтамасыз ету мәселелері осы технологияларды мемлекеттік басқару саласына енгізуді тежейтін негізгі кедергілердің бірі болып табылады. Бұл жағдай қауіпсіздік талаптары мен технологиялық мүмкіндіктер арасындағы теңгерімді іздестіруді ғылыми-қолданбалы зерттеулердің өзекті бағытына айналдырады.

Зерттеулер көрсеткендей, интернет пайдаланушылардың 78%–ы өздерінің компьютерлік жүйелерін желілік шабуылдардан қалай қорғау керектігін білмейді. Бұл мемлекеттік органдар үшін ақпараттық қауіпсіздік мәселелерін тереңдетіп зерделеудің маңыздылығын көрсетеді (Kudra et al., 2011)

Зерттеудің мақсаты – мемлекеттік органдардың бұлтты сервистеріндегі ақпараттық қауіпсіздік тәуекелдерін бағалау және қорғау стратегияларын әзірлеу.

Зерттеудің міндеттері:

- бұлтты сервистердегі киберқауіптерді классификациялау;
- виртуалды инфрақұрылымды қорғаудың заманауи әдістерін талдау;
- болашақтың бұлтты қауіпсіздік технологияларын зерттеу;
- мемлекеттік органдар үшін бұлтты провайдерді таңдау критерийлерін әзірлеу.

Бұл тақырыптың негіздемесі көп пәтерлілік және жауапкершілікті бөлу қағидаттарына негізделген қоғамдық бұлттық архитектура мен ұлттық заңнама талаптары арасындағы негізгі қарама–қайшылыққа негізделген. Мақалада көрсетілгендей, қаржылық емес тәуекел санаттары мемлекеттік органдар үшін бірінші кезектегі мәселе болып табылады: әлеуметтік–саяси тұрақтылық, мемлекеттік егемендікті сақтау және қорғаныс қабілеті. Бұл зерттеудің нысаны – мемлекеттік органдарда орналастырылған бұлттық қызметтер (SaaS, PaaS, IaaS), ал тақырыбы – тәуекелдерді бағалау әдіснамасы және қауіпсіздік архитектурасы. Бұл жұмыстың практикалық маңыздылығы Қазақстан үкіметінің ҚазақстанVүкіметінің мемлекеттік органдардың бүкіл IT инфрақұрылымын мемлекеттік қызметтерді көрсетуге қатысты өзекті мәселелерді шешетін, электрондық үкіметті жетілдіретін, мемлекеттік органдар арасындағы электрондық құжат айналымының жылдамдығын арттыратын, ақпараттық қауіпсіздіктің жоғары сенімділігін қамтамасыз ететін және IT инфрақұрылымының қымбат қаржылық шығындарын азайтатын инновациялық технологиялардың жаңа моделіне көшіру мәселесін көтеруінде жатыр. Сондықтан, практикалық маңыздылығы Қазақстан үкіметінің бүкіл IT инфрақұрылымын бұлттық технологияларға көшіру үшін бұлтты есептеу платформаларын таңдау мәселесін шешу, осылайша мемлекеттік органдардың жоғарыда аталған барлық IT мәселелерін шешу болып табылады (Armbrust et al., 2010)

Әдістер мен материалдар.

Бұлттық қауіпсіздік – бұлттық инфрақұрылымды сынға алушылар

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

көтерген негізгі мәселелердің бірі. Көпшілік үшін деректерін бұлттағы компьютерлерге жылжыту эмоционалды түрде мазасыздық тудыруы мүмкін, онда олар оны басқара алмайды. Сонымен қатар, бұл тәсіл сәйкестікті және әртүрлі реттеуші аспектілерді ескеруді талап етеді. Алайда, шын мәнінде, бұлттық орта дәстүрлі деректер орталығынан кем емес, тіпті одан да қауіпсіз болуы мүмкін. Дегенмен, бұлттық ортамен жұмыс істеген кезде ақпараттық қауіпсіздікке деген көзқарасыңыз дәстүрлі ортада үйреніп қалған тәсіліңізден түбегейлі өзгеше болады. Онлайн ақпараттық қауіпсіздік бүгінгі таңда әрбір пайдаланушыға әсер ететін өзекті мәселе болып қала береді. Сондай–ақ, сауалнамаға қатысқан интернет пайдаланушыларының 78%–ы компьютерлік жүйелерін әртүрлі желілік шабуылдардан қалай қорғау керектігін білмейтінін мойындағанын атап өткен жөн. Сондықтан, бұлттық есептеулерге көшу туралы шешім қабылдаған кезде, ақпараттық қауіпсіздіктің маңызды аспектілері бұлттық провайдерлермен толығымен қамтылғанын түсінуіңіз керек.

Сіздің бизнесіңізге ешқандай қатысы жоқ, бірақ деректеріңіздің қауіпсіздігіне айтарлықтай қауіп төндіруі мүмкін сыртқы факторлар бар. Мысалы, келесі оқиғалардың кез келгені сіздің инфрақұрылымыңызда мәселелер тудыруы мүмкін (Barham et al., 2017)

• Сізге бұлттық қызметтерді ұсынатын компания банкрот деп жарияланады, оның активтері (серверлерді қоса алғанда) тәркіленеді және провайдер қызмет көрсетуді тоқтатады.

• Сізге қатысы жоқ үшінші тарап (немесе одан да жаманы, бәсекелес) сіздің бұлттық провайдеріңізге сотқа береді және сот арқылы бұлттық провайдерге тиесілі барлық серверлерге толық қол жеткізеді.

• Сіздің бұлттық провайдеріңіздің инфрақұрылым компоненттерін, әсіресе физикалық қол жеткізуді басқаруға келгенде, жеткілікті түрде қорғай алмауы сіздің жүйелеріңізге қауіп төндіруі мүмкін.

Келесі қадамдар кез келген жағдайда қабылдауға болатын, бірақ көптеген пайдаланушылар жиі бағаламайтын осы мәселелерді шешуге көмектеседі:

Барлық ақпаратты, барлық желілік байланыстарды шифрлаңыз және қашықтан сақтық көшірмелер жасаңыз (бұл мақсатта коммерциялық және ашық бастапқы кодты шешімдер бар). Бұл сіздің бұлт провайдеріңіз жоғалып кетсе де, ағымдағы және тарихи деректердің қалпына келуін қамтамасыз етеді.

Барлық мүмкін сценарийлер үшін аталған шараларды қолдануды қарастырайық:

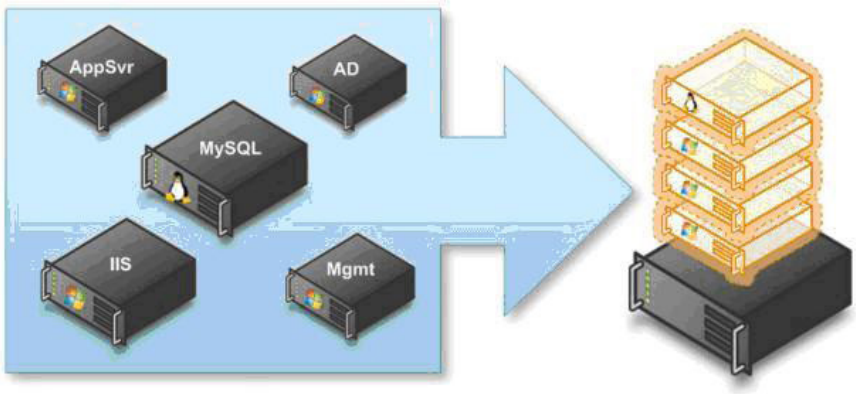
1. Бұлттық қызмет провайдері банкротқа ұшыраса не болады ?

Бұл сценарий үшін бірнеше мүмкін сценарийлер бар: банкроттық, басқа қызмет саласына қайта назар аудару үшін бизнестің жабылуы немесе электр қуатының кең көлемді және ұзаққа созылған үзілуіне байланысты ұзақ уақытқа тоқтап қалу. Нәтижесіне қарамастан, сіз басқа компанияның әрекеттеріне байланысты өндірістік жүйелеріңізге қол жеткізу мүмкіндігін жоғалту қаупін тудырасыз. Сонымен қатар, сіз деректеріңізді басқаратын ұйымның бұрын жасалған қызмет көрсету деңгейі туралы келісімдерге сәйкес оны қорғай алмау

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

қаупін тудырасыз (1 сур., қара).

Бұл жағдайда ең маңызды аспект – қашықтан сақтық көшірмелерді үнемі жасау және сақтық көшірмелерді өндірістік ортаңыздан тыс сақтау. Бұл шара сізді бұлт провайдеріңіздің тоқтап қалуының теріс салдарынан қорғауы керек. Одан да жақсысы, ауыстыру инфрақұрылымын іске қоса алатын екінші бұлт провайдерін пайдаланыңыз. (Ванина т.б., 2015)



Сур. 1. Серверді виртуалдандыру

2. Бұлттық қызмет провайдеріңізді деректеріңізді жариялауға мәжбүрлейтін сотқа шақыру қағазы түскенде не болады?

Әрине, егер сіз сот ісіне қатысып, сотқа шақыру қағазы тікелей сізге жолданса, сіз сақтық шараларын қабылдағаныңызға және деректеріңіз бұлттық ортада немесе өзіңіздің IT инфрақұрылымыңызда сақталғанына қарамастан, деректерді соттарға беруге міндеттісіз. Дегенмен, біз мұнда басқа сценарийді қарастырып жатырмыз – сотқа шақыру қағазы сізге емес, сіздің бұлттық провайдеріңізге жолданған және сіз сот ісіне қатыспаған және онымен ешқандай байланысыңыз болмаған жағдай.

Таза техникалық тұрғыдан алғанда, сотқа шақыру қағазы мәселелердің тар ауқымын қамтуы және сізге әсер етпеуі керек. Дегенмен, бәсекелес фирмалар арасындағы дамып келе жатқан технологиялардағы басымдықтарға қатысты дауларға қатысты сотқа шақыру қағаздарының дұрыс тұжырымдалатынына, атап айтқанда, мүдделі тараптардың жеткілікті тар шеңберін қамтитындай етіп жазылатынына толық сенімді бола алмайсыз. Сонымен қатар, сотқа шақыру қағазы берілгенін білетініңізге сенімді бола алмайсыз.

Деректеріңізді толық шифрлау ғана сізді бұл жағдайдан қорғайды. Шақыру қағазы сіздің бұлт провайдеріңізден сотқа деректеріңізді және оған кіру мүмкіндігін беруді талап етуі мүмкін, бірақ провайдерде сіздің кіру кілтіңіз немесе шифрды ашу кілтіңіз болмайды. Оларды алу үшін сот сізбен байланысып, шақыру қағазын шығаруы керек. Нәтижесінде, сіз бұлттағы деректеріңізді өзіңіздің жеке деректер орталығыңыздағыдай бақылау деңгейіне ие боласыз.

3. Бұлттық қызмет провайдері өз желісі үшін тиісті қауіпсіздікті қамтамасыз ете алмаса, не болады?

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

Бұлт провайдерін таңдаған кезде, олардың физикалық қауіпсіздігімен және олардың желісі мен жеке хосттарын қорғауды қалай ұйымдастыратынымен танысуыңыз керек. Қаншалықты парадоксалды болып көрінсе де, ең қауіпсіз бұлт провайдері – сіз ешқашан бұл ақпаратты ала алмайтын және виртуалды дананы іске қосатын сервердің физикалық орналасқан жерін біле алмайтын провайдер. Егер сіз мұны болжай алмасаңыз да, сіздің ұйымыңыз туралы ақпарат жинайтын арнайы шабуылдаушы сіздің хостингіңізді қамтамасыз ететін ортаның физикалық орналасқан жерін анықтауға тырысқанда осындай қиындықтарға тап болуы мүмкін (Abdaly, 2021)

Бүгінгі таңда бұлттық қауіпсіздік саласындағы жетекші сарапшы – Cloud Security Alliance (CSA). Бұл ұйым бұлттық есептеу тәуекелдерін бағалау кезінде ескеру қажет жүздеген нюанстар мен ұсыныстарды сипаттайтын нұсқаулық шығарды және жақында жаңартты. Нұсқаулық 76 беттен тұрады және сізді осындай ұзақ құжатты оқу қиындықтарынан құтқару үшін, онда әлеуетті бұлттық қызмет провайдеріне алдымен қою керек ең маңызды сұрақтар көрсетілген. Сондай–ақ, онда сіз күтуіңіз керек жауаптар берілген. Бұлттық қауіпсіздік аспектілерін қамтитын тағы бір ұйым – Trusted Computing Group (TCG), ол осы және басқа салалардағы бірнеше стандарттардың, соның ішінде кеңінен қолданылатын Trusted Storage, Trusted Network Connect (TNC) және Trusted Platform Module (TPM) стандарттарының авторы.

Келесі сұрақтар сіз кімнің бұлттық қызметтерін пайдалануды жоспарлап отырған провайдерге қоюға болатын негізгі сұрақтар болып табылады. Қойылған мәселелердің шешімін табу барысында стандарттау негізіндегі тәсілдерді қолданудың тиімділігін алдын ала саралау қажет. Бұл ұстаным ақпараттық қауіпсіздікті қамтамасыз етудің барлық деңгейлеріне ортақ сипатқа ие. Зерттеулер мен практикалық тәжірибе көрсеткендей, меншіктік (проприетарлық) архитектуралар ашық стандарттарға негізделген жүйелермен салыстырғанда қорғаныс механизмдерінің төменгі сенімділік деңгейін қамтамасыз етеді. Бұл бағалау нарық субъектілерінің, мемлекеттік институттардың және стандарттау жөніндегі уәкілетті органдардың кең ауқымды консенсусы ретінде қалыптасқан және салалық қауымдастық тарапынан жалпы мойындалған методологиялық принцип болып табылады. Міне, сондықтан Advanced Encryption Standard (AES) және Transport Layer Security (TLS) сияқты стандарттар кең таралған. Олар жылдар бойы талдау мен жетілдіруден өтті. Сонымен қатар, жалпы қабылданған стандарттарға негізделген қауіпсіздік жүйелерін пайдалану арқылы тұтынушылар қажет болған жағдайда қызмет көрсетушілерді ауыстыра алу мүмкіндігінің қосымша артықшылығына ие болады, себебі көптеген провайдерлер стандартталған шешімдерді қолдайды. Тағы бір нақтылауға тұрарлық мәселе: провайдеріңіздің өз уәделерін орындауын қалай қамтамасыз ете аласыз? Қызмет көрсету деңгейі туралы келісім (SLA), келісімшарт немесе провайдердің міндеттемелерін анық көрсететін басқа жазбаша құжат сізге мұны жүзеге асыруға көмектеседі (Трофименко, 2020)

Әрі қарай, жалпыдан нақтыға дейінгі бірқатар сұрақтарды қарастырайық,

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

оларды нақтылауға тұрарлық:

1. Сақталған деректердің қауіпсіздігі.

Қызмет көрсетуші сақталған деректердің қауіпсіздігін қалай қамтамасыз етеді?

Сақталған деректерді қорғаудың ең жақсы шарасы – шифрлау технологияларын пайдалану. Қызмет көрсетуші рұқсатсыз кірудің алдын алу үшін өз серверлерінде сақталған клиенттік ақпаратты әрқашан шифрлауы керек. Қызмет көрсетуші сонымен қатар деректерді қажет етпейтін және болашақта қажет болмайтын кезде оларды біржола жоюы керек.

2. Тасымалдау кезінде деректерді қорғау.

Провайдер тасымалдау кезіндегі деректердің қауіпсіздігін қалай қамтамасыз етеді (бұлт ішінде және бұлтқа/бұлттан жолда)?

Берілген деректер әрқашан шифрлануы және пайдаланушыға тек аутентификациядан кейін ғана қолжетімді болуы керек. Бұл тәсіл ешкімнің бұл деректерді өзгерте немесе оқи алмайтынына кепілдік береді, тіпті олар желідегі сенімсіз түйіндер арқылы қол жеткізсе де. Бұл технологиялар көптеген жылдар бойы әзірленді және сенімді хаттамалар мен алгоритмдердің (мысалы, TLS, IPsec және AES) жасалуына әкелді. Провайдерлер өз хаттамаларын қолданудың орнына осы хаттамаларды еңгізу керек.

3. Аутентификация.

Бұлттық сервис провайдерінің клиенттің жеке басын сәйкестендіру механизмі негізгі қауіпсіздік факторларының бірі болып табылады. Аутентификацияның кең таралған тәсілі ретінде парольдік қорғаныс қолданылады, алайда қауіпсіздік деңгейін күшейту мақсатында провайдерлер сертификаттар мен токендер сияқты күшейтілген аутентификация құралдарын енгізуге бет бұруда. Сонымен қатар, провайдердің LDAP және SAML сияқты салалық стандарттармен үйлесімділігі клиенттің ішкі пайдаланушыларды басқару жүйесімен интеграциялану және авторизация процестерін автоматтандыру тұрғысынан маңызды болып табылады. Бұл провайдердің уәкілетті пайдаланушылар туралы деректердің өзектілігін үздіксіз қамтамасыз етуіне мүмкіндік береді. Ең қолайсыз сценарий ретінде клиенттің провайдерге уәкілетті тұлғалардың статикалық тізімін ұсынуы қарастырылады, мұндай жағдай қызметкерлердің кадрлық өзгерістері (жұмыстан босату, лауазымдық ауысу) кезінде басқарушылық қиындықтар туғызуы мүмкін (Augustine et al., 2025).

4. Пайдаланушыны оқшаулау.

Бір клиентке тиесілі деректер мен қолданбалардың басқа клиенттердің тиісті ресурстарынан бөлінуі міндетті талап болып табылады. Осы тұрғыда ең тиімді шешім әрбір клиент үшін бөлек виртуалды машина (VM) және виртуалды желілік инфрақұрылымды пайдалану болып саналады. Виртуалды машиналар арасындағы шектеуді гипервизорлар қамтамасыз етсе, виртуалды желілер VLAN, VPLS және VPN секілді стандартталған технологиялар негізінде құрылады. Кейбір провайдерлер барлық клиенттердің деректерін ортақ бағдарламалық

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

ортада орналастырып, бағдарламалық кодты өзгерту арқылы оқшаулауға тырысады. Алайда, бұл тәсіл сенімсіз және қауіпті деп бағаланады. Біріншіден, стандартты емес кодта осалдықтар болуы мүмкін, олар шабуылдаушыға рұқсатсыз деректерге қол жеткізуге жол ашады. Екіншіден, бағдарламалау қателері бір клиенттің басқа клиенттің ақпаратын кездейсоқ қарауына әкеп соғуы мүмкін. Соңғы кезеңде екі жағдай да тіркелген. Осы себепті, пайдаланушы деректерін тиімді бөлу үшін бөлек виртуалды машиналар мен виртуалды желілерді қолдану неғұрлым сенімді әрі ғылыми негізделген шешім болып табылады.

5. Нормативті–реттеуші мәселелер.

Бұлтты есептеулер саласындағы провайдердің заңнамалық және реттеуші талаптарға сәйкестігі маңызды критерийлердің бірі ретінде қарастырылады. Қолданыстағы заңдар мен ережелер юрисдикцияға қарай елеулі түрде дифференцияланады: олар деректерді трансшекаралық тасымалдауға тыйым салуды, қауіпсіздік шараларының нақты деңгейін, белгілі бір стандарттарды міндетті сақтауды және аудит жүргізу мүмкіндігін талап етуі мүмкін. Сонымен қатар, құқықтық нормалар мемлекеттік органдар мен сот инстанцияларының ақпаратқа қол жеткізуін регламенттейді. Провайдер тарапынан осы талаптарды елемеу клиенттер үшін елеулі заңдық салдарлар мен қаржылық шығындарға әкелуі мүмкін. Провайдер қатаң реттеуші стандарттарды сақтауға және бірыңғай құқықтық стратегияны ұстануға міндетті. Бұл міндеттемелер пайдаланушы деректерінің құпиялылығын, оларды экспорттау шарттарын, салалық стандарттарға сәйкестікті, аудит өткізу тәртібін, деректерді сақтау және жою рәсімдерін, сондай-ақ ақпаратты жария ету жағдайларын (әсіресе бірнеше клиенттердің деректері бір физикалық серверде сақталған кезде өзекті) қамтиды.

6. Оқиғаға жауап беру.

Қызмет көрсетуші оқиғаларға қалай жауап береді және олардың тұтынушылары қаншалықты қатысуы мүмкін?

Кейде істер жоспар бойынша жүрмейді. Осыған орай, сервис провайдерлерінің дағдарыстық жағдайлардағы іс-әрекеттері алдын ала белгіленген және тиісті түрде құжатталған мінез-құлық регламенттеріне негізделуі тиіс. Бұл регламенттер инциденттерді дер кезінде анықтау, олардың теріс салдарларын локализациялау және олардың әсер ету дәрежесін барынша төмендету, сондай-ақ пайдаланушыларды туындаған жағдай туралы уақтылы және толық ақпараттандыру сияқты процедуралық міндеттемелерді қамтуы қажет. Аталмыш шаралар провайдерлердің операциялық тұрақтылығы мен клиенттер алдындағы ашықтығын қамтамасыз етудің негізгі механизмдері болып табылады. Ең дұрысы, олар тұтынушыларға мәселе бойынша үнемі егжей–тегжейлі ақпарат беруі керек. Сонымен қатар, тұтынушылар қауіпсіздік мәселелерінің ықтималдығын бағалап, тиісті шаралар қабылдауы керек (Robert, 2010)

Нәтижелер және оларды талқылау.

Бұлтты технологиялар дамыған сайын киберқауіптер де қатар дамып келеді. Келесі қауіп кластарын ажырату керек:

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

Дәстүрлі бағдарламалық жасақтама шабуылдары. Желілік хаттамалардағы, операциялық жүйелердегі, модульдік компоненттердегі және басқа да деңгейлердегі осалдықтар дәстүрлі ақпараттық қауіпсіздік тәуекелдерінің санатына жатады. Осыған орай, оларға қарсы антивирустық бағдарламалық қамтамасыз ету, желілік экран (брандмауэр), шабуылдарды анықтау және алдын алу жүйелері (IPS) секілді классикалық қорғаныс құралдарын пайдалану жеткілікті болып табылады. Алайда, аталған механизмдердің бұлттық инфрақұрылымның ерекшеліктеріне бейімделуі және виртуалдандырылған ортада тиісті тиімділікпен жұмыс істеуі шешуші мәнге ие. Бұлт элементтеріне бағытталған функционалдық шабуылдар ерекше қауіп тобын құрайды. Шабуылдың бұл түрі бұлттық архитектураның көпқабатты құрылымымен, сондай-ақ жүйенің жалпы қауіпсіздік деңгейі оның ең осал буынының қорғаныс деңгейімен анықталатындығы туралы іргелі қауіпсіздік принципімен тығыз байланысты. Атап айтқанда, бұлттық жүйенің алдыңғы шебінде орналасқан кері прокси-серверге қарсы сәтті жүзеге асырылған DoS-шабуылы ішкі желілік коммуникациялар үздіксіз жұмыс істеген жағдайда да бүкіл бұлттық ресурсқа кіруді толығымен бұғаттай алады. Сол сияқты, қолданбалық сервер арқылы жүзеге асырылатын SQL-инъекция шабуылы деректерді сақтау деңгейіндегі қолжетімділік ережелеріне тәуелсіз түрде жүйелік деректерге рұқсатсыз қол жеткізуге мүмкіндік береді.

Функционалдық шабуылдардан тиімді қорғану үшін бұлттық архитектураның әрбір деңгейіне сәйкес мамандандырылған қауіпсіздік шараларын қолдану қажет: прокси-деңгейде DoS-қорғанысы, веб-сервер деңгейінде беттің тұтастығын бақылау, қолданбалық сервер деңгейінде қолданбалық желілік экрандар, дерекқор деңгейінде SQL-инъекциядан қорғаныс, ал сақтау жүйесінде резервтік көшіру және қолжетімділікті бақылау механизмдері. Аталған қорғаныс құралдарының әрқайсысы дербес әзірленгенімен, олар интеграцияланған кешенді бұлттық қауіпсіздік жүйесіне біріктірілмеген. Осы себепті, оларды бірыңғай архитектуралық шешімге кіріктіру міндеті бұлттық инфрақұрылымды жобалау сатысында шешілуге тиіс (Al–zahrani, 2025).

Клиенттік шабуылдар. Шабуылдың бұл түрі веб–ортада жасалған, бірақ бұлтқа да қатысты, себебі клиенттер әдетте бұлтқа браузер арқылы қосылады. Бұған сайтаралық скрипттеу (XSS), веб–сессияны ұрлау, құпия сөзді ұрлау, «ортада тұрған адам» шабуылдары және басқа да шабуылдар кіреді. Бұл шабуылдардан қорғаныс дәстүрлі түрде күшті аутентификацияға және өзара аутентификациямен шифрланған қосылымдарды пайдалануға негізделген. Дегенмен, барлық бұлтты әзірлеушілер мұндай қымбат және көбінесе қолайсыз қауіпсіздік шараларын көтере алмайды (1 кестені қара). Сондықтан, ақпараттық қауіпсіздіктің бұл саласында әлі де шешілмеген мәселелер және жаңа қауіпсіздік шешімдеріне орын бар.

Виртуалдандыру қауіптері. Виртуалды орталар дәстүрлі түрде бұлтты компоненттер үшін платформа ретінде қызмет ететіндіктен, виртуалдандыру жүйесіне жасалған шабуылдар бүкіл бұлтқа да қауіп төндіреді. Бұл қауіп түрі

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

тек бұлтты есептеулерге ғана тән, сондықтан біз оны төменде егжей–тегжейлі қарастырамыз. Кейбір виртуалдандыру қауіптеріне шешімдер пайда бола бастады, бірақ бұл сала салыстырмалы түрде жаңа, сондықтан әлі белгіленген шешімдер әзірленген жоқ. Ақпараттық қауіпсіздік нарығы жақын арада осы қауіп түріне қарсы қорғаныс құралдарын әзірлеуі әбден мүмкін.

Кесте 1. SaaS қызметтері

Citrix Systems	Piston Cloud Computing	DotCloud	Microsoft	Zoho
Salesforce.com				

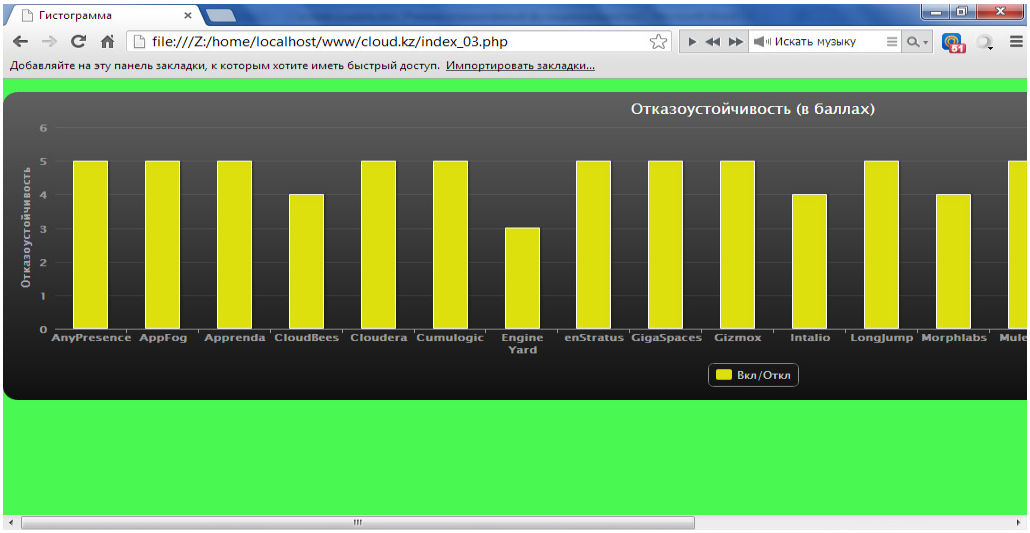
Бұлттық инфрақұрылымды басқарудың күрделі қауіптері. Бұлттық ортаны әкімшілендіру және басқару процестері де дербес қауіпсіздік санатына жататын мәселелер кешенін құрайды. Негізгі сын-қатерлер мыналарды қамтиды: барлық бұлттық ресурстардың толық есепке алынуын қамтамасыз ету, бақылаудан тыс қалған виртуалды машиналардың пайда болуын болдырмау, шаруашылық жүргізуші субъектілер үшін функционалдық маңызы жоқ бизнес-процестердің орындалуын тоқтату, сондай-ақ бұлттың жекелеген қабаттары мен компоненттері арасындағы өзара конфигурациялық байланыстардың тұтастығын сақтау. Аталған міндеттердің әрқайсысы жүйелік бақылау мен басқару стратегиясының ажырамас бөлігі ретінде қарастырылуы тиіс, себебі олардың кез келгеніндегі ақаулық бұлттық сервистің жалпы функционалдығы мен қауіпсіздік деңгейіне тікелей әсер етеді. Бұл қауіп түрі бірыңғай ақпараттық жүйе ретінде бұлтты басқарумен және ақпараттық жүйені күтіп ұстауға қажетсіз шығындарға әкелуі мүмкін бұлттық жұмыстағы теріс пайдаланушыларды немесе басқа да бұзылуларды анықтаумен байланысты. Мысалы, егер бұлт файлды вирусты анықтау үшін жіберуге мүмкіндік берсе, мұндай анықтаулардың ұрлануын қалай болдырмауға болады? Бұл қауіп түрі ең жоғары деңгейлі болып табылады және әмбебап қауіпсіздік шаралары ол үшін жеткіліксіз – оның жалпы қорғанысы әрбір бұлтқа жеке бейімделуі керек. Жалпы тәуекелдерді басқару моделі бұған көмектесе алады, бірақ оны әлі де бұлттық инфрақұрылымдарға дұрыс қолдану қажет (Тұрсынбеков, 2015; Saad et al., 2020)

Қауіптердің алғашқы екі түрі жеткілікті түрде зерттелген және олар үшін қорғаныс құралдары әзірленген, бірақ оларды бұлтта пайдалану үшін бейімдеу қажет. Мысалы, брандмауэрлер периметрді қорғауға арналған, бірақ бұлтта периметрді жеке клиентке тағайындау қиын, бұл қорғауды айтарлықтай қиындатады. Сондықтан брандмауэр технологиясын бұлттық инфрақұрылымға бейімдеу қажет. Мысалы, Check Point қазіргі уақытта осы салада белсенді жұмыс істеп жатыр. Бұлттық есептеулер үшін жаңа қауіп түрі – виртуалдандыру мәселелері. Себебі виртуалдандыру жүйеге қосымша шабуылға ұшырайтын элементтерді енгізеді. Оларға гипервизор, виртуалды машиналарды бір түйіннен екіншісіне көшіретін жүйе және виртуалды машинаны басқару жүйесі жатады.

Басқару жүйелеріне шабуылдар. Бұлттарда, әсіресе қоғамдық бұлттарда қолданылатын виртуалды машиналардың көптігі виртуалды машиналарды

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

жасауды, көшіруді және жоюды сенімді түрде басқара алатын басқару жүйелерін қажет етеді. Басқару жүйелерін бұзу көрінбейтін виртуалды машиналардың жасалуына, белгілі бір машиналардың бұғатталуына және бұлт қабаттарына рұқсатсыз элементтердің енгізілуіне әкелуі мүмкін. Мұның бәрі шабуылдаушыларға бұлттан ақпарат алуға немесе бұлттың бір бөлігін немесе тұтастай басып алуға мүмкіндік береді. Айта кету керек, жоғарыда аталған барлық қауіптер қазіргі уақытта тек гипотетикалық болып табылады, себебі мұндай нақты шабуылдар туралы ақпарат іс жүзінде жоқ. Дегенмен, виртуалдандыру және бұлтты есептеулер танымал болғаннан кейін, осы шабуылдардың барлығы нақты болуы мүмкін. Сондықтан оларды бұлтты жүйелерді жобалау кезеңінде де ескеру қажет (Prabowo et al., 2025; Hendradi et al., 2020)



Сур. 2. Ақаулыққа төзімділік гистограммасы

Қоғамдық өмірде, әсіресе мемлекеттік басқару саласында ақпараттық жүйе әрқашанда нақты уақыт режимінде өмір сүріп келеді. Мұндай жүйе ақпараттың өзін (деректер жиынтығын), оны өңдеудің формаларын, әдістері мен құралдарын, сондай-ақ ақпараттық процестерге қатысатын субъектілерді қамтитын күрделі органикалық тұтастық болып табылады. Осы тұрғыдан алғанда, мемлекеттік басқару жүйесіндегі ақпараттық жүйені (немесе жүйелер кешенін) құру мен жетілдіру мәселесін талқылағанда, біз жекелеген объектілер мен субъектілердің динамикалық күйлерін бейнелейтін деректерді жасау, тіркеу, жинау, өңдеу және сақтау функцияларын атқаратын дәстүрлі мағынадағы жүйе туралы емес, сапалық жағынан жаңа, түбегейлі өзгеше сипаттағы құбылыс туралы сөз қозғап отырмыз.

Мәселенің мәні 1960-жылдары көптеген зерттеушілер мен практиктер ұстанған көзқарастай, әкімшілік процестерге есептеу техникасының, желілік технологиялардың және бағдарламалық қамтамасыз етудің жаңа буынын енгізумен шектелмейді. Бұл міндет әлдеқайда кешенді, көп қырлы, терең

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

мазмұнды және шешімдерін табуы күрделі сипатқа ие. Микроэлектроника, информатика, микропроцессорлық технологиялар, робототехника және заманауи ақпараттық қолдаудың басқа да құралдарын кешенді пайдалану ақпараттық менеджменттің барлық аспектілерін сапалы жаңа ғылыми-техникалық деңгейге көтеруге, озық және жоғары тиімді ақпараттық технологияларды құрудың кең перспективаларын ашады. Бұл ретте, ақпараттық жүйелерді трансформациялау тек техникалық жаңғырту ғана емес, сонымен бірге басқару философиясы мен әдіснамасының эволюциясын да білдіреді. (Sharma et al., 2025; Rittinghaus et al., 2017)

Қорытынды.

Ақпараттық технологиялардың пайда болу барысында ақпараттық жүйелерді құрудың бірнеше модельдері пайда болды. Ол монолитті мейнфрейм архитектурасынан басталды. Мейнфрейм – бұл үлкен, әмбебап, жоғары өнімді, ақауларға төзімді, айтарлықтай енгізу/шығару ресурстары, үлкен көлемдегі жедел жады және сыртқы жады бар, қарқынды пакеттік және нақты уақыт режиміндегі транзакцияларды өңдеумен маңызды жүйелерде пайдалануға арналған сервер. Ол перспективалы клиент–сервер архитектурасымен ауыстырылды. Мұнда арнайы дерекқор сервері болды, ал пайдаланушылар қалың клиенттермен жұмыс істеп, дерекқор серверін босататын. Содан кейін одан да заманауи архитектура пайда болды – үш деңгейлі (немесе көп деңгейлі) архитектура, мұнда қолданбалы логика қолданбалы сервер деп аталатын бөлек компьютерге көшірілді, ал пайдаланушылар веб–браузерлер арқылы жұқа клиенттермен жұмыс істеді. Қазіргі кездегі қолданбалардың көпшілігі осы архитектураны пайдаланып жасалған. Бұл архитектуралар бүкіл IT инфрақұрылымын жергілікті жерде орналастыруды қамтиды. Бұлтты есептеулер ақпараттық жүйе архитектурасының эволюциясындағы келесі қадам болып табылады. Бұл тәсілдің орасан зор артықшылықтарына байланысты, жақын арада көптеген ақпараттық жүйелер бұлтқа көшірілетіні анық. 2011 жылы Қазақстан басқа елдерден озып кету үшін бұлтты технологияларды әзірлеуді бастады. «Қазақтелеком» АҚ еншілес компаниясы KT Cloud Lab жоба менеджері болды. NEC Neva Communication Systems компаниясы Қазақстан астанасы Алматыда өкілдік ашты. Бұл компанияның өкілдері Қазақстанның шағын және орта бизнесінің бұлтты есептеулер IT шешімдеріне деген қажеттіліктерін қанағаттандыруға дайын екендіктерін білдірді. Ғылыми зерттеу нәтижесінде алынған негізгі қорытындыларды тұжырымдайық:

- Бұл зерттеу жұмысында мемлекеттік қызметтер үшін бұлтты есептеу платформаларын таңдау мәселесі қарастырылады.
- Шет елдердегі бұлтты технологиялардың дамуын талдау қарастырылады.
- Қазақстанда бұлтты қызметтерді енгізу, олардың артықшылықтары мен мемлекеттік сектор үшін пайдасы талдаудан өткізілді.
- SaaS, PaaS және IaaS модульдеріне сәйкес, бұлттық қызметтер арасында әлемдегі ең бәсекеге қабілетті және ең үздік компаниялар тізімі кесте түрінде

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

жасалды.

- Қазақстанның мемлекеттік органдарында бұлтты технологияларды енгізу үшін оларды таңдаудың негізгі критерийлері ұсынылады.
- Бұлттық нарықтағы ірі ойыншылардың бұлттық қызметтерге арналған бағдарламалық өнімдері шолудан өтеді.
- Бұлтты технологиялар саласындағы киберқауіптерге тап болған кезде ақпараттық қауіпсіздікті қамтамасыз етудің шешімдері ұсынылады.
- Hyper–V қауіпсіздік саласындағы ең жақсы тәжірибелерге шолу жасайды.

ӘДЕБИЕТТЕР

Al–zahrani I.A.A. (2025). Degree of Use of Cloud Artificial Intelligence in Improving Academic Guidance Systems in Virtual Learning Environments from the Perspective of Faculty Members // Journal of Educational and Human Sciences. No. 43. — Б. 435–466. DOI:10.33193/JEAHS.43.2025.618. [Ағыл. тіл.].

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., & Zaharia, M. (2010). A view of cloud computing // In Communications of the ACM — Т. 53. — No. 4. — Б. 50–58. DOI:https://doi.org/10.1145/1721654.1721672. [Ағыл. тіл.].

Abdaly, S. (2021). Cloud computing and the foundation of security in the cloud // Engineering Journal of Satbayev University. — Т. 143. — No. 2. — Б. 193–198. DOI: https://doi.org/10.51301/vest.su.2021.i2.25. [Ағыл. тіл.].

Alakuu A., Delali Kwasi Dake. (2025). Cloud Computing in Education: A review of Architecture, Applications, and Integration Challenges // International Journal of Computer Applications. — Т. 186. — No. 66. — Б. 49–65. DOI: https://doi.org/10.5120/ijca2025924472. [Ағыл. тіл.].

Ali S., Nawaiseh S. and A., Jameel A. and H., Y. and M. I. Fathy I. and K. (2020). Dr. Emadeldin, A Proposed Model Based on Cloud Computing Technology to Improve Higher Education Institutions Performance (2020) // International Journal of Advanced Research in Engineering and Technology. — Т. 11. — No. 9. — Б. 612–628. https://ssrn.com/abstract=3712837. [Ағыл. тіл.].

Barham P., Dragovic B., Fraser K. et al. (2017). Xen and the Art of Virtualization // ACM SIGOPS Operating Systems Review. — Т. 35. — No. 4. — Б. 164–177. DOI: https://doi.org/10.1145/1165389.945462. [Ағыл. тіл.].

Hendradi P., Abd Ghani M.K. (2020). Artificial Intelligence Influence In Education 4.0 To Architecture Cloud–Based E–Learning System. (2020) // International Journal of Artificial Intelligence Research. DOI: https://doi.org/10.29099/IJAIR.V4I1.109. [Ағыл. тіл.].

Ванина М.Ф., Ерохин А.Г., Фролова Е.А. (2015). Применение облачных технологий в компаниях малого и среднего бизнеса // Век качества. №1. URL: https://cyberleninka.ru/article/n/primenenie–oblachnyh–tehnologiy–v–kompaniyah–malogo–i–srednego–biznesa. [Орыс. тіл.].

Kudra V. (2011). Federal Cloud Computing Strategy // White Houze. URL: https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/egov_docs/federal–cloud–computing–strategy.pdf. [Ағыл. тіл.].

Prabowo R.Y. (2025). The Triad of Cloud, Analytics, And Pedagogy: A Systematic Review of AI–Driven Personalization in Cloud–Based Learning Environments // Journal of Educational Technology. — Т. 10. — No. 1. — Б. 44–59. DOI:10.17977/um039v10i12025p44–59. [Ағыл. тіл.].

Rittinghaus J.W., Ransom J.F. (2017). Cloud Computing – Implementation, Governance, and Security // Taylor and Francis Group. — Б. 174. https://ndl.ethernet.edu.et/bitstream/123456789/26737/1/John%20W.%20Rittinghouse.pdf. [Ағыл. тіл.].

Sharma A.K. Nitin, S. Kumar (eds.) (2025). Establishing AI–Specific Cloud Computing Infrastructure // Hershey: IGI Global Scientific Publishing. — Б. 450. DOI: 10.4018/979–8–3693–9694–0. [Ағыл. тіл.].

Schmidt R. (2010). VCP VMware Certified Professional vSphere 4 Study Guide (Exam VCP410) // McGraw Hill Professional. ISBN: 9780071633673. https://books.google.ru/books?id=C_WoaRZ2FGIC&hl=ru. [Ағыл. тіл.].

Тұрсынбеков Н.Қ. (2015). Қазақстандағы бұлтты технологияларды дамыту перспективалары // Вестник КазНТУ. No. 2. — Б. 45–52. https://ust.kz/word/bulttyq_tehnologiyalar_qazaqstandagy_bulttyq_tehnologiyalardyng_damyy–394041.html. [Қаз. тіл.].

Трофименко Е.В. (2020). Введение в облачные вычисления. Основные понятия // ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ. – Воронеж: Издательский дом ВГУ. — Б. 59. EDN HRRJNZ.

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

https://www.elibrary.ru/item.asp?id=47672758. [Орыс. тіл.].

REFERENCES

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., & Zaharia, M. (2010). A view of cloud computing // In Communications of the ACM. — Vol. 53. — No. 4. — Pp. 50–58. DOI: https://doi.org/10.1145/1721654.1721672.[In Eng.].

Augustine Alakuu, Delali Kwasi Dake. (2025). Cloud Computing in Education: A review of Architecture, Applications, and Integration Challenges // International Journal of Computer Applications. — Vol. 186. — No. 66. — Pp. 49–65. DOI: https://doi.org/10.5120/ijca2025924472.[In Eng.].

Abdaly, S. (2021). Cloud computing and the foundation of security in the cloud // Engineering Journal of Satbayev University. — Vol. 143. — No. 2. — Pp. 193–198. DOI: https://doi.org/10.51301/vest.su.2021.i2.25. [In Eng.].

Al–zahrani I.A.A. (2025). Degree of Use of Cloud Artificial Intelligence in Improving Academic Guidance Systems in Virtual Learning Environments from the Perspective of Faculty Members // Journal of Educational and Human Sciences. No. 43. — Pp. 435–466. DOI:10.33193/JEAHS.43.2025.618.[In Eng.].

Ali S., Nawaiseh S. and A., Jameel A. and H., Y. and M. I. Fathy I. and K. (2020). Dr. Emadeldin, A Proposed Model Based on Cloud Computing Technology to Improve Higher Education Institutions Performance // International Journal of Advanced Research in Engineering and Technology. — Vol. 11. — No. 9. — Pp. 612–628. https://ssrn.com/abstract=3712837.[In Eng.].

Barham P., Dragovic B., Fraser K. et al. (2017). Xen and the Art of Virtualization // ACM SIGOPS Operating Systems Review. — Vol. 35. — No. 4. — Pp. 164–177. DOI: https://doi.org/10.1145/1165389.945462. [In Eng.].

Hendradi P., Mohd Khanapi Abd Ghani. (2020). Artificial Intelligence Influence In Education 4.0 To Architecture Cloud–Based E–Learning System. (2020) // International Journal Of Artificial Intelligence Research. DOI: https://doi.org/10.29099/IJAIR.V4I1.109.[In Eng.].

Kudra V. (2011). Federal Cloud Computing Strategy // White Houze. URL: https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/egov_docs/federal–cloud–computing–strategy.pdf.[In Eng.].

Prabowo R.Y. (2025). The Triad of Cloud, Analytics, And Pedagogy: A Systematic Review of AI–Driven Personalization in Cloud–Based Learning Environments // Journal of Educational Technology. — Vol. 10. — No. 1. — Pp. 44–59. DOI:10.17977/um039v10i12025p44–59.[In Eng.].

Robert Schmidt. (2010). VCP VMware Certified Professional vSphere 4 Study Guide (Exam VCP410) // McGraw Hill Professional. ISBN: 9780071633673. https://books.google.ru/books?id=C_WoaRZ2FGIC&hl=ru. [In Eng.].

Rittinghaus J.W., Ransom J.F. (2017). Cloud Computing – Implementation, Governance, and Security // Taylor and Francis Group. — Pp. 174. https://ndl.ethernet.edu.et/bitstream/123456789/26737/1/John%20W.%20Rittinghouse.pdf.[In Eng.].

Sharma A.K. Nitin, S. Kumar (eds.) (2025). Establishing AI–Specific Cloud Computing Infrastructure – Hershey: IGI Global Scientific Publishing. — Pp. 450. DOI: 10.4018/979–8–3693–9694–0.[In Eng.].

Tursynbekov, N.K. (2015). Prospects for the Development of Cloud Technologies in Kazakhstan // Bulletin of KazNTU. — Vol. 2. — Pp. 45–52. https://ust.kz/word/bulttyq_tehnologiyalar_qazaqstandagy_bulttyq_tehnologiyalardyng_damyy–394041.html.[In Kaz.].

Trofimenko E.V. (2020). Vvedenie v oblachnye vychisleniya. Osnovnye ponyatiya / VORONEZHSKII GOSUDARSTVENNYI UNIVERSITET. – Voronezh: Izdatel'skii dom VGU. — Pp. 59. EDN HRRJNZ. https://www.elibrary.ru/item.asp?id=47672758.[In Russ.].

Vanina M.F., Erokhin A.G., Frolova E.A. (2015). Primenenie oblachnykh tekhnologii v kompaniyakh malogo i srednego biznesa // Vek kachestva. №1. URL: https://cyberleninka.ru/article/n/primenenie–oblachnyh–tehnologiy–v–kompaniyah–malogo–i–srednego–biznesa.[In Russ.].

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

INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES

ХАЛЫҚАРАЛЫҚ АҚПАРАТТЫҚ ЖӘНЕ КОММУНИКАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАР ЖУРНАЛЫ

МЕЖДУНАРОДНЫЙ ЖУРНАЛ ИНФОРМАЦИОННЫХ И КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

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

Главный редактор:
Колесникова Катерина Викторовна

Ответственный редактор:
Мрзабаева Раушан Жалиевна

Компьютерная верстка:
Калабай Замзагуль Ертугановна

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

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

Издание АО "Международного университета информационных технологий"