

MINISTRY OF SCIENCE AND HIGHER EDUCATION OF THE REPUBLIC OF KAZAKHSTAN  
ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ  
МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РЕСПУБЛИКИ КАЗАХСТАН  
KAZAKHSTAN



**INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION  
TECHNOLOGIES**

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

**ХАЛЫҚАРАЛЫҚ АҚПАРАТТЫҚ ЖӘНЕ КОММУНИКАЦИЯЛЫҚ  
ТЕХНОЛОГИЯЛАР ЖУРНАЛЫ**

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

**МЕЖДУНАРОДНЫЙ ЖУРНАЛ ИНФОРМАЦИОННЫХ И  
КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ**

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

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

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

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

#### EDITOR-IN-CHIEF:

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

#### DEPUTY EDITOR-IN-CHIEF:

**Madina Ipalakova** — Candidate of Technical Sciences, associate professor, Director of the Research Department, International Information Technology University (Kazakhstan)

#### EDITORIAL BOARD:

**Abdul Razak** — PhD, professor, Department of Cybersecurity, International Information Technology University (Kazakhstan)

**Lucio Tommaso De Paolis** — Director of the R&D Department of the AVR Laboratory, Department of Engineering for Innovation, University of Salento (Italy)

**Liz Bacon** — Professor, Deputy Vice-Chancellor, Abertay University (United Kingdom)

**Michele Pagano** — PhD, Professor, University of Pisa (Italy)

**Mukhtarbay Otelbayev** — Doctor of Physical and Mathematical Sciences, professor, academician of the National Academy of Sciences of the Republic of Kazakhstan, professor of the Department of Mathematical and Computer Modeling, International Information Technology University (Kazakhstan)

**Bolatbek Rysbauly** — Doctor of Physical and Mathematical Sciences, professor, professor of the Department of Computing and Data Science, Astana IT University (Kazakhstan)

**Yevgeniya Daineko** — PhD, research professor, Department of Information Systems, International Information Technology University (Kazakhstan)

**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 Тоқсуғаевич** — 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 Максудовна 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 Токсуажевич** — 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 Максуговна 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

**D. Abzhanova, A. Biloshchytski**

A MODEL AND METHOD FOR MANAGING DATA ON EMISSIONS FROM STATIONARY SOURCES OF POLLUTION IN AN INTELLIGENT ENVIRONMENTAL MONITORING SYSTEM .....9

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

EARLY DETECTION OF HYDROLOGICAL HAZARDS BASED ON SPATIOTEMPORAL ANALYSIS .....25

## INFORMATION TECHNOLOGY

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

AI TECHNOLOGIES IN LANGUAGE EDUCATION: PRACTICAL ASPECTS AND CHALLENGES OF STUDENT USAGE .....36

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

HYBRID STACKING FRAMEWORK FOR CROP CLASSIFICATION USING UAV DATA .....50

**A.K. Aitim**

JOINT MORPHOLOGICAL DISAMBIGUATION AND POS TAGGING FOR AGGLUTINATIVE LANGUAGES .....62

**S.A. Yesniyazova, S.T. Kaimov**

PREDICTIVE MAINTENANCE OF HEAVY-DUTY TRUCKS USING EXPLAINABLE MACHINE LEARNING .....78

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

DATA COMPRESSION ALGORITHM BASED ON WAVELET TRANSFORMER; ANALYSIS AND IMPLEMENTATION IN MATLAB .....92

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

A MATHEMATICAL AND ALGORITHMIC APPROACH TO THE DEVELOPMENT OF AN INTELLIGENT TEXT-TO-SQL SYSTEM BASED ON LARGE LANGUAGE MODELS .....110

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

MACHINE LEARNING FOR COMPREHENSIVE EVALUATION OF CARDIOVASCULAR DISEASE RISK AND BIOCHEMICAL ALTERATIONS: FOCUS ON ASPARTATE AMINOTRANSFERASE .....131

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

INTEGRATION OF MEMS ACCELEROMETER SENSOR MODULES IN INDUSTRIAL MONITORING SYSTEMS .....146

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

KAZCAUSAL: THE FIRST CORPUS-BASED ANNOTATION OF CAUSAL RELATIONSHIPS IN THE KAZAKH LANGUAGE .....160

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

DIVIDING DEVICES WITH PRELIMINARY PREPARATION OF MULTIPLES OF THE DIVISOR .....172

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

MATHEMATICAL AND ALGORITHMIC APPROACHES TO THE DEVELOPMENT OF A COLLABORATIVE FILTERING-BASED RECOMMENDER SYSTEM .....188

**S. Sharmukhanbet, G. Turmukhanova, O. Findik, V. Makhatova, L. Kurmangazyeva**

HIGH-PRECISION ROBOTIC ASSEMBLY UNDER VARIABLE ILLUMINATION: A ROBUST MECHATRONIC ARCHITECTURE FOR VISUAL SERVOING .....209

## INFORMATION SECURITY AND COMMUNICATION TECHNOLOGIES

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

MACHINE LEARNING ALGORITHM FOR EARLY DETECTION OF AUTISM SPECTRUM DISORDERS IN CHILDREN BASED ON MULTIMODAL ANALYSIS OF EYE MOVEMENTS AND FACIAL EXPRESSIONS .....227

**K. Baisylbayeva, Sh. Mussiraliyeva, Zh. Yeltay**

DETECTION OF EXTREMIST IDEOLOGY IN THE KAZAKH LANGUAGE: ANNOTATION CHALLENGES AND DEEP LEARNING APPROACHES .....242

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

DEVELOPMENT AND RESEARCH OF A METHOD FOR ANALYZING NETWORK TRAFFIC TO IDENTIFY A CYBER THREAT .....	261
<b>D.I. Prokopovych-Tkachenko, N.K. Zhumagalieva, D.N. Shchytyov, N.F. Mormul, D.A. Cherkaskyi</b>	
FUZZY MODEL FOR EVALUATING INFORMATION SECURITY PARAMETERS OF INFORMATION SYSTEMS UNDER INCOMPLETE AND QUALITATIVE DATA: CONSTRUCTION METHODOLOGY, RULE BASE TUNING, AND DEMONSTRATION CASE FOR ORGANIZATIONS .....	279
<b>E.A. Pustovoy, O.A. Pustovaya, A.N. Raushanova, I.S. Zaurbekov</b>	
EVALUATION OF THE EFFECTIVENESS OF SYNTHESIS OF STOCHASTIC MODELS WITH CONTROLLED PROPERTIES .....	305
<b>Y. Serzhan, T. Umarov, A. Abilbayeva</b>	
FRAUD DETECTION IN CREDIT CARD TRANSACTIONS USING MACHINE LEARNING: A COMPARATIVE ANALYSIS .....	321

## МАЗМҰНЫ

### ӘЛЕУМЕТТІК-ЭКОНОМИКАЛЫҚ ЖҮЙЕЛЕРДІ ДАМУДАҒЫ ЦИФРЛЫҚ ТЕХНОЛОГИЯЛАР

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

### АҚПАРАТТЫҚ ТЕХНОЛОГИЯЛАР

<b>Ф.Н. Абдранмова, А.А. Керейбаева, Д.С. Дюсенова, Д.А. Алиева, Т.Ж. Токтарова</b>	
ТІЛ БІЛІМІНДЕ ЖАСАНДЫ ИНТЕЛЛЕКТ ТЕХНОЛОГИЯЛАРЫ: СТУДЕНТТЕР ҚОЛДАНУЫНЫҢ ПРАКТИКАЛЫҚ АСПЕКТІЛЕРІ МЕН МӘСЕЛЕЛЕРІ .....	36
<b>Г.Т. Азиева, М.Б. Есенова, А.К. Абжаппарова, Г.Б. Абдикеримова, Р. Schmidt</b>	
UAV ДЕРЕКТЕРІ НЕГІЗІНДЕ АУЫЛ ШАРУАШЫЛЫҒЫ DAҚЫЛДАРЫН ЖІКТЕУГЕ АРНАЛҒАН ГИБРИДТІ СТЕКИНГ МОДЕЛІ .....	50
<b>Ә.Қ. Әйтiм</b>	
АГГЛЮТИНАТИВТІ ТІЛДЕРГЕ АРНАЛҒАН МОРФОЛОГИЯЛЫҚ ДИЗАМБИГУАЦИЯ МЕН POS-ТАҢ-БАЛАУДЫ БІРЛЕСІП МОДЕЛЬДЕУ .....	62
<b>С.А. Есниязова, С.Т. Каимов</b>	
ТҮСІНДІРІЛЕТІН МАШИНАЛЫҚ ОҚЫТУДЫ ҚОЛДАНА ОТЫРЫП АУЫР ЖҮК КӨЛІКТЕРІНЕ БОЛЖАМДЫ ТЕХНИКАЛЫҚ ҚЫЗМЕТ КӨРСЕТУ .....	78
<b>Т.Д. Иманбекова, Ж.Б. Ибраева, Г.Т. Джаканова, Г.Т. Асқанбай</b>	
МӘЛІМЕТТЕРДІ ВЕЙВЛЕТ-ТҮРЛЕНДІРГІШТІҢ НЕГІЗІНДЕ ҚЫСУ АЛГОРИТМІ; MATLAB ОРТАСЫНДА ТАЛДАУ ЖӘНЕ ІСКЕ АСЫРУ .....	92
<b>Б.З. Кенжегулов, Ж.Т. Билялова, К.Н. Утеулиева, Л. Нурғалиева, Ш.С. Нуржанова</b>	
ҮЛКЕН ТІЛДІК МОДЕЛЬДЕР НЕГІЗІНДЕ ИНТЕЛЛЕКТУАЛДЫ ТЕХТ-ТО-SQL ЖҮЙЕСІН ӨЗІРЛЕУДІҢ МАТЕМАТИКАЛЫҚ-АЛГОРИТМДІК ТӘСІЛІ .....	110
<b>Н.Ш. Максұтова, Ж.А. Тусупов, А.Ә. Шекербек, Ж.Е. Кенжебаева, К.О. Рахимов</b>	
ЖҮРЕК-ҚАН ТАМЫРЛАРЫ АУРУЛАРЫНЫҢ ҚАУІП-ҚАТЕРІН ЖӘНЕ БИОХИМИЯЛЫҚ ӨЗГЕРІСТЕРДІ КЕШЕНДІ БАҒАЛАУ ҮШІН МАШИНАЛЫҚ ОҚЫТУ: АСПАРТАМИНОТРАНСФЕРАЗАҒА ЕРЕКШЕ НАЗАР .....	131
<b>О.С. Салықова, В.А. Мадин, Б.Р. Салықов, Д.Н. Комаров, Н.В. Мануилов</b>	
ӨНЕРКӘСІПТІК МОНИТОРИНГ ЖҮЙЕЛЕРІНДЕГІ MEMS-АКСЕЛЕРОМЕТРЛЕРДІҢ СЕНСОРЛЫҚ МОДУЛЬДЕРІН ИНТЕГРАЦИЯЛАУ .....	146
<b>Р. Таберхан, М.А. Самбетбаева, Г. Қалман</b>	
KAZCAUSAL: ҚАЗАҚ ТІЛІНДЕГІ СЕБЕП-САЛДАРЛЫҚ ҚАТЫНАСТАРДЫҢ АЛҒАШҚЫ КОРПУСТЫҚ АННОТАЦИЯСЫ .....	160
<b>С. Тынымбаев, С.Е. Маманова, Р. Бердібаев, Ж.Е. Темірбекова, Т. Чинибаева</b>	
БӨЛГІШТІҢ ЕСЕЛІ МӘНДЕРІН АЛДЫН АЛА ДАЙЫНДАУМЕН ЖҮЗЕГЕ АСЫРЫЛАТЫН БӨЛУ ҚҰРЫЛҒЫЛАРЫ .....	172



<b>К.Н. Утеулиева, Б.З. Кенжегулов, Т.А. Каражигитова, Х. Булбул, З.Ж. Жанузакова</b> КОЛЛАБОРАТИВТІК СҮЗГІЛЕУ НЕГІЗІНДЕГІ ҰСЫНЫМДЫҚ ЖҮЙЕНІ ӨЗІРЛЕУДІҢ МАТЕМАТИКАЛЫҚ-АЛГОРИТМДІК ТӘСІЛДЕРІ .....	188
<b>С. Шармуханбет, Г. Тұрмуханова, О. Финдик, В. Махатова, Л. Курмангазиева</b> АЙНЫМАЛЫ ЖАРЫҚ ЖАҒДАЙЫНДАҒЫ ЖОҒАРЫ ДӘЛДІКТІ РОБОТТЫҚ ҚҰРАСТЫРУ: ВИЗУАЛДЫ СЕРВОТЕЖЕУДІҢ ТӨЗІМДІ МЕХАТРОНИКАЛЫҚ АРХИТЕКТУРАСЫ .....	209

### АҚПАРАТТЫҚ ҚАУІПСІЗДІК ЖӘНЕ КОММУНИКАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАРҒА АРНАЛҒАН

<b>А. Амирбай, З. Аманбайқызы, К. Максүтова, А. Муханова, М. Kassim</b> КӨЗ ҚОЗҒАЛЫСТАРЫ МЕН БЕТ МИМИКА БЕЛГІЛЕРІН МУЛЬТИМОДАЛЬДЫ ТАЛДАУҒА НЕГІЗ- ДЕЛГЕН БАЛАЛАРДАҒЫ АУТИЗМ СПЕКТРІНІҢ БҰЗЫЛЫСТАРЫН ЕРТЕ АНЫҚТАУҒА АРНАЛҒАН МАШИНАЛЫҚ ОҚЫТУ АЛГОРИТМІ .....	227
<b>К.Д. Байсылбаева, Ш.Ж. Мусиралиева, Ж. Елтай</b> ҚАЗАҚ ТІЛІНДЕГІ ЭКСТРЕМИСТІК ИДЕОЛОГИЯНЫ АНЫҚТАУ: АННОТАЦИЯЛАУ МӘСЕЛЕЛЕРІ ЖӘНЕ ТЕРЕҢ ОҚЫТУ ТӘСІЛДЕРІ .....	242
<b>М.А. Болатбек, А.М. Усманова, Қ.Б. Багитова, Г.Б. Байспай</b> КИБЕР ҚАУІПТІ АНЫҚТАУ ҮШІН ЖЕЛІЛІК ТРАФИКТІ ТАЛДАУ ӘДІСІН ӨЗІРЛЕУ ЖӘНЕ ЗЕРТТЕУ .....	261
<b>Д.И. Прокопович-Ткаченко, Н.К. Жумагалиева, Д.Н. Щитов, Н.Ф. Мормуль, Д.А. Черкасский</b> ТОЛЫҚ ЕМЕС ЖӘНЕ САПАЛЫҚ ДЕРЕКТЕР ЖАҒДАЙЫНДА АҚПАРАТТЫҚ ЖҮЙЕЛЕРДІҢ АҚПА- РАТТЫҚ ҚАУІПСІЗДІК ПАРАМЕТРЛЕРІН БАҒАЛАУДЫҢ БҰЛЫҢҒЫР МОДЕЛІ: ҚҰРУ ӘДІСТЕМЕСІ, ЕРЕЖЕЛЕР БАЗАСЫН БАПТАУ ЖӘНЕ ҰЙЫМДАРҒА АРНАЛҒАН ДЕМОНСТРАЦИЯЛЫҚ КЕЙС .....	279
<b>Е.А. Пустовой, О.А. Пустовая, А.Н. Раушанова, И.С. Заурбеков</b> БАСҚАРЫЛАТЫН ҚАСИЕТТЕРІ БАР СТОХАСТИКАЛЫҚ МОДЕЛЬДЕРДІ СИНТЕЗДЕУДІҢ ТИМДІЛІГІН БАҒАЛАУ .....	305
<b>Е. Сержан, Т. Умаров, А. Әбілбаева</b> МАШИНАЛЫҚ ОҚУ ӘДІСІ АРҚЫЛЫ КРЕДИТ КАРТА ОПЕРАЦИЯЛАРЫНДАҒЫ АЛАЯҚТЫҚТЫ АНЫҚТАУ: САЛЫСТЫРМАЛЫ ТАЛДАУ .....	321

### СОДЕРЖАНИЕ

#### ЦИФРОВЫЕ ТЕХНОЛОГИИ В РАЗВИТИИ СОЦИО-ЭКОНОМИЧЕСКИХ СИСТЕМ

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

#### ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

<b>Ф.Н. Абдраимова, А.А. Керейбаева, Д.С. Дюсенова, Д.А. Алиева, Т.Ж. Токтарова</b> ТЕХНОЛОГИИ ИИ В ЯЗЫКОВОМ ОБРАЗОВАНИИ: ПРАКТИЧЕСКИЕ АСПЕКТЫ И ПРОБЛЕМЫ ПРИМЕНЕНИЯ СТУДЕНТАМИ .....	36
<b>Г.Т. Азиева, М.Б. Есенова, А.К. Абжаппарова, Г.Б. Абдикеримова, P. Schmidt</b> ГИБРИДНАЯ МОДЕЛЬ СТЕКИНГА ДЛЯ КЛАССИФИКАЦИИ СЕЛЬСКОХОЗЯЙСТВЕННЫХ КУЛЬТУР ПО ДАННЫМ UAV .....	50
<b>Ә.Қ. Әйтiм</b> СОВМЕСТНАЯ МОРФОЛОГИЧЕСКАЯ ДИЗАМБИГУАЦИЯ И POS-РАЗМЕТКА ДЛЯ АГГЛЮТИНАТИВНЫХ ЯЗЫКОВ .....	62
<b>С.А. Есниязова, С.Т. Каимов</b> ПРЕДИКТИВНОЕ ТЕХНИЧЕСКОЕ ОБСЛУЖИВАНИЕ ТЯЖЁЛЫХ ГРУЗОВИКОВ С ИСПОЛЬЗОВАНИ- ЕМ ОБЪЯСНИМОГО МАШИННОГО ОБУЧЕНИЯ .....	78
<b>Т.Д. Иманбекова, Ж.Б. Ибраева, Г.Т. Джаканова, Г.Т. Асқанбай</b>	

АЛГОРИТМ СЖАТИЯ ДАННЫХ НА ОСНОВЕ ВЕЙВЛЕТ-ПРЕОБРАЗОВАТЕЛЯ: АНАЛИЗ И РЕАЛИЗАЦИЯ В МАТЛАВ .....	92
<b>Б.З. Кенжегулов, Ж.Т. Билялова, К.Н. Утеулиева, Л. Нургалиева, Ш.С. Нуржанова</b>	
МАТЕМАТИКО-АЛГОРИТМИЧЕСКИЙ ПОДХОД К РАЗРАБОТКЕ ИНТЕЛЛЕКТУАЛЬНОЙ ТЕХТ-TO-SQL СИСТЕМЫ НА ОСНОВЕ БОЛЬШИХ ЯЗЫКОВЫХ МОДЕЛЕЙ .....	110
<b>Н.Ш. МаксUTOва, Д.А. Тусупов, А.А. Шекербек, Ж.Е. Кенжебаева, К.О. Рахмтов</b>	
МАШИННОЕ ОБУЧЕНИЕ ДЛЯ КОМПЛЕКСНОЙ ОЦЕНКИ РИСКА СЕРДЕЧНО-СОСУДИСТЫХ ЗАБОЛЕВАНИЙ И БИОХИМИЧЕСКИХ ИЗМЕНЕНИЙ: АКЦЕНТ НА АСПАРТАМИНОТРАНСФЕРАЗЕ ...	131
<b>О.С. Салыкова, В.А. Мадин, Б.Р. Салыков, Д.Н. Комаров, Н.В. Мануйлов</b>	
ИНТЕГРАЦИЯ СЕНСОРНЫХ МОДУЛЕЙ MEMS-АКСЕЛЕРОМЕТРОВ В СИСТЕМАХ ПРОМЫШЛЕННОГО МОНИТОРИНГА .....	146
<b>Р. Таберхан, М.А. Самбетбаева, Г. Калман</b>	
КАЗСАUSAL: ПЕРВАЯ КОРПУСНАЯ АННОТАЦИЯ ПРИЧИННО-СЛЕДСТВЕННЫХ СВЯЗЕЙ НА КАЗАХСКОМ ЯЗЫКЕ .....	160
<b>С. Тынымбаев, С.Е. Маманова, Р. Бердибаев, Ж.Е. Темирбекова, Т. Чинибаева</b>	
УСТРОЙСТВА ДЕЛЕНИЯ ЧИСЕЛ С ПРЕДВАРИТЕЛЬНОЙ ПОДГОТОВКОЙ КРАТНЫХ ДЕЛИТЕЛЮ .....	172
<b>К.Н. Утеулиева, Б.З. Кенжегулов, Т.А. Каражигитова, Х.Бюльбюль, З.Ж. Жанузакова</b>	
МАТЕМАТИКО-АЛГОРИТМИЧЕСКИЕ ПОДХОДЫ К РАЗРАБОТКЕ РЕКОМЕНДАТЕЛЬНОЙ СИСТЕМЫ НА ОСНОВЕ КОЛЛАБОРАТИВНОЙ ФИЛЬТРАЦИИ .....	188
<b>С. Шармуханбет, Г. Турмуханова, О.Финдик, В.Махатова, Л. Курмангазиева</b>	
ВЫСОКОТОЧНАЯ РОБОТИЗИРОВАННАЯ СБОРКА ПРИ ПЕРЕМЕННОЙ ОСВЕЩЁННОСТИ: РОБАСТНАЯ МЕХАТРОННАЯ АРХИТЕКТУРА ВИЗУАЛЬНОГО СЕРВОУПРАВЛЕНИЯ .....	209

## ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ

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



INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES

ISSN 2708–2032 (print)

ISSN 2708–2040 (online)

Vol. 7. Is.2. Number 26 (2026). Pp. 279–304

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

<https://doi.org/10.54309/IJICT.2026.26.2.018>

IRSTI / FTAXP / MPHTI 81.93.29; 28.23.19

## **FUZZY MODEL FOR EVALUATING INFORMATION SECURITY PARAMETERS OF INFORMATION SYSTEMS UNDER INCOMPLETE AND QUALITATIVE DATA: CONSTRUCTION METHODOLOGY, RULE BASE TUNING, AND DEMONSTRATION CASE FOR ORGANIZATIONS.**

***D.I. Prokopovych-Tkachenko<sup>1\*</sup>, N.K. Zhumagalieva<sup>2</sup>, D.N. Shchyotov<sup>1</sup>, N.F. Mormul<sup>1</sup>, D.A. Cherkaskyi<sup>3</sup>***

<sup>1</sup>University of Customs and Finance, Dnipro, Ukraine;

<sup>2</sup>Satbayev University, Almaty, Kazakhstan;

<sup>3</sup>National Technical University «Dnipro Polytechnic», Dnipro, Ukraine.

E-mail: [omega2417@gmail.com](mailto:omega2417@gmail.com).

**Dmytro Prokopovych-Tkachenko** — PhD in Technical Sciences, Associate Professor, Head of the Department of Cybersecurity and Information Technologies at the University of Customs and Finance; Senior Research Fellow at the State Scientific Institution “Institute of Information, Security and Law of the National Academy of Legal Sciences of Ukraine”; Doctor of Science Candidate at the Department of Cybersecurity Systems and Technologies, State University of Information and Communication Technologies, Dnipro, Ukraine

E-mail: [omega2417@gmail.com](mailto:omega2417@gmail.com), <https://orcid.org/0000-0002-6590-3898>;

**Nazym Zhumagalieva** — Postgraduate Student, Satbayev University, Almaty, Kazakhstan  
<https://orcid.org/0000-0003-1130-3405>;

**Dmytro Shchyotov** — PhD in Economics, Senior Lecturer at the Department of Management and Administration (Dnipro Faculty of Management and Business, KNUKiM), Doctoral Student at the University of Customs and Finance, Dnipro, Ukraine

<https://orcid.org/0000-0003-4306-8016>;

**Mykola Mormul** — PhD in Technical Sciences, Associate Professor at the Department of Cybersecurity and Information Technologies, University of Customs and Finance, Dnipro, Ukraine

<https://orcid.org/0000-0002-8036-3236>;

**Davyd Cherkaskyi** — Postgraduate Student, National Technical University «Dnipro Polytechnic», Dnipro, Ukraine

<https://orcid.org/0009-0003-8516-6252>.

© D.I. Prokopovych-Tkachenko, N.K. Zhumagalieva, D.N. Shchyotov, N.F. Mormul, D.A. Cherkaskyi

**Abstract.** The paper proposes an interpretable fuzzy model for evaluating information



security parameters of information systems under conditions of incomplete observations, heterogeneity of sources, and the prevalence of qualitative descriptions. The model is oriented toward the practice of regular management control in organizations of the Republic of Kazakhstan, including the public sector, financial, and educational institutions. The core idea is the separation of observed indicators (technical, organizational, and human factors) from latent security parameters related to confidentiality, integrity, and availability. A Mamdani fuzzy inference mechanism, accounting for rule weights and membership discounting during data gaps, is applied to transition from fuzzy observations to numerical estimates. The input vector includes 11 features: vulnerability and patch management, segmentation, privilege management, IDS coverage, SIEM correlation maturity, backup and recovery, endpoint protection, configuration and change management, incident response, the human factor, and an explicit indicator of observability and data quality. Linguistic variables and membership functions on a normalized scale are presented, along with rule base construction principles and tuning methods: the Delphi expert procedure, quantitative elimination of contradictions, rule weight optimization based on calibration data, and sensitivity analysis. Model quality is assessed by expert consensus (Kendall's coefficient), resilience to noise and gaps (Monte Carlo, coefficient of variation), and practical validity compared to incident data and independent audits of the information security management system. A demonstration case was conducted for a typical public sector organization with a distributed branch network, showing how qualitative observations and incomplete telemetry are transformed into numerical security parameters and risk levels, and how sensitivity analysis guides the prioritization of measures. Limitations and development prospects are discussed, including integration with Zero Trust architecture and the use of multimodal AI to combine logs, network flows, and binary artifacts visualized via the Byte2Image approach.

**Keywords:** information security, risk management, fuzzy logic, incomplete data, expert evaluations, Mamdani inference, IDS, SIEM, public sector, Kazakhstan, resilience

**For citation:** D.I. Prokopovych-Tkachenko, N.K. Zhumagalieva, D.N. Shchytov, N.F. Mormul, D.A. Cherkaskyi (2026). Fuzzy Model for Evaluating Information Security Parameters of Information Systems under Incomplete and Qualitative Data: Construction Methodology, Rule Base Tuning, and Demonstration Case for Organizations // International Journal of Information and Communication Technology. Vol. 7. No. 26. Pp. 279–304. <https://doi.org/10.54309/IJICT.2026.26.2.018>. (In Russ.).

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

**ТОЛЫҚ ЕМЕС ЖӘНЕ САПАЛЫҚ ДЕРЕКТЕР ЖАҒДАЙЫНДА АҚПАРАТТЫҚ ЖҮЙЕЛЕРДІҢ АҚПАРАТТЫҚ ҚАУІПСІЗДІК ПАРАМЕТРЛЕРІН БАҒАЛАУДЫҢ БҰЛЫҢҒЫР МОДЕЛІ: ҚҰРУ ӘДІСТЕМЕСІ, ЕРЕЖЕЛЕР БАЗАСЫН БАПТАУ ЖӘНЕ ҰЙЫМДАРҒА АРНАЛҒАН ДЕМОНСТРАЦИЯЛЫҚ КЕЙС.**

*Д.И. Прокопович-Ткаченко<sup>1\*</sup>, Н.К. Жумагалиева<sup>2</sup>, Д.Н. Щитов<sup>1</sup>,*



**Н.Ф. Мормуль<sup>1</sup>, Д.А. Черкасский<sup>3</sup>**<sup>1</sup>Кеден ісі және қаржы университеті, Днепр, Украина;<sup>2</sup>Satbayev University, Алматы, Қазақстан;<sup>3</sup>Днепр политехникасы ұлттық техникалық университеті, Днепр, Украина.

E-mail: omega2417@gmail.com.

**Прокопович-Ткаченко Дмитрий** — техника ғылымдарының кандидаты, доцент, Кеден ісі және қаржы университетінің киберқауіпсіздік және ақпараттық технологиялар кафедрасының меңгерушісі; «Украина Ұлттық құқықтық ғылымдар академиясының Ақпарат, қауіпсіздік және құқық институты» мемлекеттік ғылыми мекемесінің аға ғылыми қызметкері; Ақпараттық-коммуникациялық технологиялар мемлекеттік университетінің киберқауіпсіздік жүйелері мен технологиялары кафедрасының докторанты, Днепр, Украина

E-mail: omega2417@gmail.com, <https://orcid.org/0000-0002-6590-3898>;**Жұмағалиева Назым** — аспирант, Satbayev University, Алматы, Қазақстан<https://orcid.org/0000-0003-1130-3405>;

**Щитов Дмитрий** — экономика ғылымдарының кандидаты, менеджмент және әкімшілендіру кафедрасының аға оқытушысы (КҰМӨУ Днепр менеджмент және бизнес факультеті), Кеден ісі және қаржы университетінің докторанты, Днепр, Украина

<https://orcid.org/0000-0003-4306-8016>;

**Мормуль Николай** — техника ғылымдарының кандидаты, Кеден ісі және қаржы университетінің киберқауіпсіздік және ақпараттық технологиялар кафедрасының доценті, Днепр, Украина

<https://orcid.org/0000-0002-8036-3236>;

**Черкасский Давид** — аспирант, «Днепр политехникасы» ұлттық техникалық университеті, Днепр, Украина

<https://orcid.org/0009-0003-8516-6252>.

© Д.И. Прокопович-Ткаченко, Н.К. Жумағалиева, Д.Н. Щитов, Н.Ф. Мормуль, Д.А. Черкасский

**Аннотация.** Жұмыста бақылаулардың толық еместігі, дереккөздердің әртүрлілігі және сапалық сипаттамалардың басымдылығы жағдайында ақпараттық жүйелердің ақпараттық қауіпсіздік параметрлерін бағалауға арналған интерпретацияланатын бұлыңғыр модель ұсынылған. Модель Қазақстан Республикасының ұйымдарындағы, соның ішінде мемлекеттік сектордағы, қаржы және білім беру мекемелеріндегі тұрақты басқарушылық бақылау тәжірибесіне бағытталған. Негізгі идея бақыланатын индикаторларды (техникалық, ұйымдастырушылық және адами факторлар) құпиялылыққа, тұтастыққа және қолжетімділікке қатысты жасырын қауіпсіздік параметрлерінен бөлуге негізделген. Бұлыңғыр бақылаулардан сандық бағалауларға өту үшін ережелердің салмағы мен деректердің жетіспеушілігі кезіндегі мүшелік функцияларын дисконттауды ескеретін Мамдани бұлыңғыр қоры-



тынды механизмі қолданылады. Кіріс векторы 11 белгіні қамтиды: осалдықтар мен патчтарды басқару, сегментация, артықшылықтарды басқару, басып кіруді анықтау жүйесімен (IDS) қамту, қауіпсіздік оқиғаларын басқару жүйесіндегі (SIEM) корреляцияның жетілуі, резервтік көшіру және қалпына келтіру, соңғы нүктелерді қорғау, конфигурациялар мен өзгерістерді басқару, инциденттерге ден қою, адами фактор, сондай-ақ бақылаудың және деректер сапасының нақты индикаторы. Нормаланған шкаладағы лингвистикалық айнымалылар мен мүшелік функциялары ұсынылған, ережелер базасын құру принциптері мен баптау әдістері келтірілген: Дельфи сарапшылық процедурасы, қайшылықтарды сандық жою, калибрлеу деректері бойынша ережелер салмағын оңтайландыру және сезімталдықты тексеру. Модель сапасы сарапшылардың келісімі (Кендалл коэффициенті), шу мен оқшылықтарға төзімділік (Монте-Карло, вариация коэффициенті), сондай-ақ инциденттер деректерімен және ақпараттық қауіпсіздікті басқару жүйесінің тәуелсіз аудитімен салыстырғандағы практикалық негізділігі бойынша бағаланады. Бөлімшелерінің тармақталған желісі бар типтік мемлекеттік сектор ұйымы үшін демонстрациялық кейс жүргізілді: сапалық бақылаулар мен толық емес телеметрияның сандық қауіпсіздік параметрлеріне және тәуекел деңгейіне қалай айналатыны, сондай-ақ сезімталдық негізінде іс-шаралардың басымдығы қалай қалыптасатыны көрсетілген. Zero Trust архитектура-сымен интеграциялауды және Byte2Image тәсілімен визуализацияланатын логтарды, желілік ағындарды және бинарлық артефактілерді біріктіру үшін мультимодальды жасанды интеллектті пайдалануды қоса алғанда, шектеулер мен даму перспективалары бөлек талқыланды.

**Түйінді сөздер:** ақпараттық қауіпсіздік, тәуекелдерді басқару, бұлыңғыр логика, толық емес деректер, сарапшылық бағалау, Мамдани қорытындысы, IDS, SIEM, мемлекеттік сектор, Қазақстан, тұрақтылық

**Дәйексөздер үшін:** Д.И. Прокопович-Ткаченко, Н.К. Жумагалиева, Д.Н. Щитов, Н.Ф. Мормуль, Д.А. Черкасский (2026). Толық емес және сапалық деректер жағдайында ақпараттық жүйелердің ақпараттық қауіпсіздік параметрлерін бағалаудың бұлыңғыр моделі: құру әдістемесі, ережелер базасын баптау және ұйымдарға арналған демонстрациялық кейс // Халықаралық ақпараттық және коммуникациялық технологиялар журналы. Т. 7. No. 26. Б. 279–304. <https://doi.org/10.54309/IJICT.2026.26.2.018>. (Орыс. тіл.).

**Мүдделер қақтығысы:** авторлар мүдделер қақтығысының жоқтығын мәлімдейді.

## НЕЧЕТКАЯ МОДЕЛЬ ОЦЕНИВАНИЯ ПАРАМЕТРОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ В УСЛОВИЯХ НЕПОЛНЫХ И КАЧЕСТВЕННЫХ ДАННЫХ: МЕТОДИКА ПОСТРОЕНИЯ, НАСТРОЙКА БАЗЫ ПРАВИЛ И ДЕМОСТРАЦИОННЫЙ КЕЙС ДЛЯ ОРГАНИЗАЦИЙ.

*Д.И. Прокопович-Ткаченко<sup>1\*</sup>, Н.К. Жумагалиева<sup>2</sup>, Д.Н. Щитов<sup>1</sup>,*



**Н.Ф. Мормуль<sup>1</sup>, Д.А. Черкасский<sup>3</sup>**

<sup>1</sup>Университет таможенного дела и финансов, Днепр, Украина;

<sup>2</sup>Satbayev University, Алматы, Казахстан;

<sup>3</sup>Национальный технический университет Днепровская политехника, Днепр, Украина.

E-mail: omega2417@gmail.com.

**Прокопович-Ткаченко Дмитрий** — кандидат технических наук, доцент, заведующий кафедрой кибербезопасности и информационных технологий Университета таможенного дела и финансов; старший научный сотрудник Государственного научного учреждения «Институт информации, безопасности и права Национальной академии правовых наук Украины»; докторант кафедры систем и технологий кибербезопасности Государственного университета информационно-коммуникационных технологий, Днепр, Украина

E-mail: omega2417@gmail.com, <https://orcid.org/0000-0002-6590-3898>;

**Жумагалиева Назым** — аспирант, Satbayev University, Алматы, Казахстан

<https://orcid.org/0000-0003-1130-3405>;

**Щитов Дмитрий** — кандидат экономических наук, старший преподаватель кафедры менеджмента и администрирования (Днепровский факультет менеджмента и бизнеса КНУКИМ), докторант Университета таможенного дела и финансов, Днепр, Украина

<https://orcid.org/0000-0003-4306-8016>;

**Мормуль Николай** — кандидат технических наук, доцент кафедры кибербезопасности и информационных технологий, Университет таможенного дела и финансов, Днепр, Украина

<https://orcid.org/0000-0002-8036-3236>;

**Черкасский Давид** — аспирант, Национальный технический университет «Днепровская политехника», Днепр, Украина

<https://orcid.org/0009-0003-8516-6252>.

© Д.И. Прокопович-Ткаченко, Н.К. Жумагалиева, Д.Н. Щитов, Н.Ф. Мормуль, Д.А. Черкасский

**Аннотация.** В работе предложена интерпретируемая нечёткая модель для оценивания параметров информационной безопасности информационных систем при неполноте наблюдений, разнородности источников и преобладании качественных описаний. Модель ориентирована на практику регулярного управленческого контроля в организациях Республики Казахстан, включая государственный сектор, финансовые и образовательные учреждения, где одновременно присутствуют требования к защите персональных данных, формальные регламенты процессов и реальная неоднородность телеметрии. В основу положена идея разделения наблюдаемых индикаторов (технических, организационных и человеческих факторов) и скрытых параметров безопасности, связанных с конфиденциальностью, це-

лостностью и доступностью. Для перехода от размытых наблюдений к численным оценкам применяется механизм нечёткого вывода Мамдани с учетом веса правил и дисконтирования принадлежностей при пропусках данных. Входной вектор включает 11 признаков: управление уязвимостями и патчами, сегментация, управление привилегиями, покрытие системой обнаружения вторжений (IDS), зрелость корреляции в системе управления событиями безопасности (SIEM), резервное копирование и восстановление, защита конечных точек, управление конфигурациями и изменениями, реагирование на инциденты, человеческий фактор, а также явный индикатор наблюдаемости и качества данных. Представлены лингвистические переменные и функции принадлежности на нормированной шкале, приведены принципы построения базы правил, методы настройки: экспертная процедура Дельфи, количественная элиминация противоречий, оптимизация весов правил по калибровочным данным и проверка чувствительности. Качество модели оценивается по согласованности экспертов (коэффициент Кендалла), устойчивости к шуму и пропускам (Монте-Карло, коэффициент вариации), а также по практической валидности в сопоставлении с данными инцидентов и независимым аудитом системы менеджмента информационной безопасности. Проведен демонстрационный кейс для типовой организации государственного сектора с распределенной сетью филиалов: показано, как качественные наблюдения и неполная телеметрия преобразуются в численные параметры безопасности и уровень риска, а также как на основе чувствительности формируется приоритизация мероприятий. Отдельно обсуждены ограничения и перспективы развития, включая интеграцию с архитектурой Zero Trust и использование мультимодального искусственного интеллекта для объединения логов, сетевых потоков и бинарных артефактов, визуализируемых подходом Byte2Image.

**Ключевые слова:** информационная безопасность, управление рисками, нечёткая логика, неполные данные, экспертные оценки, вывод Мамдани, IDS, SIEM, государственный сектор, Казахстан, устойчивость

**Для цитирования:** Д.И. Прокопович-Ткаченко, Н.К. Жумагалиева, Д.Н. Щитов, Н.Ф. Мормуль, Д.А. Черкасский (2026). Нечеткая модель оценивания параметров информационной безопасности информационных систем в условиях неполных и качественных данных: методика построения, настройка базы правил и демонстрационный кейс для организаций // Международный журнал информации и коммуникационной технологии. Т. 7. No. 26. Стр. 279–304. <https://doi.org/10.54309/IJICT.2026.26.2.018>. (На русс.).

**Конфликт интересов:** авторы заявляют об отсутствии конфликта интересов.

## Введение.

Оценивание параметров информационной безопасности (далее-ИБ) в реальных организациях редко опирается на полный набор измерений. Даже при наличии развитого мониторинга значимая часть информации о защите имеет качественный характер: результаты аудита процессов, зрелость процедур, дисциплина исполнения политики доступа, фактическое применение регламентов, культура реагирования и

человеческий фактор. В сетях электронных коммуникаций, поддерживающих критичные сервисы (электронные услуги, платежи, образовательные платформы), проблема усугубляется множеством гетерогенных сегментов, отличающихся по технологическому уровню и наблюдаемости. Практика показывает, что при одинаково декларируемых требованиях зрелость защиты на центральной площадке и в филиалах может различаться кратно, а журналы событий и записи мониторинга поступают в систему управления событиями безопасности фрагментарно, что затрудняет сопоставимые оценки состояния ИБ и управленческую приоритезацию мер. Для организаций Республики Казахстан дополнительным стимулом к формализации оценки выступают требования национального правового поля и государственной политики в области кибербезопасности. Регулирование в сфере информатизации и защиты персональных данных задает обязательность процессов учета, контроля и ответственности, а государственная концепция кибербезопасности ориентирует организации на системность и измеримость мер защиты (Sugeno, 1985; Zimmermann, 2001).

В прикладной плоскости эти требования чаще всего реализуются через построение системы менеджмента информационной безопасности на базе международных стандартов и их национальных версий (Goldberg, 1989; International Organization for Standardization, 2022), а также через риск-ориентированный подход к управлению контролями, включая применение руководств по управлению рисками и оцениванию последствий (International Organization for Standardization, 2022; Joint Task Force Transformation Initiative, 2012). Однако традиционные инструменты оценивания риска-матрицы «вероятность×ущерб», чек-листы зрелости и простые балльные шкалы-страдают методологическим разрывом между качественными наблюдениями и требованием численной отчетности. В этой зоне возникает типовой управленческий парадокс: руководству нужен сопоставимый численный показатель риска и аргументированная приоритезация работ, тогда как специалисты на местах располагают неравномерными данными и зачастую вынуждены опираться на лингвистические формулировки (низкий, приемлемый, зрелый, фрагментарный). Попытка заменить такие описания точными числами без учета неопределенности приводит либо к ложной точности, либо к некорректному «усреднению» пропусков, что особенно опасно при принятии решений о сокращении бюджетов на мониторинг и реагирование. Нечёткая логика, предложенная в классической постановке Л. А. Заде (Abubakar et al., 2020), предоставляет математический аппарат для перехода от лингвистических описаний к численным оценкам, сохраняя интерпретируемость и возможность экспертного контроля. Механизмы вывода Мамдани (Ahmed et al., 2020) и Сугэно (Bengio et al., 2020) широко применяются в задачах управления, надежности и качества, где наблюдения неполны или содержат субъективность, а модель должна быть понятна специалистам предметной области (Center for Internet Security, 2021; Decree of the Government of the Republic of Kazakhstan, 2017). В задачах ИБ нечёткие модели используются для оценивания риска, корреляции событий, приоритезации реагирования и объединения разнородных индикаторов (Law of the

Republic of Kazakhstan No. 418-V, 2015; Miller et al., 2011). Их прикладное преимущество заключается в том, что модель может быть построена при ограниченном объеме «исторической» статистики, а затем уточняться по мере накопления данных, не разрушая логическую структуру принятия решений и сохраняя объяснимость. Вместе с тем практическое внедрение нечёткой модели в организации требует ответов на прикладные вопросы: какие признаки выбрать, как формально учесть неполноту телеметрии, как выявлять и устранять противоречия в базе правил, как измерять согласованность экспертов и устойчивость вывода к шуму и пропускам. Кроме того, модель должна быть совместима с процессами системы менеджмента информационной безопасности и с инструментами мониторинга, в частности с системой обнаружения вторжений и системой управления событиями безопасности (Klir et al., 1995), а также опираться на признанные практики контроля и мониторинга защитных мер (Kennedy et al., 1995). Отдельной проблемой является то, что качество данных мониторинга не следует «прятать» внутри отдельных показателей: оно само должно выступать параметром модели, поскольку слабая наблюдаемость резко повышает вероятность незаметной компрометации и снижает достоверность управленческих выводов.

Цель работы состоит в разработке практической нечёткой модели определения параметров ИБ информационных систем в условиях неполных и качественных данных, ориентированной на типовые организации Республики Казахстан. Для достижения цели формируется набор входных признаков (технических, организационных и отражающих человеческий фактор) и вводится индикатор наблюдаемости; задаются лингвистические переменные и функции принадлежности, пригодные для аудита и мониторинга; строится база правил нечёткого вывода Мамдани с определением выходных параметров безопасности и риска; разрабатывается методика настройки, включающая экспертную процедуру Дельфи (Nataraj et al., 2011), элиминацию противоречий и оптимизацию весов правил с учетом калибровочных данных (Rose et al., 2020; Ross, 2010); предлагаются метрики качества, отражающие согласованность экспертов и устойчивость результата к шуму и пропускам; проводится демонстрационный кейс, показывающий трансляцию размытых наблюдений в численные оценки и уровни риска с опорой на сценарный принцип и привязку к тактикам атакующих (Law of the Republic of Kazakhstan No. 94-V, 2013).

### **Материалы и методы.**

В разделе «материалы и методы» описывается построение интерпретируемой нечёткой модели оценивания параметров информационной безопасности при слабой наблюдаемости и преобладании качественных оценок. Методологическая схема включает последовательные этапы: формирование набора входных индикаторов, отражающих технические, организационные и поведенческие аспекты защиты, и их нормирование на единой шкале; задание лингвистических переменных и функций принадлежности (треугольных и трапециевидных) как прозрачного для экспертов инструмента представления неопределённости; формальное учёт неполноты телеметрии через коэффициенты полноты и дисконтирование принадлежностей при пропусках наблюдений; построение базы правил на основе сценарного принципа и причин-

но-следственных цепочек инцидентов; реализация нечёткого вывода по Мамдани с агрегированием по операциям минимума/максимума и дефаззификацией центроидным методом, а также расчёт интегрального уровня риска как функции «недостатка» параметров конфиденциальности, целостности и доступности. Настройка модели выполняется комбинированно: первичная калибровка параметров и правил проводится экспертно с применением процедуры Дельфи, далее выполняется выявление и устранение противоречий в правилах и, при наличии калибровочных данных, оптимизация весов правил эволюционными методами; качество оценивается по согласованности экспертных суждений, устойчивости результата к шуму и пропускам (в том числе методом Монте-Карло) и практической валидности в сопоставлении с данными мониторинга и независимого аудита. Такая конструкция обеспечивает воспроизводимость результатов и управляемую адаптацию модели при изменении инфраструктуры и контуров мониторинга, включая подсистемы обнаружения вторжений и управления событиями безопасности. (Abubakar et al., 2020; Freund et al., 2015; Goldberg, 1989; Law of the Republic of Kazakhstan No. 94-V, 2013; Nataraj et al., 2011; Ross, 2010).

*Система входных признаков*

Пусть состояние защищенности информационной системы описывается вектором наблюдаемых признаков

$$\mathbf{X} = (x_1, x_2, \dots, x_{11}), \quad x_j \in [0,10], \quad (1)$$

где шкала 0–10 задает нормированную оценку индикатора по результатам аудита, опросов и технической телеметрии. Выбор признаков выполнен с учетом практик СМИБ (Goldberg, 1989; International Organization for Standardization, 2022), типовых контролей (Kennedy et al., 1995) и доступности данных в смешанных ИТ-сетях.

Набор признаков строится так, чтобы:

- охватывать ключевые причины инцидентов: уязвимости, привилегии, сегментация, наблюдаемость, реагирование;
- быть измеримым с приемлемой стоимостью: часть признаков берется из SIEM/IDS, часть из аудита процессов;
- допускать частичную наблюдаемость без разрушения модели: пропуски отражаются явно через коэффициенты полноты.

Признаки  $x_1 - x_7$  преимущественно технические,  $x_8 - x_9$  отражают организационные процессы,  $x_{10}$  — человеческий фактор, а моделирует наблюдаемость, то есть насколько уверенно можно доверять остальным измерениям при наличии пропусков и разрывов телеметрии.

Таблица 1 – Входные признаки модели и лингвистические термы.

Признак (интерпретация)	Термы (пример)
Управление уязвимостями и патчами (скорость закрытия, охват активов)	низкое, среднее, высокое
Сегментация и контроль сетевых потоков (VLAN, правила межсегментного доступа)	слабая, достаточная, строгая
Управление привилегиями (учет, разделение ролей, многофакторная аутентификация)	неуправляемое, частичное, зрелое
Покрытие обнаружения IDS (периметр и внутренние сегменты, актуальность правил)	низкое, среднее, высокое
Зрелость корреляции в SIEM (нормализация, сценарии, реакция по правилам)	начальная, рабочая, развитая
Резервное копирование и восстановление (регулярность, тесты восстановления)	слабое, приемлемое, надежное
Защита конечных точек (антивирус/контроль поведения, харднинг, контроль приложений)	низкая, средняя, высокая
Управление конфигурациями и изменениями (инвентаризация, дрейф, регламенты)	хаотичное, частичное, регламентированное
Реагирование на инциденты (планы, роли, обучение, постинцидентный анализ)	формальное, рабочее, зрелое
Человеческий фактор (обучение, тесты на фишинг, дисциплина соблюдения)	рискованный, средний, устойчивый
Наблюдаемость и качество данных (покрытие активов, потери логов, полнота полей)	низкая, средняя, высокая

### Лингвистические переменные и функции принадлежности

Для каждого признака  $x_j$  задается множество термов  $T_j = \{t_{j1}, t_{j2}, t_{j3}\}$  и соответствующие функции принадлежности  $\mu_{j\ell}(x_j) \in [0,1]$ . В работе применяются треугольные и трапециевидные функции как наиболее прозрачные для экспертов [5, 6]. Для универсальности вводим трапециевидную функцию:

$$\mu(x; a, b, c, d) = \begin{cases} 0, & x \leq a, \\ \frac{x-a}{b-a}, & a < x \leq b, \\ 1, & b < x \leq c, \\ \frac{d-x}{d-c}, & c < x \leq d, \\ 0, & x > d. \end{cases} \quad (2)$$

Параметры  $(a, b, c, d)$  выбираются экспертно. Принцип выбора следующий: значения около 0 соответствуют отсутствию практики или крайне низкому охвату,

значения около 10 — устойчиво работающей практике с доказуемым контролем, а середина шкалы соответствует «частичной» реализации, типичной для организаций, находящихся в переходном состоянии. Такая нормировка обеспечивает переносимость модели между подразделениями и организациями, сохраняя возможность уточнения порогов.

Пример для признака управления уязвимостями и патчами  $x_1$ :

$$\mu_{1,низк}(x_1) = \mu(x_1; 0,0,2,4), \quad \mu_{1,сред}(x_1) = \mu(x_1; 2,4,6,8), \quad \mu_{1,выс}(x_1) = \mu(x_1; 6,8,10,10).$$

Аналогично задаются функции для остальных признаков. В практической настройке полезно вести «паспорт термов»: для каждого термина фиксируются наблюдаемые критерии (например, задержка патчей, доля активов в инвентаризации, частота тестов восстановления) и допустимые источники данных. Это снижает риск того, что разные эксперты интерпретируют одну и ту же шкалу по-разному.

Для перехода от нормированных входных оценок признаков на единой шкале 0–10 к лингвистическим термам в модели используются треугольные и трапециевидные функции принадлежности. Такое задание  $\mu(x)$  обеспечивает интерпретируемость (понятные пороги и зоны неопределённости), а перекрытие термов позволяет корректно учитывать «частичную истинность» промежуточных состояний при аудитах и разнородной телеметрии.

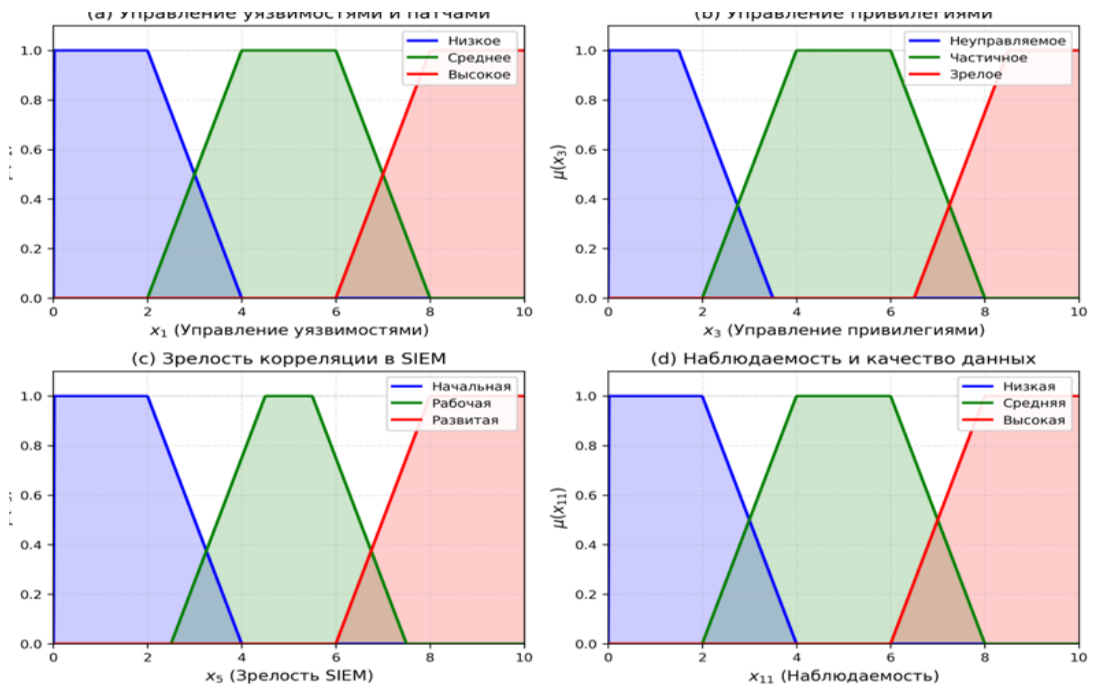


Рис. 1. Функции принадлежности лингвистических переменных

На рисунке 1 приведены примеры функций принадлежности для четырёх репрезентативных признаков: (а)  $x_1$  - управление уязвимостями и патчами (термы: «низкое», «среднее»,

«высокое»); (б)  $x_3$  - управление привилегиями («неуправляемое», «частичное», «зрелое»); (с)  $x_5$  - зрелость корреляции в SIEM («начальная», «рабочая», «развитая»); (д)  $x_{11}$  - наблюдаемость и качество данных («низкая», «средняя», «высокая»). Перекрывающиеся переходные области отражают неопределённость и обеспечивают плавную смену термов при изменении значения показателя, что критично для задач оценивания ИБ при неполных/качественных данных

#### *Моделирование неполноты данных и доверия к наблюдениям*

Пусть по каждому признаку известно значение  $x_j$  и коэффициент полноты  $q_j \in [0,1]$ , где  $q_j = 1$  означает полностью наблюдаемый признак, а  $q_j \rightarrow 0$  соответствует пропуску или крайне низкому доверию. Неполнота проявляется в типовых ситуациях:

часть активов не входит в инвентаризацию, поэтому аудит «не видит» реальные версии программного обеспечения;

логи из филиалов теряются по каналу, буферизации нет, и события до SIEM не доходят;

поля событий неполны (нет идентификатора пользователя, узла, процесса), что разрушает корреляцию;

часть контуров мониторинга отключается «временно», но временное становится постоянным.

Для учета неполноты используем дисконтирование функций принадлежности по аналогии с подходами учета доверия (Freund et al., 2015):

$$\tilde{\mu}_{j\ell}(x_j) = q_j \mu_{j\ell}(x_j) + (1 - q_j) \pi_{j\ell}, \quad (3)$$

где  $\pi_{j\ell}$  — базовая априорная принадлежность терма при отсутствии данных. В практической реализации  $\pi_{j\ell} = 1/|T_j|$  обеспечивает нейтральность: при пропуске модель не «угадывает» терм, а отражает незнание.

Коэффициенты  $q_j$  могут вычисляться автоматически. Например, для наблюдаемости и доверия к данным SIEM используют долю событий, поступивших без задержки, процент событий с заполненными ключевыми полями, а также долю активов, с которых логи реально собираются (Klir et al., 1995; Miller et al., 2011). Для признаков, определяемых аудитом процессов,  $q_j$  можно связывать с полнотой выборки документов, числом опрошенных подразделений и частотой обновления регламентов.

#### *Выходные параметры безопасности и структура вывода*

Выход модели включает три параметра безопасности и агрегированный риск:

$$\mathbf{y} = (y_C, y_I, y_A, y_R), \quad y_i \in [0,1],$$

где  $y_C$  — оценка конфиденциальности,  $y_I$  — целостности,  $y_A$  — доступности,  $y_R$  — интегральный уровень риска. Для каждого выхода задаются термы, например: *низкий, средний, высокий*. Их функции принадлежности задаются на оси трапециевидно/треугольно по (2).

Нечеткая база правил состоит из правил вида:

$$\mathcal{R}_k: \text{если } x_1 \text{ есть } A_{k1} \wedge \dots \wedge x_{11} \text{ есть } A_{k,11} \text{ то } y_R \text{ есть } B_k, \quad \text{вес } w_k,$$

где  $A_{ki}$  — выбранный терм для признака,  $x_j$ ,  $B_k$  — терм для выхода,  $w_k \in [0,1]$  — вес правила. В работе используется вывод Мамдани (Ahmed et al., 2019), где степень срабатывания правила определяется операцией минимума:

$$\alpha_k(\mathbf{x}) = w_k \cdot \min_{j=1, \dots, 11} \tilde{\mu}_{A_{kj}}(x_j). \quad (4)$$

Агрегированная функция принадлежности для выхода  $y_R$  определяется операцией максимума по правилам:

$$\mu_R(r) = \max_{k=1, \dots, K} \min(\alpha_k(\mathbf{x}), \mu_{B_k}(r)), \quad r \in [0,1]. \quad (5)$$

Четкая оценка риска вычисляется центроидной дефаззификацией:

$$\hat{y}_R = \frac{\int_0^1 r \mu_R(r) dr}{\int_0^1 \mu_R(r) dr}. \quad (6)$$

Аналогично формируются выходы  $\hat{y}_C$ ,  $\hat{y}_I$ ,  $\hat{y}_A$  (возможны отдельные подбазы правил). Для практической эксплуатации удобно разделить: нечётким выводом получить параметры безопасности, а риск вычислить как агрегированную функцию «недостатка безопасности», используя риск-ориентированную формулу:

$$\hat{y}_R = \sigma(\beta_0 + \beta_C(1 - \hat{y}_C) + \beta_I(1 - \hat{y}_I) + \beta_A(1 - \hat{y}_A)), \quad (7)$$

где  $\sigma(z) = 1/(1 + e^{-z})$  — логистическая функция, а коэффициенты  $\beta$  настраиваются по историческим данным инцидентов при наличии, либо задаются экспертно (Jensen et al., 2007; Joint Task Force Transformation Initiative, 2012). Такой двухслойный подход повышает управляемость: экспертно-понятные параметры безопасности остаются «основой разговора», а риск становится воспроизводимым итоговым показателем.

*Построение базы правил: сценарный принцип и привязка к тактикам атак*

Для предотвращения комбинаторного взрыва правил применяется сценарный принцип. База правил организуется вокруг типовых сценариев, согласованных с практиками моделирования угроз и тактик атакующих (Law of the Republic of Kazakhstan No. 94-V, 2013). Пример сценария: компрометация учетной записи через фишинг (связь с человеческим фактором), повышение привилегий при слабом управлении доступом, латеральное перемещение при слабой сегментации, закрепление и скрытность при недостаточной корреляции событий, разрушение или шифрование данных и восстановление по бэкапам.

В сценарном принципе каждое правило должно отвечать на вопрос: какое сочетание факторов делает сценарий *вероятным* и *опасным*. Это позволяет:

*уменьшить количество правил без потери смысла;*

*обеспечить объяснимость, так как каждое правило связано с конкретной практической историей;*

*проще выявлять противоречия: если два правила описывают один и тот же сценарий, их следствия должны быть согласованы.*

*Настройка базы правил*

*Экспертное согласование и метод Дельфи*

Первичная база правил и параметры функций принадлежности формируются экспертами из числа специалистов по ИБ, сетевых администраторов и владельцев процессов. Для снижения разброса применяется итерационная процедура Дельфи (Nataraj et al., 2011): независимое заполнение анкет, сведение расхождений, обсуждение крайних значений, повторный раунд до стабилизации. В анкетах целесообразно фиксировать не только пороги термов, но и примеры наблюдений, соответствующих термам, а также «типичные исключения» (например, временное отключение логирования, обслуживание критического сервиса без окна).

Согласованность группы оценивается коэффициентом Кендалла:

$$W = \frac{12S}{m^2(n^3 - n)}, \quad S = \sum_{i=1}^n (R_i - \bar{R})^2, \quad (8)$$

где  $m$  — число экспертов,  $n$  — число оцениваемых объектов (например, сценариев или подразделений),  $R_i$  — сумма рангов объекта  $i$ . Значения  $W \rightarrow 1$  соответствуют высокой согласованности; при низких значениях следует уточнить критерии термов и источники данных. Важно подчеркнуть: низкий часто является не «ошибкой экспертов», а признаком неоднозначности шкал и различий в контексте подразделений, что необходимо отразить либо в уточнении термов, либо в отдельной калибровке для классов активов.

#### *Элиминация противоречий и конфликтных правил*

Противоречия возникают, когда два правила имеют близкие посылки, но различные или несовместимые следствия. Для количественного выявления вводится метрика конфликта между правилами  $k$  и  $l$ :

$$\text{conf}(k, l) = \left( \prod_{j=1}^{11} \text{sim}(A_{kj}, A_{lj}) \right) \cdot \text{dist}(B_k, B_l), \quad (9)$$

где  $\text{sim}(\cdot)$  — мера сходства термов (1 при совпадении, 0.5 при соседних термах, 0 иначе), а  $\text{dist}(\cdot)$  — расстояние между термами выхода (0 для совпадения, 1 для противоположных). Правила с высокими значениями подлежат пересмотру.

Практически пересмотр выполняется одним из способов:

уточнение области применимости: добавление условий, чтобы правила «разошлись» по сценариям;

гармонизация следствия: замена термина выхода на промежуточный при равновесии мнений;

иерархизация: повышение веса правила для более критичного сценария и снижение веса для менее критичного.

#### *Оптимизация весов правил по калибровочным данным*

Для тонкой настройки вводятся веса  $w_k$  решается задача оптимизации по калибровочной выборке, где  $\{(\mathbf{x}^{(i)}, y^{(i)})\}_{i=1}^N$ , где  $y^{(i)}$  — эталонная оценка риска (например, по статистике инцидентов, по независимому аудиту, либо по комиссии):

$$\min_{\mathbf{w}} J(\mathbf{w}) = \sum_{i=1}^N (\hat{y}_R(\mathbf{x}^{(i)}; \mathbf{w}) - y^{(i)})^2 + \lambda \sum_{k=1}^K w_k^2, \quad 0 \leq w_k \leq 1. \quad (10)$$

Регуляризатор с параметром  $\lambda$  ограничивает чрезмерную концентрацию веса на отдельных правилах и повышает устойчивость. Для решения (International Organization for Standardization, 2022) целесообразны эволюционные методы-генетические алгоритмы (Rose et al., 2020) и метод роя частиц (Ross, 2010), поскольку поверхность ошибки может быть негладкой из-за операций min/max. В организациях с малым объемом данных допускается упрощение: оптимизируются веса только для «критичных» правил, связанных с наблюдаемостью, привилегиями и уязвимостями,

а остальные устанавливаются равными.

*Проверка чувствительности и устойчивости к шуму и пропускам*

Чувствительность модели по признаку  $x_j$  оценивается методом возмущений:

$$S_j = \mathbb{E}[|\hat{y}_R(\mathbf{x}) - \hat{y}_R(\mathbf{x} + \delta \mathbf{e}_j)|], \tag{11}$$

где  $\delta$  — малое возмущение,  $\mathbf{e}_j$  — единичный вектор. В практике полезно вычислять  $S_j$  отдельно для разных классов активов (например, периметр, внутренние сервисы, рабочие места филиалов), чтобы приоритезация мер учитывала реальную топологию и риски.

Устойчивость к шуму и пропускам оценивается Монте-Карло моделированием: в каждом прогоне случайно добавляется шум к входам и уменьшаются коэффициенты полноты  $q_j$ , после чего вычисляется коэффициент вариации выхода:

$$CV = \frac{\text{std}(\hat{y}_R)}{\text{mean}(\hat{y}_R)}, \tag{12}$$

Низкие значения CV свидетельствуют о стабильности вывода, что критично для управленческих решений: показатель риска не должен хаотично «скакать» при небольших изменениях оценок и временных пропусках телеметрии.

Для воспроизводимого расчёта параметров безопасности и интегральной оценки риска применяется конвейер нечёткого вывода Мамдани. Он позволяет объединять разнородные входные индикаторы и корректно учитывать неполноту наблюдений за счёт явного задания полноты данных по каждому признаку.

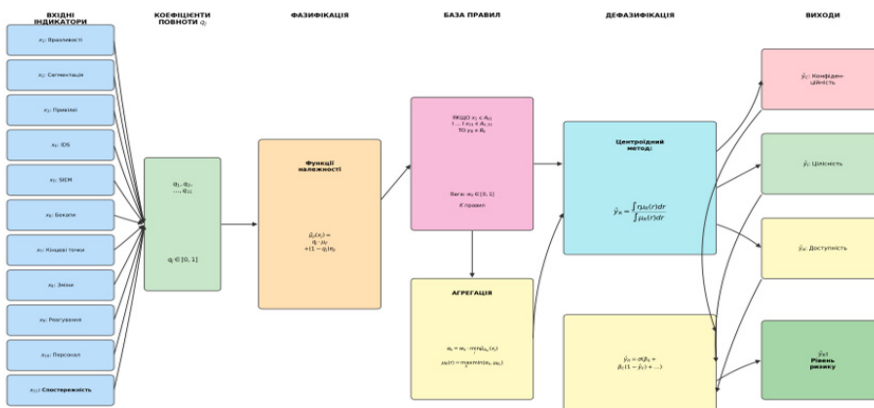


Рис. 2. Архитектура системы нечеткого вывода Мамдани

На рисунке 2 показаны основные этапы обработки: фаззификация входных индикаторов по функциям принадлежности, применение базы правил нечёткого вывода, агрегирование результатов и последующая дефаззификация. На выходе формируются интерпретируемые показатели по трём базовым свойствам безопасности и сводная оценка риска, пригодная для управленческого контроля даже при фрагментарной телеметрии.

Чтобы показать, как модель остаётся корректной при пропусках телеметрии и «размытых» оценках, на рисунке 3 визуализированы ключевые этапы получения итогового уровня риска: ослабление (дисконтирование) степеней принадлежности при неполных данных, формирование агрегированной оценки по базе правил и перевод результата в одно численное значение, удобное для отчётности и сравнения.

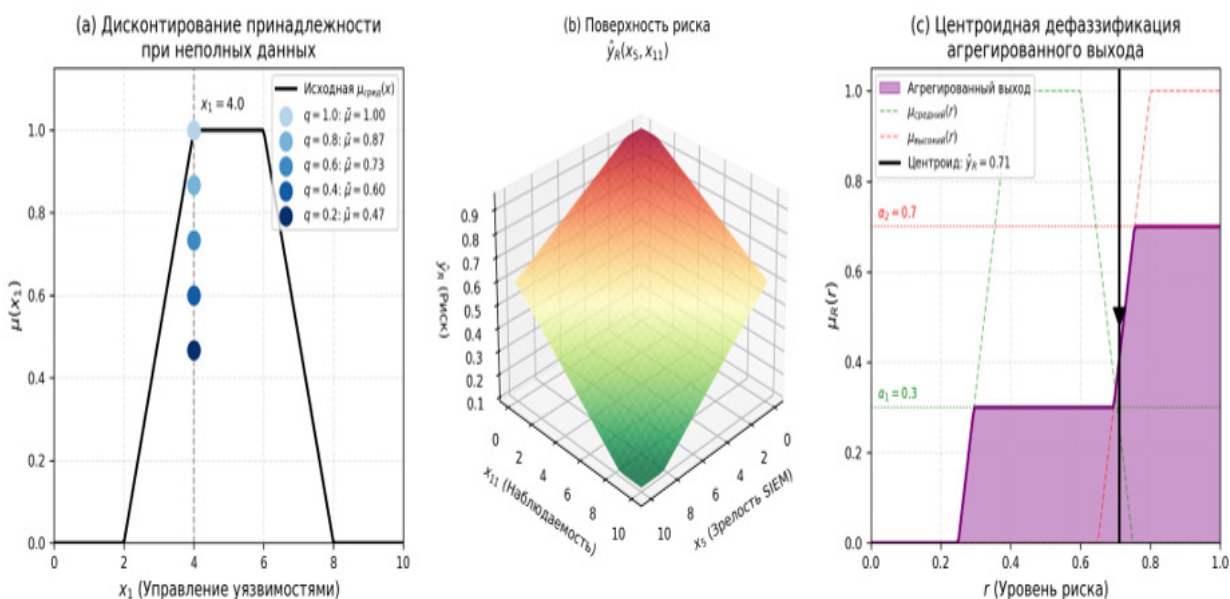


Рис. 3. Механизм нечёткого вывода: дисконтирование, поверхность риска и дефаззификация

На панели (a) показано, как при снижении полноты наблюдений уменьшаются «уверенность» модели в принадлежности показателя лингвистическим термам: даже при том же входном значении вклад термина становится слабее, что предотвращает ложную точность и занижение риска. Панель (b) иллюстрирует зависимость агрегированного риска от пары репрезентативных факторов (например, зрелости корреляции и наблюдаемости): риск возрастает при снижении зрелости и/или ухудшении наблюдаемости. На панели (c) представлено преобразование агрегированной нечёткой оценки в одно итоговое число методом дефаззификации, после чего показатель риска становится пригодным для управленческих решений и мониторинга динамики.

Разработанный методический аппарат обеспечивает воспроизводимое оце-

нивание параметров защищённости при слабой формализации и дефиците наблюдений за счёт согласованного сочетания трёх компонентов: нормированного набора входных индикаторов (технических, организационных и поведенческих), формализованного представления неопределённости через лингвистические переменные и функции принадлежности, а также механизма нечёткого вывода Мамдани с явным учётом неполноты данных посредством коэффициентов полноты и дисконтирования принадлежностей при пропусках. В результате формируется интерпретируемая модель, в которой каждая численная оценка опирается на прозрачные правила, согласуемые экспертами и привязываемые к типовым сценариям инцидентов; при этом устойчивость и корректность вывода поддерживаются процедурами настройки (экспертная сходимость по Дельфи, устранение противоречий, оптимизация весов правил по калибровочным данным) и метриками качества (согласованность экспертных суждений, чувствительность и устойчивость к шуму/пропускам) (Abubakar ET AL., 2020; Freund ET AL., 2015; Goldberg, 1989; Law of the Republic of Kazakhstan No. 94-V, 2013; Nataraj ET AL., 2011; Ross, 2010). Тем самым раздел «Методы» задаёт полный вычислительный конвейер от размытых наблюдений и неоднородной телеметрии к численным параметрам конфиденциальности, целостности и доступности и к интегральной оценке риска, пригодной для управленческой приоритизации мер и сопоставления подразделений. В следующем разделе «Результаты» этот конвейер применяется к демонстрационному кейсу типовой организации государственного сектора с распределённой сетью филиалов: приводятся исходные входные оценки и коэффициенты полноты, показывается пример расчёта принадлежностей с учётом неполноты, иллюстрируется работа репрезентативного подмножества правил и получаются итоговые значения параметров безопасности и уровня риска с последующей интерпретацией и формированием приоритетов мероприятий.

### **Результаты и обсуждение.**

В разделе «Результаты» представлена апробация разработанного вычислительного конвейера нечёткого вывода на демонстрационном кейсе типовой организации государственного сектора с распределённой сетью филиалов. Приводятся исходные входные оценки и полнота наблюдений, иллюстрируется получение итоговых параметров безопасности и интегральной оценки риска, после чего даётся интерпретация результата и формируется приоритизация мероприятий по улучшению с опорой на объяснимость и чувствительность модели.

*Демонстрационный кейс: организация государственного сектора Республики Казахстан*

Рассмотрим типовую организацию государственного сектора Республики Казахстан: региональное учреждение, оказывающее электронные услуги населению. Архитектура включает центральную площадку (серверы приложений и баз данных), несколько филиалов, каналы связи различного качества, смешанную инфраструктуру (рабочие места, серверы, сетевое оборудование разных поколений). Организация обрабатывает персональные данные граждан и действует в среде, где формально закреплены требования к защите данных и к управлению ИКТ, однако

фактическая зрелость процессов неоднородна (Sugeno, 1985; Zadeh, 1965).

Ключевая особенность кейса-неполная наблюдаемость: центральная площадка имеет относительно стабильное логирование, а филиалы предоставляют события с задержками и потерями. В результате SIEM «видит» периметр лучше, чем внутренние операции, и качество корреляции падает. Подобные условия типичны для распределенных организаций и часто приводят к эффекту ложной уверенности: контроль на периметре работает, но внутренние злоупотребления остаются «в тени».

В ходе первичного аудита и анализа телеметрии сформирован набор размытых наблюдений:

управление уязвимостями: патчи устанавливаются нерегулярно; задержка 30–60 дней; охват активов по инвентаризации около 70%;

сегментация: базовые виртуальные локальные сети настроены, но межсегментные правила часто расширяются временными исключениями;

управление привилегиями: многофакторная аутентификация для администраторов внедрена частично; сервисные учетные записи не всегда ротацируются;

IDS: датчики стоят на периметре, внутренний трафик покрыт ограниченно; обновление правил периодическое;

SIEM: корреляция развита на периметре, но сценарии по внутренним злоупотреблениям слабые;

резервное копирование: копии создаются регулярно, но тесты восстановления нерегулярны;

защита конечных точек: антивирус установлен везде, но расширенный поведенческий контроль покрывает только часть критичных рабочих мест;

изменения: инвентаризация неполная; конфигурационный дрейф выявляется эпизодически;

реагирование: план существует, но учения проводятся редко;

человеческий фактор: обучение проводится раз в год, результаты тестов на фишинг средние;

наблюдаемость: по филиалам потери событий достигают 20–30% в пиковые периоды.

Наблюдения переводятся в численные оценки (0–10) и коэффициенты полноты (0–1). Эта трансляция выполняется экспертной комиссией и фиксируется в протоколе СМИБ, что обеспечивает воспроизводимость: через квартал можно повторить оценку и сопоставить динамику. В таблице 2 приведен один возможный срез, согласованный группой.

Таблица 2 фиксирует исходный срез входных данных для демонстрационного кейса: по каждому из выбранных признаков приводятся (1) нормированная численная оценка состояния контроля по единой шкале 0–10 и (2) коэффициент полноты/доверия к наблюдениям по шкале 0–1, а также (3) краткий комментарий, который «привязывает» числа к фактам аудита и телеметрии (задержки патчей, исключения в сегментации, неполная инвентаризация, потери событий и т.д.). Срез формируется экспертной комиссией и закрепляется в протоколе СМИБ, что обеспечивает воспроиз-

изводимость: оценку можно повторять на регулярной основе и сопоставлять динамику между периодами и подразделениями. Практический смысл таблицы в том, что модель получает не только «оценку зрелости», но и качество исходных данных: при низкой полноте вывод не делает вид, что «всё измерено идеально», а аккуратно снижает вклад соответствующего признака в итоговую оценку.

Таблица 2 – Срез входных оценок для кейса и коэффициенты полноты

f	f	Комментарий
4.0	0.8	задержка патчей 30--60 дней, охват активов 70 %
5.5	0.7	сегментация есть, но много исключений
4.5	0.6	многофакторная аутентификация частично, слабая гигиена сервисных учеток
4.0	0.7	IDS преимущественно на периметре
3.5	0.6	SIEM: слабые сценарии внутренних злоупотреблений
6.0	0.8	бэкапы приемлемые, тесты нерегулярны
5.0	0.8	базовая защита везде, расширенная частично
3.5	0.5	инвентаризация неполная, дрейф фиксируется эпизодически
4.0	0.7	план есть, учения редки
4.5	0.9	обучение ежегодно, фишинг-тесты средние
4.0	0.6	потери событий 20--30% в пике

*Пример расчета степеней принадлежности и учета неполноты*

Для иллюстрации покажем вычисления по признаку  $x_1 = 4.0$ . По заданным функциям (низкое, среднее, высокое) получаем:

$$\mu_{1,\text{низк}}(4.0) = \mu(4.0; 0,0,2,4) = 0, \quad \mu_{1,\text{сред}}(4.0) = \mu(4.0; 2,4,6,8) = 1, \quad \mu_{1,\text{выс}}(4.0) = 0$$

С учетом неполноты  $q_1 = 0.8$  и нейтральных  $\pi=1/3$  по (3):

$$\tilde{\mu}_{1,\text{сред}} = 0.8 \cdot 1 + 0.2 \cdot \frac{1}{3} \approx 0.867, \quad \tilde{\mu}_{1,\text{низк}} = 0.8 \cdot 0 + 0.2 \cdot \frac{1}{3} \approx 0.067, \quad \tilde{\mu}_{1,\text{выс}} \approx 0.067.$$

Тем самым модель отражает реальную ситуацию: «формально» показатель попадает в средний терм, но из-за неполного охвата активов остается неопределенность, которая влияет на надежность вывода.

Аналогично рассчитываются принадлежности для остальных признаков. Особенно важен признак наблюдаемости  $x_{11}$ , поскольку он влияет на «силу» многих правил: при низком  $x_{11}$  и малых  $q_j$  даже хорошие оценки отдельных контролей не дают оснований считать риск низким, поскольку «хорошее» могло быть «невидимым».

*База правил: репрезентативное подмножество и смысловая интерпретация*

Полная база в реальном проекте обычно содержит 40–80 правил для риска (и отдельные подбазы для параметров конфиденциальности, целостности, доступности). Ниже приведены примеры, отражающие типовые причинно-следственные связи. Сокращенно: уязвимости  $x_1$ , сегментация  $x_2$ , привилегии  $x_3$ , IDS  $x_4$ , SIEM  $x_5$ , бэкапы  $x_6$ , конечные точки  $x_7$ , изменения  $x_8$ , реагирование  $x_9$ , персонал  $x_{10}$ , наблюдаемость  $x_{11}$ .

1. Если  $x_1$  низкое и  $x_5$  начальная и  $x_{11}$  низкая, то риск высокий. Смысл: высокая вероятность незаметных компрометаций на фоне задержек патчей и слабой корреляции.

2. Если  $x_2$  слабая и  $x_3$  неуправляемое, то риск высокий. Смысл: латеральное перемещение и злоупотребление привилегиями становятся доступными.

3. Если  $x_6$  надежное и  $x_9$  рабочее, то риск по доступности снижается до среднего. Смысл: ущерб от разрушительных инцидентов уменьшается, даже если вероятность остается заметной.

4. Если высокое и  $x_5$  развитая и  $x_{11}$  высокая, то риск низкий. Смысл: наблюдаемость и корреляция позволяют рано обнаруживать и сдерживать инциденты.

5. Если рискованный и  $x_1$  низкое, то риск высокий. Смысл: фишинг и эксплуатация незакрытых уязвимостей усиливают друг друга.

6. Если  $x_8$  хаотичное и  $x_7$  низкая, то риск высокий. Смысл: дрейф конфигураций и рост поверхности атаки при слабой защите конечных точек.

7. Если  $x_1$  среднее и  $x_2$  достаточная и  $x_3$  частичное и  $x_4$  среднее и  $x_5$  рабочая и  $x_{11}$  средняя, то риск средний. Смысл: система работает, но без «запаса прочности»

Заметим, что правила могут быть связаны с тактиками и техниками атакующих (Law of the Republic of Kazakhstan No. 94-V, 2013). Это облегчает коммуникацию с техническими командами: вместо абстрактного «низкая зрелость SIEM» обсуждается конкретный провал в сценарии обнаружения (например, отсутствие корреляции нетипичных административных действий), а затем формируется план устранения.

#### *Численные оценки параметров безопасности и риска для кейса*

Интерпретация результата принципиальна: риск в зоне высокий обусловлен не одним «плохим» контролем, а взаимным усилением факторов. Даже при приемлемых бэкапах и базовой защите конечных точек недостаточная корреляция событий и неполная наблюдаемость делают вероятность незаметной компрометации существенной. Именно этот эффект часто теряется в традиционных чек-листах: контроли формально внедрены, но «сшивки» в единый контур мониторинга и управления отсутствуют.

После выполнения нечёткого вывода (параметры безопасности) и последующей агрегации риска по (Freund et al., 2015) получены значения, представленные в таблице 3. Приведены также краткие пояснения.

Таблица 3 – Результирующие оценки параметров безопасности и риска для кейса

Показатель	Значение	Уровень	Комментарий
$\hat{y}_C$	0.46	средний-низкий	слабое управление привилегиями и недостаточная корреляция повышают риск утечки
$\hat{y}_I$	0.49	средний-низкий	задержки патчей и дрейф конфигураций увеличивают вероятность модификации данных
$\hat{y}_A$	0.58	средний	резервное копирование частично компенсирует недостатки обнаружения
$\hat{y}_R$	0.67	высокий	сочетание слабого управления изменениями, недостаточного SIEM и неполной телеметрии

Численные значения параметров безопасности и интегрального риска получены в рамках вычислительного эксперимента в двух постановках: (i) расчёт по реальному срезу кейса (аудит + телеметрия) и (ii) проверка устойчивости на синтетических данных, моделирующих шум и пропуски наблюдений. Реальные данные. Входные оценки по выбранным признакам нормируются на шкале 0–10 и дополняются коэффициентами полноты/доверия (0–1) на основе фактической наблюдаемости и подтверждаемости данных; срез согласуется и фиксируется в протоколе СМИБ. Далее выполняются этапы нечёткого вывода Мамдани: фаззификация, учёт неполноты через дисконтирование степеней принадлежности, применение базы правил и дефаззификация. Синтетические данные. Формируются дополнительные срезы вокруг профиля кейса: к входным оценкам добавляется управляемый шум, а полнота данных варьируется в заданных диапазонах. Это используется для проверки, что итоговый риск не демонстрирует «скачков» при малых изменениях оценок и корректно реагирует на ухудшение наблюдаемости. Результат. По итогам расчёта получены значения параметров безопасности (конфиденциальность, целостность, доступность) и интегрального риска, приведённые в таблице 3: 0.46, 0.49, 0.58 и 0.67 соответственно.

Предложенная модель адресует типовую проблему практического оценивания ИБ: необходимость принимать управленческие решения при отсутствии полного набора измерений и при высокой доле качественных описаний. В отличие от чисто статистических подходов, нечёткая система сохраняет интерпретируемость и поддаётся аудиту: можно проследить, какие сочетания факторов привели к итоговой оценке, и объяснить, почему снижение наблюдаемости повышает риск даже при формально внедрённых контролях. Это особенно важно для распределённых организаций, где критичен не только факт наличия мер защиты, но и уверенность в том, что они реально функционируют во всех филиалах и сегментах, а не только на центральной площадке. Результаты демонстрационного кейса подтверждают данную логику: при умеренных значениях параметров конфиденциальности, целостности и доступности итоговый интегральный риск остаётся высоким (0.67), поскольку ком-

бинация слабой корреляции событий, проблем управления изменениями и неполной телеметрии формирует значимую вероятность незаметной компрометации и ошибочных управленческих выводов.

По сравнению с традиционными матрицами «вероятность×ущерб» нечёткая модель даёт более корректный мост между качественными наблюдениями и численной отчётностью. Она позволяет интегрировать шкалы зрелости и наблюдаемости без превращения их в «жёсткие числа» без оговорок, моделировать частичную истинность и неоднозначность (тем самым снижая риск ложной точности) и формально учитывать доверие к данным через коэффициенты полноты и отдельный индикатор наблюдаемости. В практическом плане это означает, что модель не «награждает» организацию низким риском только за наличие регламентов и отдельных средств защиты, если качество мониторинга и полнота данных не позволяют подтвердить фактическую эффективность мер. Сопоставляя подход с байесовскими сетями, следует отметить, что нечёткая модель проще в развёртывании при малом объёме данных и менее чувствительна к точности априорных предположений, однако уступает в возможностях строгого вероятностного вывода при наличии хорошей статистики. Практически это задаёт рациональную стратегию применения: нечёткий подход целесообразен как первичный контур управления и средство интеграции качественных сигналов, а по мере накопления данных его можно дополнять вероятностными моделями для отдельных сценариев, где есть достаточная база инцидентов и корректно выстроенная регистрация. Отдельная ценность модели заключается в совместимости с инструментальной инфраструктурой мониторинга и процессами СМИБ.

Технические источники (IDS/SIEM, средства управления уязвимостями, телеметрия конечных точек, учёт событий изменений) обеспечивают данные для значимой части признаков, тогда как процессы СМИБ формируют измеримые артефакты для организационных и поведенческих факторов (управление изменениями, реагирование, обучение и дисциплина исполнения). В результате модель не конкурирует с существующими практиками, а выступает надстроечным механизмом синтеза показателей, перевода разнородные сигналы в сопоставимые оценки и обеспечивая объяснимую приоритезацию улучшений. Ограничения исследования связаны, прежде всего, с трудоёмкостью построения и сопровождения базы правил, риском её «устаревания» при изменении инфраструктуры и кадровой текучести, а также с потенциальным ростом размера базы при расширении числа термов и признаков.

Эти риски снижаются, если рассматривать правила как управляемый артефакт СМИБ с регламентом пересмотра, применять сценарный принцип и модульность (раздельные подбазы для параметров безопасности, типов активов и классов сценариев), а также поддерживать конфигурационную дисциплину источников данных. Дополнительная методическая сложность связана с тем, что эталонные значения риска часто недоступны или искажены неполной регистрацией инцидентов; поэтому настройка и оптимизация весов должна опираться не только на статистику, но и на экспертные оценки и независимый аудит, иначе формальная «калибровка» мо-

жет закрепить искажения наблюдаемости. Перспективы развития работы целесообразно рассматривать в русле двух направлений. Во-первых, в архитектуре Zero Trust, где доступ предоставляется динамически по контексту и уровню доверия, нечёткая логика может выступать интерпретируемым слоем агрегирования сигналов доверия (состояние устройства, риск учётной записи, полнота телеметрии) для микросегментации и политик доступа; при неполных данных это предпочтительнее бинарной логики «доверять/не доверять», поскольку позволяет вводить градуированную, управляемую осторожность. Во-вторых, в задачах мультимодального анализа артефактов, где объединяются текстовые отчёты, логи, сетевые потоки и бинарные данные, подходы визуализации бинарных артефактов (например, Byte2Image) и методы распознавания образов могут поставлять дополнительные признаки, а нечёткая модель-служить управляющим слоем, обеспечивающим объяснимость решения на уровне управления и явное отражение доверия к каждому источнику. Такой гибридный контур позволяет совместить сильные стороны глубоких моделей (извлечение признаков) и нечёткого вывода (интерпретируемая агрегация и управленческая пригодность результата).

### **Заключение.**

Разработана интерпретируемая нечёткая модель оценивания параметров информационной безопасности информационных систем в условиях неполных наблюдений и преобладания качественных описаний. Сформирован набор из 11 входных признаков, охватывающий технические, организационные и поведенческие факторы, а также введён явный индикатор наблюдаемости и качества данных. Для признаков заданы лингвистические переменные и функции принадлежности, реализован вывод Мамдани с учётом весов правил и механизмом «ослабления» принадлежностей при пропусках телеметрии, что позволяет избежать ложной точности и сохранять объяснимость результата для аудита и управленческого контроля. Предложена методика настройки модели, включающая согласование экспертов по процедуре Дельфи, выявление и устранение противоречий в базе правил, ограниченную оптимизацию весов по калибровочным данным и обязательную проверку чувствительности и устойчивости. На демонстрационном кейсе типовой организации государственного сектора Республики Казахстан показано, как размытые наблюдения и фрагментарная телеметрия преобразуются в численные оценки конфиденциальности, целостности, доступности и итогового уровня риска. Полученные результаты демонстрируют ключевой практический вывод: наблюдаемость выступает не вторичным «качеством данных», а полноценным фактором риска, поэтому повышение полноты мониторинга и зрелости корреляции в SIEM способно снижать риск сильнее, чем локальные улучшения отдельных технических контролей без укрепления контура наблюдения. Для внедрения модели в организациях Казахстана целесообразно начинать с компактной и полностью трассируемой базы правил, изначально закладывая явный учёт пропусков и качества телеметрии (без подмены отсутствующих данных усреднением), сочетать экспертную калибровку с осторожной настройкой весов на доступной статистике

и материалах аудита, применять анализ чувствительности для обоснования приоритетов и бюджета, а также интегрировать результаты модели в регулярные процессы СМИБ, чтобы оценки использовались как инструмент управленческого цикла, а не разовый отчёт.

## REFERENCES

- Abubakar N. & Pranggono S. (2020). Fuzzy correlation of security events for SIEM enhancement // *Journal of Information Security and Applications*. [In Eng.].
- Ahmed A. & Mahmoud R. (2019). Fuzzy inference for incident triage in security operations centers. *Future Generation Computer Systems*. [In Eng.].
- Bengio Y., Goodfellow I. & Courville A. (2016). *Deep learning*. MIT Press.
- Center for Internet Security. (2021). CIS critical security controls (v8). <https://www.cisecurity.org/controls/v8>. [In Eng.].
- Committee for Technical Regulation and Metrology. (2023). Information security, cybersecurity and privacy protection. Information security management system. Requirements (ST RK ISO/IEC 27001-2023). Republic of Kazakhstan. [In Eng.].
- Decree of the Government of the Republic of Kazakhstan No. 407. (2017, June 30). On approval of the Cybersecurity Concept (“Cyber Shield of Kazakhstan”). <https://adilet.zan.kz/rus/docs/P1700000407>. [In Eng.].
- Freund J. & Jones J. (2015). Measuring and managing information risk: A FAIR approach. Butterworth-Heinemann. <https://doi.org/10.1016/C2013-0-09966-5> [In Eng.].
- Goldberg D.E. (1989). *Genetic algorithms in search, optimization, and machine learning*. Addison-Wesley. [In Eng.].
- International Organization for Standardization. (2022a). Information security, cybersecurity and privacy protection — Information security management systems — Requirements (ISO/IEC 27001:2022). [In Eng.].
- International Organization for Standardization. (2022b). Information security, cybersecurity and privacy protection — Guidance on managing information security risks (ISO/IEC 27005:2022). [In Eng.].
- Jensen F.V. & Nielsen T.D. (2007). *Bayesian networks and decision graphs* (2nd ed.). Springer. DOI: <https://doi.org/10.1007/978-0-387-68282-2> [In Eng.].
- Joint Task Force Transformation Initiative. (2012). Guide for conducting risk assessments (NIST SP 800-30 Rev. 1). National Institute of Standards and Technology. DOI: <https://doi.org/10.6028/NIST.SP.800-30r1> [In Eng.].
- Kennedy J. & Eberhart R. (1995). Particle swarm optimization. *Proceedings of the IEEE International Conference on Neural Networks (ICNN'95)*. — Vol. 4. — Pp. 1942–1948. DOI: <https://doi.org/10.1109/ICNN.1995.488968> [In Eng.].
- Klir G.J. & Yuan B. (1995). *Fuzzy sets and fuzzy logic: Theory and applications*. Prentice Hall. [In Eng.].
- Law of the Republic of Kazakhstan No. 94-V. (2013, May 21). On personal data and their protection. <https://adilet.zan.kz/eng/docs/Z1300000094> [In Eng.].
- Law of the Republic of Kazakhstan No. 418-V. (2015, November 24). On informatization. <https://adilet.zan.kz/eng/docs/Z1500000418> [In Eng.].
- Linstone H. & Turoff M. (Eds.). (1975). *The Delphi method: Techniques and applications*. Addison-Wesley. [In Eng.].
- Mamdani E.H., & Assilian S. (1975). An experiment in linguistic synthesis with a fuzzy logic controller // *International Journal of Man-Machine Studies*. — Vol. 7. — No. 1. Pp. 1–13. DOI: [https://doi.org/10.1016/S0020-7373\(75\)80002-2](https://doi.org/10.1016/S0020-7373(75)80002-2) [In Eng.].
- Miller D., Harris S., Harper A., VanDyke S. & Blask C. (2011). *Security information and event management (SIEM) implementation*. McGraw-Hill. [In Eng.].
- MITRE. (n.d.). MITRE ATT&CK®: Adversarial tactics, techniques, and common knowledge. Retrieved January 11, 2026, from <https://attack.mitre.org/> [In Eng.].
- Nataraj L., Karthikeyan S., Jacob G. & Manjunath B.S. (2011, July). Malware images: Visualization and automatic classification // *Proceedings of the 8th International Symposium on Visualization for Cyber Security (VizSec'11)*. Pp. 1–7. DOI: <https://doi.org/10.1145/2016904.2016908> [In Eng.].
- Rose S., Borchert O., Mitchell, S. & Connelly S. (2020). Zero trust architecture (NIST SP 800-207) // National Institute of Standards and Technology. DOI: <https://doi.org/10.6028/NIST.SP.800-207> [In Eng.].
- Ross T.J. (2010). *Fuzzy logic with engineering applications* (3rd ed.). John Wiley & Sons. DOI: <https://doi.org/10.1002/9781119994374> [In Eng.].
- Shafer G. (1976). *A mathematical theory of evidence*. Princeton University Press. DOI: <https://doi.org/>



org/10.1515/9780691214696 [In Eng.].

Shameli-Sendi A., Aghababaei-Barzegar R. & Cheriet M. (2016). Taxonomy of information security risk assessment (ISRA). *Computers & Security*. — Vol. 57. — Pp. 14–30. DOI: <https://doi.org/10.1016/j.cose.2015.11.001> [In Eng.].

Srinivasan S. & Karthik A. (2013). Fuzzy logic based information security risk assessment: A review and framework // *International Journal of Information Security Science*. [In Eng.].

Sugeno M. (1985). *Industrial applications of fuzzy control*. North-Holland. DOI: <https://doi.org/10.5555/537323> [In Eng.].

Zadeh L.A. (1965). Fuzzy sets. *Information and Control*. — Vol. 8. — No. 3. Pp. 338–353. DOI: [https://doi.org/10.1016/S0019-9958\(65\)90241-X](https://doi.org/10.1016/S0019-9958(65)90241-X) [In Eng.].

Zimmermann H.J. (2001). *Fuzzy set theory—and its applications* (4th ed.). Springer. DOI: <https://doi.org/10.1007/978-94-010-0646-0> [In Eng.].

**INTERNATIONAL JOURNAL OF INFORMATION AND  
COMMUNICATION TECHNOLOGIES**

**ХАЛЫҚАРАЛЫҚ АҚПАРАТТЫҚ ЖӘНЕ КОММУНИКАЦИЯЛЫҚ  
ТЕХНОЛОГИЯЛАР ЖУРНАЛЫ**

**МЕЖДУНАРОДНЫЙ ЖУРНАЛ ИНФОРМАЦИОННЫХ И  
КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ**

**Собственник:**

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

**Главный редактор:**

Колесникова Катерина Викторовна

**Ответственный редактор:**

Мрзабаева Раушан Жалиевна

**Компьютерная верстка:**

Калабай Замзагуль Ертугановна

Сайт журнала: <https://journal.iitu.edu.kz>

ISSN 2708–2032 (print)

ISSN 2708–2040 (online)

Подписано в печать 30.06.2026.

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