

ISSN 2518-1726 (Online),  
ISSN 1991-346X (Print)

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ  
ҰЛТТЫҚ ҒЫЛЫМ АКАДЕМИЯСЫ

әл-Фараби атындағы Қазақ ұлттық университетінің

# Х А Б А Р Л А Р Ы

---

---

## ИЗВЕСТИЯ

НАЦИОНАЛЬНОЙ АКАДЕМИИ  
НАУК РЕСПУБЛИКИ КАЗАХСТАН  
Қазақстан Республикасының  
Ғылым Академиясының  
Әл-Фараби атындағы  
Қазақ ұлттық университеті

## NEWS

OF THE ACADEMY OF SCIENCES  
OF THE REPUBLIC OF  
KAZAKHSTAN  
al-Farabi Kazakh National University

**PHYSICO-MATHEMATICAL SERIES**

**1 (345)**

**JANUARY – MARCH 2023**

PUBLISHED SINCE JANUARY 1963

PUBLISHED 4 TIMES A YEAR

ALMATY, NAS RK

## БАС РЕДАКТОР:

**МУТАНОВ Ғалымқайыр Мұтанұлы**, техника ғылымдарының докторы, профессор, ҚР ҰҒА академигі, ҚР БҒМ ҚҰО ақпараттық және есептеу технологиялар институтының бас директорының м.а. (Алматы, Қазақстан), **Н=5**

## РЕДАКЦИЯ АЛҚАСЫ:

**КАЛИМОЛДАЕВ Мақсат Нұрәліұлы** (бас редактордың орынбасары), физика-математика ғылымдарының докторы, профессор, ҚР ҰҒА академигі, ҚР БҒМ ҚҰО ақпараттық және есептеу технологиялар институты бас директорының кеңесшісі, зертхана меңгерушісі (Алматы, Қазақстан), **Н=7**

**МАМЫРБАЕВ Өркен Жұмажанұлы** (ғалым хатшы), Ақпараттық жүйелер саласындағы техника ғылымдарының (PhD) докторы, ҚР БҒМ ҚҰО ақпараттық және есептеу технологиялар институты директорының ғылым жөніндегі орынбасары (Алматы, Қазақстан), **Н=5**

**БАЙГУНЧЕКОВ Жұмаділ Жанабайұлы**, техника ғылымдарының докторы, профессор, ҚР ҰҒА академигі, Кибернетика және ақпараттық технологиялар институты, қолданбалы механика және инженерлік графика кафедрасы, Сәтбаев университеті (Алматы, Қазақстан), **Н=3**

**ВОЙЧИК Вальдемар**, техника ғылымдарының докторы (физ-мат), Люблин технологиялық университетінің профессоры (Люблин, Польша), **Н=23**

**СМОЛАРЖ Анджей**, Люблин политехникалық университетінің электроника факультетінің доценті (Люблин, Польша), **Н=17**

**ӘМІРҒАЛИЕВ Еділхан Несіпханұлы**, техника ғылымдарының докторы, профессор, ҚР ҰҒА академигі, Жасанды интеллект және робототехника зертханасының меңгерушісі (Алматы, Қазақстан), **Н=12**

**КИЛАН Әлімхан**, техника ғылымдарының докторы, профессор (ғылым докторы (Жапония), ҚР БҒМ ҚҰО ақпараттық және есептеу технологиялар институтының бас ғылыми қызметкері (Алматы, Қазақстан), **Н=6**

**ХАЙРОВА Нина**, техника ғылымдарының докторы, профессор, ҚР БҒМ ҚҰО ақпараттық және есептеу технологиялар институтының бас ғылыми қызметкері (Алматы, Қазақстан), **Н=4**

**ОТМАН Мохаммед**, PhD, Информатика, коммуникациялық технологиялар және желілер кафедрасының профессоры, Путра университеті (Селангор, Малайзия), **Н=23**

**НЫСАНБАЕВА Сауле Еркебұланқызы**, техника ғылымдарының докторы, доцент, ҚР БҒМ ҚҰО ақпараттық және есептеу технологиялар институтының аға ғылыми қызметкері (Алматы, Қазақстан), **Н=3**

**БИЯШЕВ Рустам Гакашевич**, техника ғылымдарының докторы, профессор, Информатика және басқару мәселелері институты директорының орынбасары, Ақпараттық қауіпсіздік зертханасының меңгерушісі (Қазақстан), **Н=3**

**КАПАЛОВА Нұрсұлту Алдажарқызы**, техника ғылымдарының кандидаты, ҚР БҒМ ҚҰО ақпараттық және есептеу технологиялар институтының киберқауіпсіздік зертханасының меңгерушісі (Алматы, Қазақстан), **Н=3**

**КОВАЛЕВ Александр Михайлович**, физика-математика ғылымдарының докторы, Украина Ұлттық Ғылым академиясының академигі, Қолданбалы математика және механика институты (Донецк, Украина), **Н=5**

**МИХАЛЕВИЧ Александр Александрович**, техника ғылымдарының докторы, профессор, Беларусь Ұлттық Ғылым академиясының академигі (Минск, Беларусь), **Н=2**

**ТИГИНЯНУ Ион Михайлович**, физика-математика ғылымдарының докторы, академик, Молдова Ғылым академиясының президенті, Молдова техникалық университеті (Кишинев, Молдова), **Н=42**

## «ҚР ҰҒА Хабарлары. Информатика сериясы».

ISSN 2518-1726 (Online),

ISSN 1991-346X (Print)

Меншіктеуші: «Қазақстан Республикасының Ұлттық ғылым академиясы» РҚБ (Алматы қ.). Қазақстан Республикасының Ақпарат және қоғамдық даму министрлігінің Ақпарат комитетінде 14.02.2018 ж. берілген **№ 16906-Ж** мерзімдік басылым тіркеуіне қойылу туралы куәлік.

Тақырыптық бағыты: *физика-математикалық сериясы*.

Қазіргі уақытта: *«ақпараттық технологиялар» бағыты бойынша ҚР БҒМ БҒСБҚ ұсынған журналдар тізіміне енді.*

Мерзімділігі: *жылына 4 рет.*

Тиражы: *300 дана.*

Редакцияның мекен-жайы: *050010, Алматы қ., Шевченко көш., 28, 218 бөл., тел.: 272-64-39*

*<http://www.physico-mathematical.kz/index.php/en/>*

© Қазақстан Республикасының Ұлттық ғылым академиясы, 2023  
Типографияның мекен-жайы: «Аруна» ЖК, Алматы қ., Мұратбаев көш., 75.

## Главный редактор:

**МУТАНОВ Галимкаир Мутанович**, доктор технических наук, профессор, академик НАН РК, и.о. генерального директора «Института информационных и вычислительных технологий» КН МНВО РК (Алматы, Казахстан), **Н=5**

## Редакционная коллегия:

**КАЛИМОЛДАЕВ Максат Нурадилович**, (заместитель главного редактора), доктор физико-математических наук, профессор, академик НАН РК, советник генерального директора «Института информационных и вычислительных технологий» КН МНВО РК, заведующий лабораторией (Алматы, Казахстан), **Н=7**

**МАМЫРБАЕВ Оркен Жумажанович**, (ученый секретарь), доктор философии (PhD) по специальности «Информационные системы», заместитель директора по науке РГП «Институт информационных и вычислительных технологий» Комитета науки МНВО РК (Алматы, Казахстан), **Н=5**

**БАЙГУНЧЕКОВ Жумадил Жанабаевич**, доктор технических наук, профессор, академик НАН РК, Институт кибернетики и информационных технологий, кафедра прикладной механики и инженерной графики, Университет Саптаева (Алматы, Казахстан), **Н=3**

**ВОЙЧИК Вальдемар**, доктор технических наук (физ.-мат.), профессор Люблинского технологического университета (Люблин, Польша), **Н=23**

**СМОЛАРЖ Анджей**, доцент факультета электроники Люблинского политехнического университета (Люблин, Польша), **Н=17**

**АМИРГАЛИЕВ Едилхан Несипханович**, доктор технических наук, профессор, академик Национальной инженерной академии РК, заведующий лабораторией «Искусственного интеллекта и робототехники» (Алматы, Казахстан), **Н=12**

**КЕЙЛАН Алимхан**, доктор технических наук, профессор (Doctor of science (Japan)), главный научный сотрудник РГП «Института информационных и вычислительных технологий» КН МНВО РК (Алматы, Казахстан), **Н=6**

**ХАЙРОВА Нина**, доктор технических наук, профессор, главный научный сотрудник РГП «Института информационных и вычислительных технологий» КН МНВО РК (Алматы, Казахстан), **Н=4**

**ОТМАН Мохамед**, доктор философии, профессор компьютерных наук, Департамент коммуникационных технологий и сетей, Университет Путра Малайзия (Селангор, Малайзия), **Н=23**

**НЫСАНБАЕВА Сауле Еркебулановна**, доктор технических наук, доцент, старший научный сотрудник РГП «Института информационных и вычислительных технологий» КН МНВО РК (Алматы, Казахстан), **Н=3**

**БИЯШЕВ Рустам Гакашевич**, доктор технических наук, профессор, заместитель директора Института проблем информатики и управления, заведующий лабораторией информационной безопасности (Казахстан), **Н=3**

**КАПАЛОВА Нурсулу Алдажаровна**, кандидат технических наук, заведующий лабораторией кибербезопасности РГП «Института информационных и вычислительных технологий» КН МНВО РК (Алматы, Казахстан), **Н=3**

**КОВАЛЕВ Александр Михайлович**, доктор физико-математических наук, академик НАН Украины, Институт прикладной математики и механики (Донецк, Украина), **Н=5**

**МИХАЛЕВИЧ Александр Александрович**, доктор технических наук, профессор, академик НАН Беларуси (Минск, Беларусь), **Н=2**

**ТИГИНЯНУ Ион Михайлович**, доктор физико-математических наук, академик, президент Академии наук Молдовы, Технический университет Молдовы (Кишинев, Молдова), **Н=42**

**«Известия НАН РК. Серия информатики».**

**ISSN 2518-1726 (Online),**

**ISSN 1991-346X (Print)**

Собственник: *Республиканское общественное объединение «Национальная академия наук Республики Казахстан» (г. Алматы).*

Свидетельство о постановке на учет периодического печатного издания в Комитете информации Министерства информации и общественного развития Республики Казахстан **№ 16906-Ж** выданное 14.02.2018 г.

Тематическая направленность: *серия физика-математическая.*

В настоящее время: *вошел в список журналов, рекомендованных ККСОН МОН РК по направлению «информационные коммуникационные технологии».*

Периодичность: *4 раз в год.*

Тираж: *300 экземпляров.*

Адрес редакции: *050010, г. Алматы, ул. Шевченко, 28, оф. 218, тел.: 272-64-39*

*<http://www.physico-mathematical.kz/index.php/en/>*

© Национальная академия наук Республики Казахстан, 2023  
Адрес типографии: ИП «Аруна», г. Алматы, ул. Муратбаева, 75.

### Chief Editor:

**MUTANOV Galimkair Mutanovich**, doctor of technical sciences, professor, academician of NAS RK, acting General Director of the Institute of Information and Computing Technologies CS MES RK (Almaty, Kazakhstan), **H=5**

### EDITORIAL BOARD:

**KALIMOLDAYEV Maksat Nuradilovich**, (Deputy Editor-in-Chief), Doctor of Physical and Mathematical Sciences, Professor, Academician of NAS RK, Advisor to the General Director of the Institute of Information and Computing Technologies of the CS MES RK, Head of the Laboratory (Almaty, Kazakhstan), **H = 7**

**Mamyrbayev Orken Zhumazhanovich**, (Academic Secretary, PhD in Information Systems, Deputy Director for Science of the Institute of Information and Computing Technologies CS MES RK (Almaty, Kazakhstan), **H = 5**

**BAIGUNCHEKOV Zhumadil Zhanabaevich**, Doctor of Technical Sciences, Professor, Academician of NAS RK, Institute of Cybernetics and Information Technologies, Department of Applied Mechanics and Engineering Graphics, Satbayev University (Almaty, Kazakhstan), **H=3**

**WOJCIK Waldemar**, Doctor of Technical Sciences (Phys.-Math.), Professor of the Lublin University of Technology (Lublin, Poland), **H=23**

**SMOLARJ Andrej**, Associate Professor Faculty of Electronics, Lublin polytechnic university (Lublin, Poland), **H= 17**

**AMIRGALIEV Edilkhan Nesipkhanovich**, Doctor of Technical Sciences, Professor, Academician of NAS RK, Head of the Laboratory of Artificial Intelligence and Robotics (Almaty, Kazakhstan), **H= 12**

**KEILAN Alimkhan**, Doctor of Technical Sciences, Professor (Doctor of science (Japan)), chief researcher of Institute of Information and Computational Technologies CS MES RK (Almaty, Kazakhstan), **H= 6**

**KHAIROVA Nina**, Doctor of Technical Sciences, Professor, Chief Researcher of the Institute of Information and Computational Technologies CS MES RK (Almaty, Kazakhstan), **H= 4**

**OTMAN Mohamed**, PhD, Professor of Computer Science Department of Communication Technology and Networks, Putra University Malaysia (Selangor, Malaysia), **H= 23**

**NYSANBAYEVA Saule Yerkebulanovna**, Doctor of Technical Sciences, Associate Professor, Senior Researcher of the Institute of Information and Computing Technologies CS MES RK (Almaty, Kazakhstan), **H= 3**

**BIYASHEV Rustam Gakashevich**, doctor of technical sciences, professor, Deputy Director of the Institute for Informatics and Management Problems, Head of the Information Security Laboratory (Kazakhstan), **H= 3**

**KAPALOVA Nursulu Aldazharovna**, Candidate of Technical Sciences, Head of the Laboratory cybersecurity, Institute of Information and Computing Technologies CS MES RK (Almaty, Kazakhstan), **H=3**

**KOVALYOV Alexander Mikhailovich**, Doctor of Physical and Mathematical Sciences, Academician of the National Academy of Sciences of Ukraine, Institute of Applied Mathematics and Mechanics (Donetsk, Ukraine), **H=5**

**MIKHALEVICH Alexander Alexandrovich**, Doctor of Technical Sciences, Professor, Academician of the National Academy of Sciences of Belarus (Minsk, Belarus), **H=2**

**TIGHINEANU Ion Mihailovich**, Doctor of Physical and Mathematical Sciences, Academician, President of the Academy of Sciences of Moldova, Technical University of Moldova (Chisinau, Moldova), **H=42**

### News of the National Academy of Sciences of the Republic of Kazakhstan.

Series of informatics.

ISSN 2518-1726 (Online),

ISSN 1991-346X (Print)

Owner: RPA «National Academy of Sciences of the Republic of Kazakhstan» (Almaty). The certificate of registration of a periodical printed publication in the Committee of information of the Ministry of Information and Social Development of the Republic of Kazakhstan No. 16906-Ж, issued 14.02.2018

Thematic scope: *series physical-mathematical series.*

Currently: *included in the list of journals recommended by the CCSES MES RK in the direction of «information and communication technologies».*

Periodicity: *4 times a year.*

Circulation: *300 copies.*

Editorial address: *28, Shevchenko str., of. 218, Almaty, 050010, tel. 272-64-39*

*<http://www.physico-mathematical.kz/index.php/en/>*

© National Academy of Sciences of the Republic of Kazakhstan, 2023

Address of printing house: ST «Aruna», 75, Muratbayev str, Almaty.

NEWS OF THE NATIONAL ACADEMY OF SCIENCES  
OF THE REPUBLIC OF KAZAKHSTAN  
PHYSICO-MATHEMATICAL SERIES  
ISSN 1991-346X

Volume 1, Number 345 (2023), 22-36  
<https://doi.org/10.32014/2023.2518-1726.166>

МРНТИ 81.93.29  
УДК 621.39:004.05

© **Z. Avkurova** , **S. Gnatyuk** , **L. Kydyralina** \*, **N. Kurmangaliev** , 2023  
Karaganda Industrial University, Temirtau, Kazakhstan.  
E-mail: zhadyra.avkurova.83@mail.ru

### **THE INTELLECTUALIZED METHOD OF EARLY DETECTION AND IDENTIFICATION OF THE VIOLATOR IN INFORMATION AND COMMUNICATION SYSTEMS**

**Z. Avkurova** — master of Technical Sciences. Karaganda Industrial University. Temirtau, Kazakhstan.  
E-mail: zhadyra.avkurova.83@mail.ru, <https://orcid.org/0000-0002-0706-6075>;

**S. Gnatyuk** — candidate of technical sciences. Kyiv, Ukraine.  
E-mail: sergio.gnatyuk@gmail.com, <https://orcid.org/0000-0003-4992-0564>;

**L. Kydyralina** — PhD. acting associate professor. Shakarim University in Semey, Semey, Kazakhstan.  
E-mail: lazat\_75@mail.ru, <https://orcid.org/0000-0002-2836-0919>;

**N. Kurmangaliev** — PhD. Head of the Department of Information and technical sciences. EI “ALIKHAN BOKEIKHAN UNIVERSITY”. Semey, Kazakhstan.  
E-mail: nurgulkk62@mail.ru, <https://orcid.org/0000-0003-1709-662X>.

**Abstract:** Protection of the resources of information and communication systems. Some of these systems allow you to determine not only the nature of violations (type of attack), but also the category of the violator. There are two basic approaches for building such systems - signature and behavioral (abnormal). Almost all existing systems are built on the first approach and are not effective in the conditions of fuzzy formalization of input data. The analysis of publications has shown the effectiveness of using the mathematical apparatus of fuzzy logic to solve problems related to identifying attacks on information resources and cybersecurity violators in a weakly formalized environment (cyberspace is certainly such an environment). In this regard, the paper proposes an intellectualized method of early detection and identification of the violator in information and communication systems, which, through the use of fuzzy logic methods, makes it possible to identify the cybersecurity violator in a poorly formalized environment and more accurately identify him in accordance with the selected categories. The input data of the method are network and /or host parameters (the model of network and host parameters proposed by the authors in previous works is used) and the identifiers of

the violator (possible categories), the output generates a message about fixing the fact of the violator and the result of the procedure for categorizing the violator. In future works, based on the proposed method, the authors plan to develop a software system that will effectively identify and identify the violator in information and communication systems.

**Keywords:** identification, intruder, attack, information security, decisive rules, information and communication system

© Ж.С. Авкурова, С. Гнатюк, Л.М. Кыдыралина\*,  
Н.К. Курмангалиева, 2023

Қарағанды индустриялық университеті, Теміртау, Қазақстан.

E-mail: zhadyra.avkurova.83@mail.ru

## АҚПАРАТТЫҚ-КОММУНИКАЦИЯЛЫҚ ЖҮЙЕЛЕРДЕ ҚҰҚЫҚ БҰЗУШЫНЫ ЕРТЕ АНЫҚТАУ ЖӘНЕ СӘЙКЕСТЕНДІРУДІҢ ИНТЕЛЛЕКТУАЛДЫ ӘДІСІ

**Авкурова Ж.С.** — Техника ғылымдарының магистрі. Жасанды интеллект технологиялары кафедрасы. Энергетика. көлік және басқару жүйелері факультет. Қарағанды индустриялық университеті. 101400. Теміртау, Қазақстан.

E-mail: zhadyra.avkurova.83@mail.ru, <https://orcid.org/0000-0002-0706-6075>;

**Гнатюк С.** — Техника ғылымдарының кандидаты. Ұлттық авиациялық университеті. Киев, Украина.

E-mail: sergio.gnatyuk@gmail.com, <https://orcid.org/0000-0003-4992-0564>;

**Кыдыралина Л.М.** — PhD. Семей қаласының Шәкәрім атындағы университеті КеАҚ, Семей, Қазақстан.

E-mail: lazat\_75@mail.ru, <https://orcid.org/0000-0002-2836-0919>;

**Курмангалиева Н.К.** — PhD. ALIKHAN BOKEIKHAN UNIVERSITY, ББМ. Семей, Қазақстан.

E-mail: nurgulkk62@mail.ru, <https://orcid.org/0000-0003-1709-662X>.

**Аңдатпа.** Ақпараттық-коммуникациялық жүйелердің ресурстарын қорғау үшін басып кіруді анықтау және алдын алу жүйелері қолданылады. Осы жүйелердің кейбіреулері бұзушылықтардың сипатын (шабуыл түрін) ғана емес, сонымен қатар бұзушының санатын да анықтауға мүмкіндік береді. Мұндай жүйелерді құрудың екі негізгі тәсілі бар — сигнатуралық және мінездік (қалыпты емес). Іс жүзінде барлық қолданыстағы жүйелер бірінші тәсілге негізделген және кіріс мәліметтерін анық емес рәсімдеу жағдайында тиімсіз. Жарияланымдарды талдау нашар рәсімделетін ортада ақпараттық ресурстарға жасалатын шабуылдарды және киберқауіпсіздікті бұзушыларды анықтауға байланысты міндеттерді шешу үшін анық емес логиканың математикалық аппаратын қолданудың тиімділігін көрсетті (мұндай орта сөзсіз киберкеңістік болып табылады). Осыған байланысты, жұмыста анық емес логика әдістерін қолдану арқылы нашар рәсімделген ортада киберқауіпсіздік бұзушыны анықтауға және оны анықталған санаттарға сәйкес дәлірек анықтауға мүмкіндік беретін ақпараттық-коммуникациялық жүйелердегі бұзушыны

ерте анықтау және сәйкестендірудің интеллектуалды әдісі ұсынылған. Әдістің кіріс мәліметтері желілік және / немесе хост параметрлері (авторлардың алдыңғы ұсынған жұмыстарында желілік және хост параметрлерінің моделі қолданылады) және бұзушының идентификаторлары (мүмкін санаттары) болып табылады, нәтижесінде бұзушы фактісін анықтау және санаттау рәсімінің нәтижесі туралы хабарлама жасалады. Ұсынылған әдіс негізінде келесі жұмыстарда авторлар ақпараттық-коммуникациялық жүйелердегі бұзушыны тиімді анықтайтын және сәйкестендіретін бағдарламалық жасақтама жүйесін құруды жоспарлап отыр.

**Түйін сөздер:** сәйкестендіру, бұзушы, шабуыл, ақпараттық қауіпсіздік, шешуші ережелер, ақпараттық-коммуникациялық жүйе

© **Ж.С. Авкурова, С.А. Гнатюк, Л.М. Кыдыралина\***,  
**Н.К. Курмангалиева, 2023**

Карагандинский индустриальный университет, Темиртау, Казахстан.  
E-mail: zhadyra.avkurova.83@mail.ru

## **ИНТЕЛЛЕКТУАЛИЗИРОВАННЫЙ МЕТОД РАННЕГО ВЫЯВЛЕНИЯ ИДЕНТИФИКАЦИИ НАРУШИТЕЛЯ В ИНФОРМАЦИОННО- КОММУНИКАЦИОННЫХ СИСТЕМАХ**

**Авкурова Ж.С.** — Магистр технических наук. Кафедра Технологий искусственного интеллекта. Факультет Энергетики, транспорта и систем управления Карагандинский индустриальный университет. г. Темиртау, Казахстан.

E-mail: zhadyra.avkurova.83@mail.ru, <https://orcid.org/0000-0002-0706-6075>;

**Гнатюк С.А.** — Национальный авиационный университет. г. Киев, Украина.

E-mail: sergio.gnatyuk@gmail.com, <https://orcid.org/0000-0003-4992-0564>;

**Кыдыралина Л.М.** — PhD. НАО Университет имени Шакарима, города Семей, г. Семей, Казахстан.

E-mail: lazat\_75@mail.ru, <https://orcid.org/0000-0002-2836-0919>;

**Курмангалиева Н.К.** — PhD. УО Alikhan Bokeikhan university, г.Семей, Казахстан.

E-mail: nurgulkk62@mail.ru, <https://orcid.org/0000-0003-1709-662X>.

**Аннотация.** Для защиты ресурсов информационно-коммуникационных систем (ИКС) применяются системы выявления и предотвращения вторжений. Все эти системы построены на сигнатурном принципе и являются не эффективными в условиях нечеткости входных данных. Некоторые из таких систем позволяют определить не только характер нарушений (тип атаки), а также и категорию нарушителя. Существует два базовых подхода для построения таких систем — сигнатурный и поведенческий (аномальный). Практически все существующие системы построены на первом подходе и являются не эффективными в условиях нечеткой формализации входных данных. Анализ публикаций показал эффективность применения математического аппарата нечеткой логики для решения задач, связанных с выявлением атак на информационные ресурсы и нарушителей

кибербезопасности в слабо формализованной среде (такой средой, безусловно, является киберпространство). В связи с этим, в работе предложен интеллектуализированный метод раннего обнаружения и идентификации нарушителя в информационно-коммуникационных системах, который за счет использования методов нечеткой логики, дает возможность выявить нарушителя кибербезопасности в слабоформализованной среде и более точно его идентифицировать в соответствии с выделенными категориями. Входными данными метода являются сетевые и / или хостовые параметры (используется модель сетевых и хостовых параметров, предложенная авторами в предыдущих работах) и идентификаторы нарушителя (возможные категории), на выходе формируется сообщение о фиксации факта нарушения и результат процедуры категоризации нарушителя. В дальнейших работах, на основе предложенного метода, авторы планируют разработать программную систему, которая будет эффективно выявлять и идентифицировать нарушителя в информационно-коммуникационных системах.

**Ключевые слова:** идентификация, нарушитель, атака, информационная безопасность, решающие правила, информационно-коммуникационная система

### **Вступление**

Сегодня для защиты ресурсов ИКС применяются системы выявления вторжений, а в аспекте выявления факта нарушения информационной безопасности злоумышленником — системы выявления нарушителя. Практически все эти системы построены на сигнатурном принципе и являются неэффективными в условиях нечеткости входных данных (Khosravi et al., 2020). Поэтому целесообразной является разработка систем, которые работают по решающему принципу, а это в свою очередь усложняется использованием статистических данных, что значительно увеличивает требования таких систем к часовым и вычислительным ресурсам. Данную проблему может решить применение методов нечеткой логики. Поэтому разработка метода выявления и идентификации нарушителя в ИКС на основе методов нечетких множеств и предложенных в предыдущих работах моделей является актуальной задачей.

### **Материалы и основные методы**

В работах (Yan et al., 2020) показана эффективность применения математического аппарата нечеткой логики для решения задач, связанных с выявлением атак на информационные ресурсы и нарушителей информационной безопасности в слабо формализуемой среде. В (Iashvili et al., 2021) разработана модель эталонов лингвистических переменных для параметров нечеткого характера за счет формирования множеств пар “нарушитель → параметр” и “нарушитель → набор логико-лингвистических связей”, которая позволяет формализовать процессы обнаружения нарушителя в слабо формализуемой среде с нечеткими условиями. Кроме того, сформированы обнаружения



нарушителя, которые за счет множества эталонных параметров позволяют провести непосредственное обнаружение признаков деятельности неавторизованной стороны и определить его тип с определенным показателем опасности, порожденной возможной атакой нарушителя.

В связи с этим, целью данной работы является разработка метода обнаружения и идентификации нарушителя информационной безопасности в ИКС, использование которого позволит синтезировать систему обнаружения и идентификации нарушителя и повысить эффективность ее работы в условиях нечеткости за счет применения решающих правил (РП) и экспертных методов.

### **Основная часть исследования**

Предложенный метод решает задачу выявления злоумышленника в ИКС, процессы в которых по своей сути являются слабо формализуемой и нечеткой средой. В методе используются элементы нечеткой логики для предварительного принятия решения о возбуждении и идентификации лица-нарушителя, а также базис обычной четкой логики, обеспечивает уточняющую идентификацию.

Метод имеет 3 фазы:

- 1) Подготовительная;
- 2) Работы с нечеткими параметрами;
- 3) Работы с четкими параметрами, которые в свою очередь состоят из отдельных этапов.

Рассмотрим предложенный метод более подробно. Первая фаза предназначена для организации работы системы обнаружения и идентификации нарушителя в ИКС, которая разработана на основе данного метода, ее настройки и определения исходных данных. Для формирования функций принадлежности будем использовать метод лингвистических термов с использованием статистических данных (МЛТС), в нечеткой арифметике - метод линейной аппроксимации по локальным максимумам (ЛЛАМ) и для сравнения функций принадлежности — метод -уровневого расстояния (АУР). Названные методы будут использоваться для обработки нечетких данных при решении поставленной задачи. В первой фазе реализованы этапы 1–4.

*Этап 1 — Выбор метода определения коэффициентов важности (МОКВ)*

На этом этапе проходит выбор МОКВ с заданного множества, используемый в дальнейшем для формирования РП (МОКВ1, МОКВ2 ..., МОКВ25, например, метод средних рангов (СР), мультипликативная свертка Кини (МСК), метод случайных векторов (МСВ) и др.), среди которых выбирается рабочий метод. На выбор метода влияют такие критерии, как форма представления входных (ВхД) и выходных данных (ВыхД), трудоемкость и рекомендуемая шкала (Gnatyuketel, 2021). Если заданным критериям соответствуют несколько методов, то окончательный выбор осуществляется по решению эксперта. Например, в соответствии с заданными критериями и приоритетами из множества  $МОКВ_i (i = \overline{1,25})$  выбирается метод средних рангов.

*Этап 2 — формирование множеств категорий нарушителя и параметров*

Этап ориентирован на определение множеств категорий нарушителя и параметров, которые используются для обнаружения нарушителя. На основе анализа среды ИКС формируются идентификаторы нарушителя для  $k$ -го узла  $I_i^k (i = \overline{1, n}; k = \overline{1, l})$ , а также множества контролируемых нечетких параметров  $P_i^k$  и четких параметров  $SP_i^k (i = \overline{1, m}; k = \overline{1, l})$  и с определенной, заранее установленной, периодичностью их текущие значения заносятся в регистры системы обнаружения и идентификации нарушителя. Согласно фиксируются  $I_i^k, P_i^k$  и  $SP_i^k$ , которые позволяют выявить признаки деятельности 6 видов нарушителя  $I_1^k, I_2^k, I_3^k, I_4^k, I_5^k, I_6^k$  ( $D^k, S^k, C^k, H^k, SB^k$  и  $B^k$  и - дезинформатор, спамер, кречер, хакер, спам-бот и бот-взломщик соответственно) на основе 8 нечетких параметров  $P_1^k, P_2^k, P_3^k, P_4^k, P_5^k, P_6^k, P_7^k$  и  $F_8^k$  ( $Tlog^k, Nlog^k, Tlog^k, I^k, CPU^k, CPU^k, NER^k$  и  $RTPR/F^k$ - время входа в систему, Частота запросов на вход в систему, время, затраченное на вход в систему, Интенсивность действий, процессорное время / загруженность процессора, Количество выполняемых файлов, Количество сбоев и ошибок, время выполнения процесса / файла соответственно) и 7 четких параметров  $SP_1^k, SP_2^k, SP_3^k, SP_4^k, SP_5^k, SP_6^k$  и  $SP_7^k$  ( $UID^k, AtEF^k, UPr^k, TrFin^k, ModF^k, TrFount^k$  и  $KS^k$ - Имя пользователя при входе, Тип используемых файлов при атаке, Несвойственные процессы, Передача файла в систему, Изменение файлов, копирование / передача фалов из системы, Нажатие клавиш клавиатуры соответственно) (Fanetal, 2018).

#### Этап 3 — формирование эталонов ЧП

Этот этап направлен на получение эталонных величин, необходимых для измерения текущих значений контролируемых параметров. На основе входных данных, полученных на этапе 2, формируем соответствующие значения эталонов лингвистических переменных для всех  $T_{ij}^e = \bigcup_{f=1}^r T_{ij}^{ef}$  использованием выбранного метода формирования ФН, например,  $\{T_{Tlog}^{ef}, T_{Nlog}^{ef}, T_{Tlog}^{ef}, T_{I}^{ef}, T_{CPU}^{ef}, \dots\}$  (Grimesetal, 2002). Так, для CPU получим в идеале значение  $T_{CPU}^e = \bigcup_{j=1}^3 T_{CPU}^{ej}$ , которые можно представить в виде лингвистических термов для CPU-  $\{T_{CPU}^{e1}, T_{CPU}^{e2}, T_{CPU}^{e3}\} = \{H^e, C^e, B^e\}$  с помощью процедуры визуализации.

#### Этап 4 – формирование множества ИП

Создание наборов четких и нечетких РП, используемых для выявления нарушителей в ИКС на основе сравнения эталонных и текущих значений. С использованием аппарата множества лингвистических идентификаторов  $LI = \bigcup_{i=1}^d LI_i$  и наборов логико-лингвистических связей  $LC = \bigcup_{i=1}^n (\bigcup_{j=1}^n LC_{ij}^n)$  (Iashvilietal, 2021) формируется множество альтернатив  $ER_{ij}^k ((i = \overline{1, n}; k = ,$  где  $n$  - количество категорий нарушите-

лей,  $r_n$  - количество правил для обнаружения  $n$ -ой категории нарушителя, а  $d$  - количество альтернативных вариантов для формирования одного правила). Например, для первой категории нарушителя и первого правила получим  $\bigcup_{k=1}^d ER_{11}^k = \{ER_{11}^1, ER_{11}^2, \dots, ER_{11}^5\}$ . Формирование правил осуществляется на основе множества альтернатив с помощью процедуры их выбора, основанная на одном из МОКВ, формируя таким образом наборы ОП, например,

$$ER_3 = \{ER_{31} = (t_I \cong B, t_{CPU} \cong B, t_{NEr} \cong B, t_{RTPr/F} \cong DM) \rightarrow B, ER_{32} = (t_I \cong B, t_{CPU} \cong B, t_{NEr} \cong B, t_{RTPr/F} \cong M) \rightarrow BBH\}.$$

Во второй фазе обрабатываются нечеткие параметры, используемые для обнаружения нарушителя информационной безопасности и отнесения его к одной из предложенных категорий. Если результат работы второй фазы является положительным, то есть обнаружены признаки нарушения информационной безопасности, запускается третья фаза метода. Фаза работы с четкими параметрами имеет уточняющее значение, поскольку процесс идентификации злоумышленника значительно эффективнее на основе четких параметров в отличие от процесса выявления факта нарушения, который целесообразно проводить на основе нечеткой логики. Хотя вторая и третья фазы различны физически и выполняются отдельно их целесообразно логично объединить.

*Этап 5 — формирование связи категории нарушителя с параметрами*

Во время выполнения второй фазы осуществляется обработка нечетких параметров. При этом формируются связи конкретного типа нарушителя информационной безопасности с параметрами, которые необходимы для его обнаружения. Для нашего случая при  $n = 6$  и  $m = 8$  в  $k$ -м узле для идентификаторов нарушителя  $I_1^k, I_2^k, I_3^k, I_4^k, I_5^k$  и  $I_6^k$  создаются связи с параметрами  $P_{n_1}^k = P_{n_2}^k = P_{n_3}^k = (P_1^k, P_2^k, P_3^k, P_4^k, P_5^k, P_6^k, P_7^k, P_8^k)$ ,

$$P_{n_2}^k = P_{n_3}^k = (P_4^k, P_5^k, P_6^k, P_7^k) \text{ и } P_{n_6}^k = (P_1^k, P_2^k, P_3^k, P_4^k, P_5^k, P_6^k, P_7^k, P_8^k), \text{ то есть}$$

$$D^k = C^k = H^k \rightarrow \{T \log^k, S^k = SB^k \rightarrow \{I^k, CPU^k, NEr^k, RTPr/F^k\}\} \text{ и}$$

$$B^k \rightarrow \{T \log^k, N \log^k, TS \log^k, I^k, CPU^k, NEF^k, NEr^k, RTPr/F^k\}, (k = \overline{1, l}),$$

где  $l$  - количество узлов ИКС. После перехода к третьей фазе выполняется обработка четких параметров для формирования связи конкретного типа нарушителя с четкими параметрами, которые необходимы для его идентификации. Например, при  $n = 6$  и  $m = 7$  в  $k$ -м узле с идентификаторами нарушителя  $...$  и создаются связи с четкими параметрами, то есть  $...$ .

*Этап 6 — формирование и фаззификация параметров*

Работа данного этапа также проходит в два этапа: сначала с нечеткими параметрами, а затем с четкими. По окончанию процедуры формирования связи  $I_i^k \rightarrow P_{n_i}^k$  происходит преобразование множества

текущих значений параметров, фиксируемых в течение определенного времени в одно нечеткое число и таким образом получим  $m$  нечетких чисел  $t_i^k (i = \overline{1, m})$  по каждому параметру связанных с подходящим. Например, при  $m = 6$  будем иметь:  $t_1^k = t_{Tlog}^k, t_2^k = t_{Nlog}^k, t_3^k = t_{TSlog}^k, t_4^k = t_{CPU}^k, t_5^k = t_{CPU}^k, t_6^k = t_{NEF}^k, t_7^k = t_{NEr}^k, t_8^k = t_{RTPr/F}^k$ . В третьей фазе по окончании процедуры формирования связей  $I_i^k \rightarrow SP_{n_i}^k$  определяются текущие значения четких параметров  $SP_i^k$  на момент перехода к третьей фазе, которые передаются из каждого узла системы на соответствующие каждому параметру модули логической арифметики.

#### *Этап 7 — Обработка и формирование кортежей параметров*

Этап ориентирован на определение значения каждого из нечетких и четких параметров для всей системы в целом и формирования их в один кортеж. Сформированные  $t_i^k (i = \overline{1, n}, k = \overline{1, l})$  параллельно в соответствии с каждого параметра с использованием выбранного метода нечеткой арифметики обрабатываются для получения суммарных показателей  $\sum t^k$ , характеризующих величину контролируемых параметров на всех узлах ИКС. На данном этапе используется один из возможных методов реализации операций нечеткой арифметики в соответствии с заданными пользователем критериями, для предложенного метода наиболее целесообразно использовать метод ЛАЛИМ. Если процесс обнаружения нарушителя информационной безопасности осуществляется только на одном узле ИКС, то никаких логико-арифметических операций на нем не выполняется и не создаются суммарные значения переменных. Полученные суммарные показатели записываются по каждому параметру в кортеж. Фаза работы с четкими параметрами проходит следующим образом: происходит обработка четких параметров и исчисляется их результирующее (суммарное) значение  $\sum SP_i^k$  для всей ИКС. Вычисление происходит по правилам обычной логики. Если значение четкого параметра хотя бы на одном из узлов равно 1, то суммарное значение также равно 1. Если процесс обнаружения нарушителя информационной безопасности осуществляется только на одном узле ИКС, то никаких логико-арифметических операций на нем не выполняется и не создаются суммарные значения переменных. Полученные данные формируются в кортеж  $\langle \sum SP_i \rangle$ .

#### *Этап 8 — формирование результата*

Этап ориентирован на принятие решения о том – произошло ли нарушение информационной безопасности в ИКС, то есть фиксация факта нарушения и идентификация нарушителя по одной из предложенных категорий (дезинформатор, спамер, кречер, хакер, спам-бот, бот-взломщик). На основе сформированного кортежа с использованием множества правил  $ER_i (i = \overline{1, n})$  с помощью логико-лингвистических связей  $LI_i (i = \overline{1, d})$  выполняется сравнение ФН нечетких параметров с значениями ОП с помощью метода АРВ, то есть выявление возможного нарушителя и идентификация его типа.

Иными словами, каждой категории нарушителя  $I_i^k$  присваивается

логический идентификатор LI (H, БНВ, С, БВН, В, К). Полученный результат может отображаться как в лингвистической, так и в графической форме в виде нечеткого числа, изображенного на фоне сложившихся эталонных значений лингвистических переменных. Именно на этом этапе формируется промежуточный результат, удостоверяющий факт нарушения информационной безопасности в ИКС и запускает 3-ю фазу метода. После этого проходит работа с четкими параметрами на этапах 5-8.

В результате сформирован кортеж  $\langle \sum SP_i \rangle$  с использованием множества правил  $ESR_i (i = \overline{1, n})$  соответствующих определенному типу  $UI_i^k$  выполняется идентификация типа возможного нарушителя из числа перечисленных выше.

Следует отметить, что количество как идентификаторов (то есть категорий) нарушителя, так и параметров, по которым можно выявить факт нарушения информационной безопасности может быть изменено в процессе работы системы, разработанной на основе данного метода, решением эксперта.

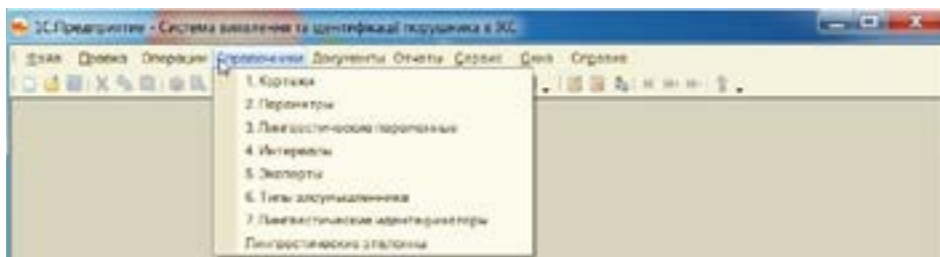
### **Результаты**

На основе предложенной методики экспериментального исследования и математических моделей в среде 1С Предприятие разработано ПО «Система обнаружения и идентификации нарушителя» для проведения имитационного моделирования. В данной программе можно запускать процедуры формирования и коррекции эталонов лингвистических перемен, кортежей и ОП, а также настраивать параметры проведения моделирования.

Выполняемый программный модуль может быть использован на любом компьютере, характеристики которых отвечают минимальным требованиям для работы с 1С Предприятием:

- Процессор IntelPentium IV/Xeon 2,4 ГГц и больше
- Оперативная память 1024 Мб и больше
- Жесткий диск 40 Гб и более
- ОС — MicrosoftWindows.

По сути, была разработана новая конфигурация, реализующая математические модели, раздела 3. Интерфейс программы представлен на рис. 1.



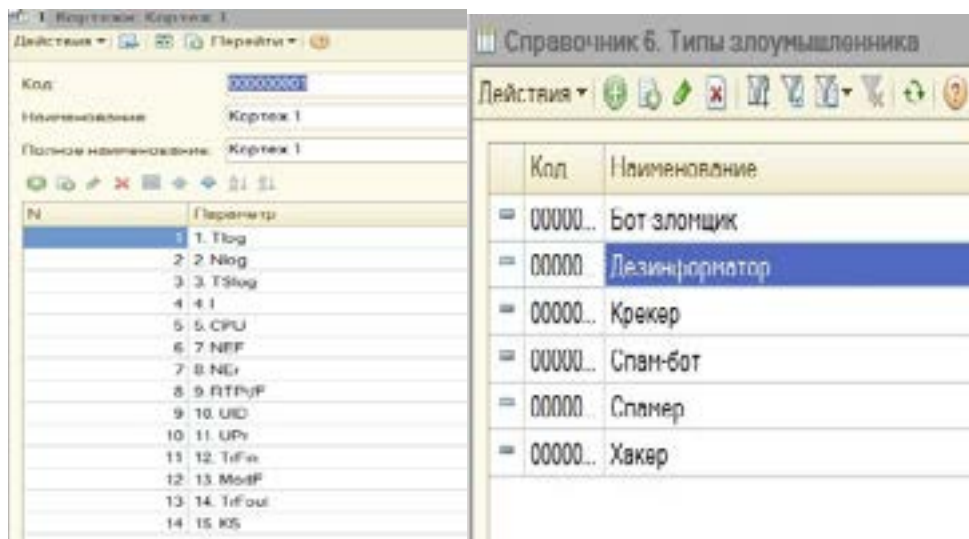
*Рис. 1 – Интерфейс программного средства «Система обнаружения и идентификации нарушителя в киберпространстве»*

*(Pic. 1 – Interface of the software tool “System for detecting and identifying an intruder in cyberspace”)*

В среде IC для работы с постоянной и условно постоянной информацией с некоторым множеством значений в системе используются объекты типа «Справочники». Для реализации предложенных математических моделей были созданы следующие объекты типа «Справочники»: «Кортежи», «Параметры», «Лингвистические Переменные», «Интервалы», «Эксперты», «Типы Злоумышленника», «Лингвистические Идентификаторы». В меню «Справочники» в интерфейсе можно получить доступ к этим справочникам.

В справочнике «Кортежи» хранятся кортежи, используемые при работе системы для обнаружения и идентификации злоумышленника и список параметров, из которых он состоит. На рис. 2а приведены окна формы элемента указанного справочника.

Справочник «Эксперты» служит для хранящейся информации по всем экспертам, принимавшим участие в исследовании (количество экспертов может быть большим, а при проведении эксперимента есть возможность выбрать эксперта с необходимой компетенцией, формировавшего эталоны и правила), а справочник «Типы Злоумышленника» необходим для хранения перечня злоумышленников, выявлявшихся при экспериментальном исследовании. На рис. 2б представлено окно формы списка справочника «Типы злоумышленника».

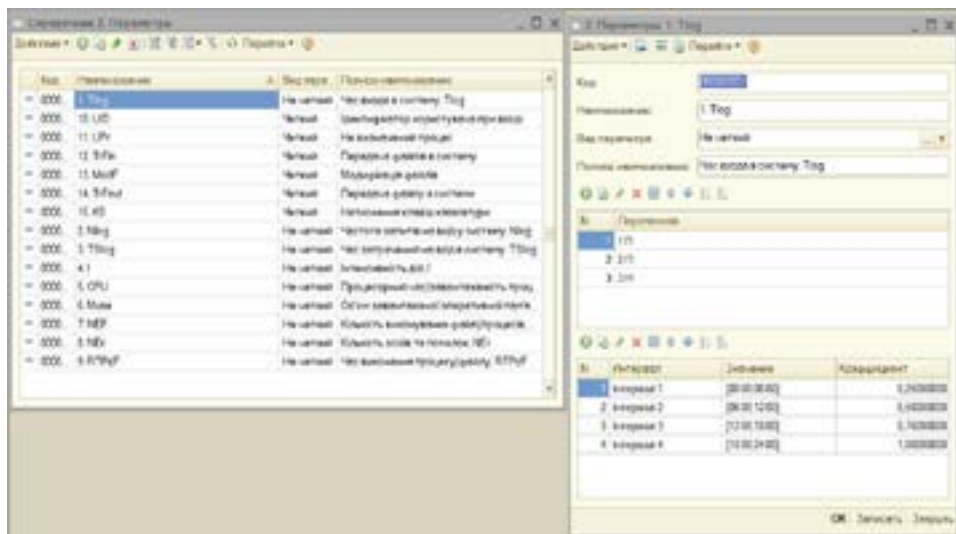


а) окно формы элемента справочника «Кортеж»

б) окно формы списка справочника «Типы злоумышленника»

(a) the form window of the “Tuple” directory element

b) the window of the list form of the reference book “Type of Manslayer”)



в) окно формы списка и формы элемента справочника «Параметры» (the window of the list form and the form of the “Parameters” directory element *Pic. 2-Examples of form windows of developed reference books*)

В справочнике «Параметры» хранятся все параметры, задействованные в кортежах. Также в каждом параметре указываются интервалы и лингвистические переменные. Для наглядности на рис. 2в приведены окна формы перечня и формы элемента справочника «Параметры».

Справочники “Лингвистические Переменные” и “Интервалы” служат для хранения информации о вышеуказанных лингвистических переменных и интервалах. Справочник «Лингвистические Идентификаторы» служит для хранящейся информации по всем лингвистическим идентификаторам, используемым в исследовании.

В ИС с помощью объектов типа «Документы» организуется ввод в систему информации об осуществлении любых операций, а также их просмотре и корректировке. В разработанной конфигурации были созданы следующие объекты типа “Документы”: “Установка Эталонов”, “Установка Правил”, “Эксперимент”. В меню «Документы» в интерфейсе можно получить доступ к этим документам.

Эталоны параметров задаются экспертом в документе «Установка эталонов» (например, см. рис. 3). На вкладке Данные эксперта экспертом заполняются значения каждого из интервалов изменения параметра. Программное средство автоматически строит график функции принадлежности эталонов лингвистического изменения.

В документе «Установка правил» эксперт задает используемые в системе лингвистические идентификаторы (пример, см. рис. 4) на вкладке «ЛИ» и присваивает один из них (Н, БНВ, БВН, В, К) соответствующим правилам на вкладке “Правила”.

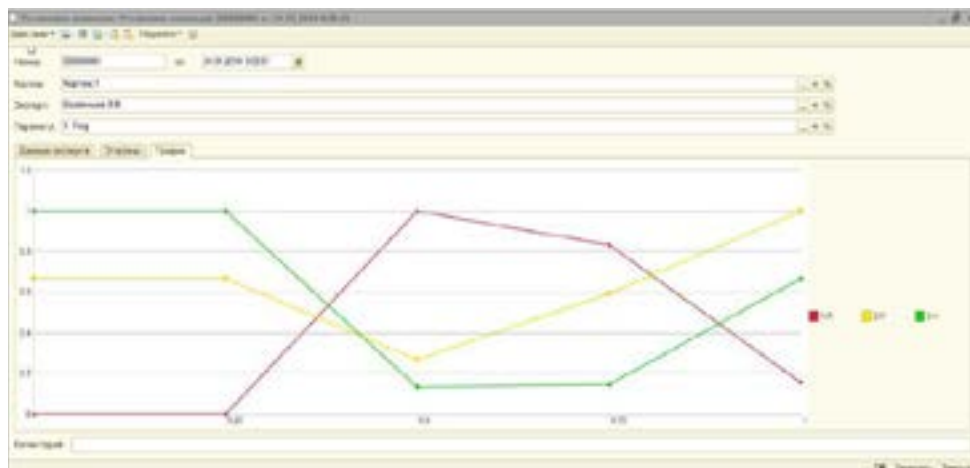


Рис. 3 – Окно формы элемента документа “Установка эталонов”  
 (Pic.3 – The window of the form of the document element “Setting standards”)

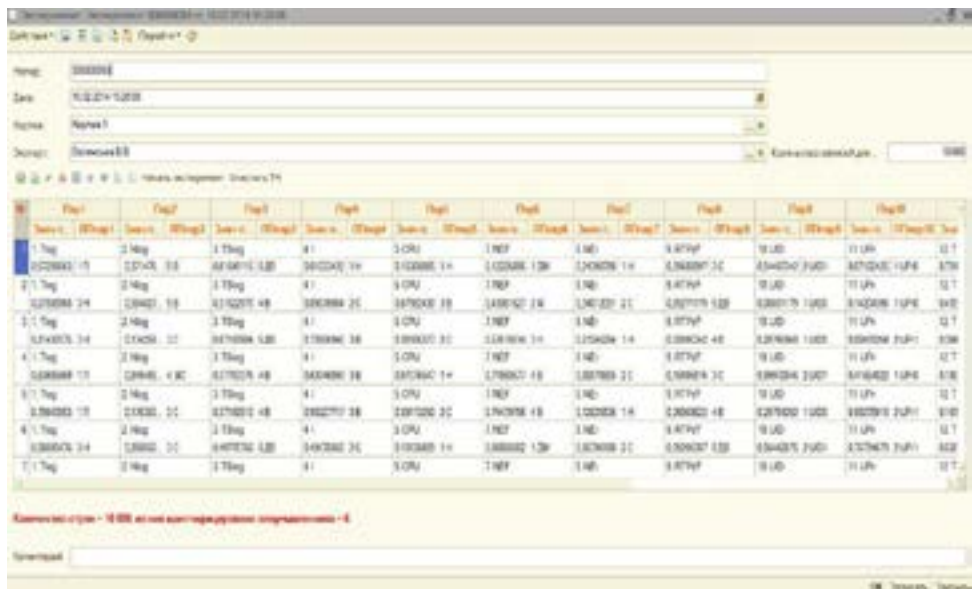
После указания эталонов и лингвистических идентификаторов с помощью документа «Эксперимент» можно произвести имитационное моделирование состояния киберпространства и выявление факта нарушения и категории злоумышленника.

№	Имя правила	Лингвистическая комбинация	Пар	Пар1	Пар2	Пар3	Пар4	Пар5	Пар6	Пар7	Пар8	Пар9	Пар10
0101	2.020	1 Tag+17.2 Mag+4.0 3 Tlog+0.20 4 1+3 0 5 CPU+0.0 7 Net+0.20 8 Net+1 H.5	1 Tag	0 Mag	0 Tlog	4.1	0 CPU	7 Net	0 Net	0 Tlog	0.20	4	1+3
0201	3.020	1 Tag+21.0 Mag+48.0 3 Tlog+0.20 4 1+3 0 5 CPU+0.0 7 Net+0.20 8 Net+1 H.5	1 Tag	0 Mag	0 Tlog	4.1	0 CPU	7 Net	0 Net	0 Tlog	0.20	4	1+3
0301	2.020	1 Tag+14.2 Mag+48.0 3 Tlog+0.20 4 1+3 0 5 CPU+0.0 7 Net+0.20 8 Net+1 H.5	1 Tag	2 Mag	0 Tlog	4.1	0 CPU	7 Net	0 Net	0 Tlog	0.20	4	1+3
0401	2.020	1 Tag+17.2 Mag+48.0 3 Tlog+0.20 4 1+3 0 5 CPU+0.0 7 Net+0.20 8 Net+1 H.5	1 Tag	0 Mag	0 Tlog	4.1	0 CPU	7 Net	0 Net	0 Tlog	0.20	4	1+3

Рис. 4 – Окно формы элемента документа «Установка правил»  
 (Pic. 4 – The form window of the document element “Setting rules”)

В форме элемента документа «Эксперимент» задается количество серий опыта в графе «Количество записей для опыта», также остальные характеристики (дата, кортеж, эксперт) и происходит его запуск (окно формы элемента изображено на рис. 5).





*Рис. 5 – Окно формы элемента документа «Эксперимент»  
(Pic. 5 – The form window of the document element “Experiment”)*

**Обсуждение**

В ИС отчеты используются для получения сводной информации на основании данных, введенных в системе. В разработанной конфигурации был создан только один объект типа Отчеты – Отчет Моделирования. С помощью данного отчета можно получить доступ к подробному отчету по результатам проведения имитационного моделирования, осуществляемого программным средством. Через меню Отчеты в интерфейсе можно получить доступ к данному отчету.

**Заклучение**

Таким образом, в работе разработан метод раннего обнаружения и идентификации нарушителя в ИКС, который за счет использования методов нечеткой логики, дает возможность выявить нарушителя информационной безопасности в слабо формализуемой среде и более точно его идентифицировать в соответствии с выделенными категориями. Метод включает в себя 3 фазы и 8 этапов. Входными данными являются сетевые и / или хостовые параметры и идентификаторы нарушителя (возможные категории), на выходе формируется сообщение о фиксации факта нарушителя и результат процедуры категоризации нарушителя.

В дальнейшем, на основе предложенного метода будет разработана система, которая будет эффективно выявлять и идентифицировать нарушителя с определенной степенью уверенности эксперта. Кроме этого, используя разработанное программное обеспечение, планируется провести экспериментальное исследование предложенного метода.

## ЛІТЕРАТУРА

Авкурова Ж., Абдураимова Б., Гнатюк С., Гизун А. 2020 — *Авкурова Ж., Абдураимова Б., Гнатюк С., Гизун А.* / Анализ современных систем обнаружения атак на основе технологий виртуальной приманки // №6(142) *Вестник КазНУИТ*, с.654-659, ноябрь, 2020

Balas E. 2004 — *Balas E.* Honeynetdataanalysis: A technique for correlatingsebek and network data /E. Balas //Workshop Information Assurance and Security US Military Academy, WestPoint, NY. — IEEE, 2004.

Deal R. Router Firewall Security / R. Deal., 2004 — *Deal R.* SF. : Cisco Press, 2004. — P. 912.

Fan W., Du Z., Fernández and D. Villagrà V.A., 2018 — *Fan W., Du Z., Fernández and D. Villagrà V.A.* “Enablingan Anatomic View to Investigate Honeypot Systems: A Survey,” in IEEE SystemsJournal, vol. 12, no. 4, pp. 3906-3919, Dec. 2018, doi:10.1109/JSYST.2017.2762161.

Grimes R. Honeypots for Windows / R. Grimes 2005 — *Grimes R. Honeypots for Windows / R. Grimes. W.* : APress, 2005. — P. 424.

Gnatyuk S., Berdibayev R., Avkurova Z., Verkhovets O., Bauyrzhan M. 2021 — *Gnatyuk S., BerdibayevR., AvkurovaZ., VerkhovetsO., BauyrzhanM.* Studiesoncloud-basedcyberincidentsdetection and identification in critical infrastructure, CEUR Workshop Proceedings, 2021, Vol. 2923, pp. 68-80.

Iashvili G., Avkurova Z., Iavich M., Bauyrzhan M., Gagnidze A., Gnatyuk S. 2021 — *Iashvili G., Avkurova Z., Iavich M., Bauyrzhan M., Gagnidze A., Gnatyuk S.* Content-Based Machine Learning Approach for Hardware Vulnerabilities Identification System, Lecture Notes on Data Engineering and Communications Technologies, Vol. 83, pp. 117-126, 2021.

Khosravi M. and Ladani B.T. 2020 — *Khosravi M. and Ladani B.T.* “Alerts Correlation and Causal Analysis for APT Based Cyber Attack Detection,” in IEEE Access, vol. 8, pp. 162642-162656, 2020, doi: 10.1109/ACCESS.2020.3021499.

Ma Z., Li Q. and Meng X., 2019 — *Ma Z., Li Q. and Meng X.,* “Discovering Suspicious APT Families Through a Large-Scale Domain Graph in Information-Centric IoT,” in IEEE Access, vol. 7, pp. 13917-13926, 2019, doi: 10.1109/ACCESS.2019.2894509.

Provos N., 2017 — *Provos N.* Virtual Honeypots: From Botnet Trackingto Intrusion Detection. — NY : Addison-Wesley Professional, 2007. — 440 p

Siddiqui, S. KhanM. S., FerensK. and Kinsner W., 2016 — *Siddiqui, S. KhanM. S., FerensK. and Kinsner W.* “Detecting advanced persistent threats using fractal dimension based machine learning classification”, Proc. ACM Int. Workshop Secur. Privacy Anal. (IWSPA), pp. 64-69, 2016.

Spitzne L. Honeypots: Tracking Hackers / L. Spitzner, 2002 — *Spitzne L. Honeypots: Tracking Hackers / L. Spitzner. NY* : Addison-Wesley Professional, 2002. — 480 p.

Tang J., Xu M., Fu S. and Huang K., 2018 — *Tang J., Xu M., Fu S. and Huang K.* “A scheduling optimization technique based on reuse in spark to defend against apt attack,” in Tsinghua Science and Technology, vol. 23, no. 5, pp. 550-560, Oct. 2018, doi: 10.26599/TST.2018.9010022.

Волянська В.В. 2012 — *Волянська В.В.* Огляд систем виявлення вторгень на основі honeypot-технологій // В.В. Волянська, А.І. Гизун, В.О. Гнатюк / Безпека інформації. - 2012. - №2 (18). – С. 75-79.

Yan L. and Xiong J., 2020 — *Yan L. and Xiong J.* “Web-APT-Detect: A Framework For Web-Based Advanced Persistent Threat Detection Using Self-Translation Machine With Attention,” in IEEE Letters of the Computer Society, vol. 3, no. 2, pp. 66-69, 1 July-Dec. 2020, doi: 10.1109/LOCS.2020.2998185.

## REFERENCES

Avkurova ZH., Abduraimova B., Gnatyuk S., Gizon A. 2020 — *Avkurova ZH., Abduraimova B., Gnatyuk S., Gizon A.* / Analiz sovremennyh system obnaruzheniya atak na osnove tekhnologij virtual'noj primanki // №6 (142) *Vestnik KazNITU*, s.654-659, noyabr', 2020. [Analysisofmodernintrusiondetectionsystemsbasedonvirtualhoneypottechnologies]

Balas E., 2004 — *Balas E.* Honeynet data analysis: A technique for correlating sebek and network data /E.Balas //Workshop on Information Assurance and Security US Military Academy, WestPoint, NY. — IEEE, 2004.

Deal R. Router Firewall Security / R. Deal. 2004 — *Deal R. Router Firewall Security / R. Deal. SF.* : CiscoPress, 2004. — P. 912.

Fan W., Du Z., Fernández and D. Villagrà V.A., 2018 — *Fan W., Du Z., Fernández and D. Villagrà V.A.* “Enabling a natomic View to Investigate Honeypot Systems: A Survey,” in *IEEE Systems Journal*, vol. 12, no. 4, pp. 3906-3919, Dec. 2018, doi:10.1109/JSYST.2017.2762161.

Grimes R. Honeypotsfor Windows / R. Grimes. 2005 — *Grimes R. Honeypotsfor Windows / R. Grimes. / W.* : APress, 2005. — P. 424.

Gnatyuk S., Berdibayev R., Avkurova Z., Verkhovets O., Bauyrzhan M. 2021 — *Gnatyuk S., Berdibayev R., Avkurova Z., Verkhovets O., Bauyrzhan M.* Studies on cloud-based cyber incidents detection and identification in critical infrastructure, *CEUR Workshop Proceedings*, 2021, Vol. 2923, pp. 68-80.

Iashvili G., Avkurova Z., Iavich M., Bauyrzhan M., Gagnidze A., Gnatyuk S. 2021 — *Iashvili G., Avkurova Z., Iavich M., Bauyrzhan M., Gagnidze A., Gnatyuk S.* Content-Based Machine Learning Approach for Hardware Vulnerabilities Identification System, *Lecture Notes on Data Engineering and Communications Technologies*, Vol. 83, pp. 117-126, 2021.

Khosravi M. and Ladani B.T., 2020 — *Khosravi M. and Ladani B.T.* “Alerts Correlation and Causal Analysis for APT Based Cyber Attack Detection,” in *IEEE Access*, vol. 8, pp. 162642-162656, 2020, doi: 10.1109/ACCESS.2020.3021499.

Ma Z., Li Q. and Meng X., 2019 — *Ma Z., Li Q. and Meng X.* “Discovering Suspicious APT Families Through a Large-Scale Domain Graph in Information-Centric IoT,” in *IEEE Access*, vol. 7, pp. 13917-13926, 2019, doi: 10.1109/ACCESS.2019.2894509.

Provos N. 2007 — *Provos N.* *Virtual Honeypots: From Botnet Tracking to Intrusion Detection.* — NY : Addison-WesleyProfessional, 2007. — 440 p.

Siddiqui S., Khan M.S., Ferens K. and Kinsner W., 2016 — *Siddiqui S., Khan M.S., Ferens K. and Kinsner W.* “Detecting advanced persistent threats using fractal dimension based machine learning classification”, *Proc. ACM Int. Workshop Secur. Privacy Anal. (IWSPA)*, pp. 64-69, 2016.

Spitzne L. Honeypots: Tracking Hackers / L. Spitzner. — NY : Addison-Wesley Professional, 2002. — 480 p.

Tang J., Xu M., Fu S. and Huang K., 2018 — *Tang J., Xu M., Fu S. and Huang K.* “A scheduling optimization technique based on reuse in spark to defend against apt attack,” in *Tsinghua Science and Technology*, vol. 23, no. 5, pp. 550-560, Oct. 2018, doi: 10.26599/TST.2018.9010022.

Volyanskaya V.V., 2012 — *Volyanskaya V.V.* *Obzor system obnaruzheniya vtorzhenij na osnove honeypot-tehnologij // V.V. Volyanskaya, A.I. Gizun, V.A. Gnatyuk / Bezopasnost' informacii.* – 2012. – №2 (18). – S. 75-79. [An Over view of Honey pot Intrusion Detection Systems]

Yan L. and Xiong J., 2020 — *Yan L. and Xiong J.* “Web-APT-Detect: A Framework For Web-Based Advanced Persistent Threat Detection Using Self-Translation Machine With Attention,” in *IEEE Letters of the Computer Society*, vol. 3, no. 2, pp. 66-69, 1 July-Dec. 2020, doi: 10.1109/LOCS.2020.2998185.

## МАЗМҰНЫ

<b>Ж.К. Абдугулова, Г.А. Ускенбаева, М.Н. Тлеген, А.К. Шукирова</b> ҚҰБЫР ЖАБДЫҒЫНДА МАЙДЫ ҚЫЗДЫРУДЫҢ ТЕХНОЛОГИЯЛЫҚ ПРОЦЕСІН АВТОМАТТАНДЫРУ.....	5
<b>Ж.С. Авкурова, С. Гнатюк, Л.М. Кыдыралина, Н.К. Курмангалиева</b> АҚПАРАТТЫҚ-КОММУНИКАЦИЯЛЫҚ ЖҮЙЕЛЕРДЕ ҚҰҚЫҚ БҰЗУШЫНЫ ЕРТЕ АНЫҚТАУ ЖӘНЕ СӘЙКЕСТЕНДІРУДІҢ ИНТЕЛЛЕКТУАЛДЫ ӘДІСІ.....	22
<b>А. Бекарыстанкызы, Ө. Ж. Мамырбаев</b> АГГЛЮТИНАТИВТІ ТІЛДЕРГЕ АРНАЛҒАН СӨЙЛЕУДІ АВТОМАТТЫ ТҮРДЕ ТАҢУ ЖҮЙЕСІ.....	37
<b>А.С. Еримбетова, Э.Н. Дайырбаева, Л. Черикбаева</b> БИКУБТЫҚ ИНТЕРПОЛЯЦИЯҒА НЕГІЗІНДЕ СУРЕТТЕРГЕ ЖАСЫРЫН АҚПАРАТТЫ ЕНГІЗУ.....	50
<b>М.Б. Есенова, Г.Б. Абдикеримова, А. Толстой, Ж.Б. Ламашева, А.А. Некесова</b> БИДАЙДАҒЫ АРАМШӨПТЕР ОШАҒЫН АНЫҚТАУ ҮШІН ТЕКСТУРАЛЫҚ БЕЛГІЛЕР ӘДІСТЕРІН ҚОЛДАНУ.....	64
<b>Л.З. Жолшиева, Т.К. Жукабаева, Ш. Тураев, М.А. Бердиева, Р.К. Сенгирбаева</b> НАҚТЫ УАҚЫТ РЕЖИМІНДЕ МЕДИАРИPE ЖӘНЕ SVM АРҚЫЛЫ ҚАЗАҚ ЫМ ТІЛІН ТАҢУ.....	82
<b>Ж.С. Иксебаева, К. Жетписов, А.Б. Медешова, И.М. Бапиев, Ж.Ж. Багисов</b> ҒАЛЫМДАРДЫҢ ҒЫЛЫМИ ЖОБАЛАР БОЙЫНША ГРАНТТЫҚ ҚАРЖЫЛАНДЫРУҒА ҚАТЫСУҒА ӨТІНІМДЕРІН ДАЙЫНДАУДЫҢ АҚПАРАТТЫҚ ЖҮЙЕСІ.....	94
<b>А.А. Иманберді, Р.Н. Молдашева</b> ӘЛЕУМЕТТІК МЕДИА ТАРАТУ ҮЛГІЛЕРІНЕ ШОЛУ.....	107
<b>Г. Қалман, М.Ғ. Есмағанбет, М.М. Жаманкарин, А.И. Габдулина, Д.В. Плескачев</b> КЛАСТЕРЛЕУ ӘДІСІН ҚОЛДАНЫП КОРЕФЕРЕНЦИЯН ШЕШУ.....	121

<b>Қ.Т. Қырғызбай, Е.Х. Какимжанов</b> ГАЗ ТЕХНОЛОГИЯЛАРЫ НЕГІЗІНДЕ АЛМАТЫ ОБЛЫСЫНЫҢ ГЕОДЕРЕКТЕР БАЗАСЫН ҚҰРУ ВІТСОІН ЖЕЛІСІНДЕГІ КҮДІКТІ ТРАНЗАКЦИЯЛАРДЫ АНЫҚТАУ.....	136
<b>Ш.Ж. Мусиралиева, М.Ж. Шайзат, А.К. Бекетова, Е. Абайұлы, А.Б. Манасова</b> ВІТСОІН ЖЕЛІСІНДЕГІ КҮДІКТІ ТРАНЗАКЦИЯЛАРДЫ АНЫҚТАУ.....	154
<b>А.Ұ. Мұхиядин, Ұ.Т. Махажанова, М.У. Мукашева, А.А. Муханова</b> АҚПАРАТТЫҚ ТЕХНОЛОГИЯЛАР ТӨТЕНШЕ ЖАҒДАЙДА ҚАШЫҚТАН ОҚЫТУДА ЭКСПЕРИМЕНТТЫҚ ДЕРЕКТЕРДІ ТАЛДАУ ҚҰРАЛЫ РЕТІНДЕ.....	170
<b>А.Б. Тоқтарова, Б.С. Омаров, Г.Н. Казбекова, С.А. Мамиков, Ф.Е. Темірбекова</b> ӘЛЕУМЕТТІК ЖЕЛІДЕГІ ҚАЗАҚ ТІЛДІ БЕЙӘДЕП СӨЗДЕР ҚОРЫН МАШИНАЛЫҚ ОҚЫТУДА ЖИНАҚТАУ.....	191
<b>А.Ә. Шекербек, Г.Б. Абдикеримова, Ж.Б. Ламашева, М.Г. Байбулова, А.К. Токкулиева</b> ТЕРЕҢ ОҚЫТУ АЛГОРИТМІМЕН РЕНТГЕНДІК КЕСКІННІҢ КЛАССИФИКАЦИЯСЫ.....	204
<b>Э.Э. Эльдарова</b> JPEG2000 ҚЫСУЫНАН KEЙІН ЦИФРЛІК БЕЙНЕЛЕРДІҢ ВИЗУАЛДЫ САПАСЫН ЖАҚСАРТУ.....	228

## СОДЕРЖАНИЕ

<b>Ж.К. Абдугулова, Г.А. Ускенбаева, М.Н. Глеген, А.К. Шукирова</b> АВТОМАТИЗАЦИЯ ТЕХНОЛОГИЧЕСКОГО ПРОЦЕССА ПОДОГРЕВА НЕФТИ НА ТРУБОПРОВОДНОМ ОБОРУДОВАНИИ.....	5
<b>Ж.С. Авкурова, С.А. Гнатюк, Л.М. Кыдыралина, Н.К. Курмангалиева</b> ИНТЕЛЛЕКТУАЛИЗИРОВАННЫЙ МЕТОД РАННЕГО ВЫЯВЛЕНИЯ ИДЕНТИФИКАЦИИ НАРУШИТЕЛЯ В ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ СИСТЕМАХ.....	22
<b>А. Бекарыстанқызы, О. Ж. Мамырбаев</b> ИНТЕГРАЛЬНАЯ СИСТЕМА АВТОМАТИЧЕСКОГО РАСПОЗНАВАНИЯ СЛИТНОЙ РЕЧИ ДЛЯ АГГЛЮТИНАТИВНЫХ ЯЗЫКОВ.....	37
<b>А.С. Еримбетова, Э.Н. Дайырбаева, Л. Черикбаева</b> ВНЕДРЕНИЕ СКРЫТОЙ ИНФОРМАЦИИ В ИЗОБРАЖЕНИИ НА ОСНОВЕ БИКУБИЧЕСКОЙ ИНТЕРПОЛЯЦИИ.....	50
<b>М.Б. Есенова, Г.Б. Абдикеримова, А. Толстой, Ж.Б. Ламашева, А.А. Некесова</b> ПРИМЕНИМОСТЬ МЕТОДОВ АНАЛИЗА ТЕКСТУРНЫХ ИЗОБРАЖЕНИЙ ДЛЯ ВЫЯВЛЕНИЯ ОЧАГОВ СОРНЫХ ТРАВ ПШЕНИЦЫ.....	64
<b>Л.З. Жолшиева, Т.К. Жукабаева, Ш. Тураев, М.А. Бердиева, Р.К. Сенгирбаева</b> РАСПОЗНАВАНИЕ КАЗАХСКОГО ЖЕСТОВОГО ЯЗЫКА В РЕАЛЬНОМ ВРЕМЕНИ С ИСПОЛЬЗОВАНИЕМ MEDIAPIPE и SVM.....	82
<b>Ж.С. Иксебаева, К. Жетписов, А.Б. Медешова, И.М. Бапиев, Ж.Ж. Багисов</b> ИНФОРМАЦИОННАЯ СИСТЕМА ПОДГОТОВКИ ЗАЯВОК ДЛЯ УЧАСТИЯ В ГРАНТОВОМ ФИНАНСИРОВАНИИ УЧЕНЫХ ПО НАУЧНЫМ ПРОЕКТАМ.....	94
<b>А.А. Иманберді, Р.Н. Молдашева</b> ОБЗОР МОДЕЛЕЙ РАСПРОСТРАНЕНИЯ ИНФОРМАЦИИ В СОЦИАЛЬНЫХ СЕТЯХ.....	107

<b>Г. Қалман, М.Ғ. Есмағанбет, М.М. Жаманқарин, А.Г. Габдулина, Д.В. Плескачев</b> РЕШЕНИЕ КОРЕФЕРЕНЦИИ С ПОМОЩЬЮ МЕТОДА КЛАСТЕРИЗАЦИИ.....	121
<b>Қ.Т. Қырғызбай, Е.Х. Какимжанов</b> СОЗДАНИЕ БАЗЫ ГЕОДАНЫХ АЛМАТИНСКОЙ ОБЛАСТИ НА ОСНОВЕ ГИС-ТЕХНОЛОГИЙ О МЕТОДЕ ИДЕНТИФИКАЦИИ ПОДОЗРИТЕЛЬНЫХ ТРАНЗАКЦИЙ В БИТКОИН СЕТИ.....	136
<b>Ш.Ж. Мусиралиева, М.Ж. Шайзат, А.К. Бекетова, Е. Абайұл, А.Б. Манасова</b> О МЕТОДЕ ИДЕНТИФИКАЦИИ ПОДОЗРИТЕЛЬНЫХ ТРАНЗАКЦИЙ В БИТКОИН СЕТИ.....	154
<b>А.Ұ. Мұхиядин, У.Т. Махажанова, М.У. Мукашева, А.А. Муханова</b> ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ КАК СРЕДСТВО АНАЛИЗА ЭКСПЕРИМЕНТАЛЬНЫХ ДАННЫХ ПРИ ЭКСТРЕННОМ ДИСТАНЦИОННОМ ОБУЧЕНИИ.....	170
<b>А.Б. Токтарова, Б.С. Омаров, Г.Н. Казбекова, С.А. Мамиков, Ф.Е. Темирбекова</b> СБОР БАЗЫ ДАННЫХ О ЯЗЫКЕ НЕНАВИСТИ В СОЦИАЛЬНОЙ СЕТИ НА КАЗАХСКОМ ЯЗЫКЕ С ИСПОЛЬЗОВАНИЕМ МАШИННОГО ОБУЧЕНИЯ.....	191
<b>А.А. Шекербек, Г.Б. Абдикеримова, Ж.Б. Ламашева, М.Г. Байбулова, А.К. Токкулиева</b> КЛАССИФИКАЦИЯ РЕНТГЕНОВСКИХ ИЗОБРАЖЕНИЙ С ПОМОЩЬЮ АЛГОРИТМА ГЛУБОКОГО ОБУЧЕНИЯ.....	204
<b>Э.Э. Эльдарова</b> УЛУЧШЕНИЕ ВИЗУАЛЬНОГО КАЧЕСТВА ЦИФРОВЫХ ИЗОБРАЖЕНИЙ ПОСЛЕ СЖАТИЕ JPEG2000.....	228

## CONTENTS

<b>J.K. Abdugulova, G.A. Uskenbayeva, M.N. Tlegen, A.K. Shukirova</b> AUTOMATION OF THE TECHNOLOGICAL PROCESS OF HEATING OIL PIPELINE EQUIPMENT.....	5
<b>Z. Avkurova, S. Gnatyuk, L. Kydyralina, N. Kurmangaliev</b> THE INTELLECTUALIZED METHOD OF EARLY DETECTION AND IDENTIFICATION OF THE VIOLATOR IN INFORMATION AND COMMUNICATION SYSTEMS.....	22
<b>A. Bekarystankyzy, O. Zh. Mamyrbayev</b> INTEGRATED AUTOMATIC SPEECH RECOGNITION SYSTEM FOR AGGLUTINATIVE LANGUAGES.....	37
<b>A. Yerimbetova, E. Daiyrbayeva, L. Cherikbayeva</b> EMBEDDING HIDDEN INFORMATION IN IMAGES BASED ON BICUBIC INTERPOLATION.....	50
<b>M. Yessenova, G. Abdikerimova, A. Tolstoy, Zh. Lamasheva, A. Nekessova</b> APPLICABILITY OF TEXTURE IMAGE ANALYSIS METHODS FOR DETECTION OF WHEAT WEED POCKS.....	64
<b>L. Zholshiyeva, T. Zhukabayeva, Sh. Turaev, M. Berdieva, R. Sengirbayeva</b> REAL-TIME KAZAKH SIGN LANGUAGE RECOGNITION USING MEDIAPIPE AND SVM.....	82
<b>Zh.S. Ixebayeva, K. Jetpisov, A.B. Medeshova, I.M. Bapiyev , Zh.Zh. Bagisov</b> AN INFORMATION SYSTEM FOR THE PREPARATION OF APPLICATIONS FOR PARTICIPATION IN GRANT FUNDING OF SCIENTISTS IN SCIENTIFIC PROJECTS.....	94
<b>A. Imanberdi, R. Moldasheva</b> REVIEW OF MODELS OF DISSEMINATION OF INFORMATION IN SOCIAL NETWORKS.....	107
<b>G. Kalman, M.G. Esmaganbet, M.M. Zhamankarin, A.I. Gabdulina, D.V. Pleskachev</b> COREFERENCE SOLUTION USING THE CLUSTERING METHOD.....	121



<b>K. Kyrgyzbay, E. Kakimzhanov</b> CREATION OF A GEODATABASE OF ALMATY REGION BASED ON GIS TECHNOLOGIES.....	136
<b>Sh. Mussiraliyeva, M. Shaizat, A. Beketova, Y. Abayuly, A. Manassova</b> IDENTIFICATION OF SUSPICIOUS TRANSACTIONS IN THE BITCOIN NETWORK.....	154
<b>A. Mukhiyadin, U. Makhazhanova, M. Mukasheva, A. Mukhanova</b>  INFORMATION TECHNOLOGIES AS A MEANS OF EXPERIMENTAL DATA ANALYSIS IN EMERGENCY DISTANCE LEARNING.....	170
<b>A.B. Toktarova, B.S. Omarov, G.N. Kazbekova, S.A. Mamikov, F.E. Temirbekova</b> COLLECTING HATE SPEECH DATABASE ON SOCIAL NETWORK IN KAZAKH LANGUAGE BY USING MACHINE LEARNING.....	191
<b>A. Shekerbek, G. Abdikerimova, Zh. Lamasheva, M. Baibulova, A. Tokkulyeva</b> CLASSIFICATION OF X-RAY IMAGES USING THE DEEP LEARNING ALGORITHM.....	204
<b>E.E. Eldarova</b> IMPROVING THE VISUAL QUALITY OF DIGITAL IMAGES AFTER JPEG2000 COMPRESSION.....	228

**Publication Ethics and Publication Malpractice  
the journals of the National Academy of Sciences of the Republic of Kazakhstan**

For information on Ethics in publishing and Ethical guidelines for journal publication see <http://www.elsevier.com/publishingethics> and <http://www.elsevier.com/journal-authors/ethics>.

Submission of an article to the National Academy of Sciences of the Republic of Kazakhstan implies that the described work has not been published previously (except in the form of an abstract or as part of a published lecture or academic thesis or as an electronic preprint, see <http://www.elsevier.com/postingpolicy>), that it is not under consideration for publication elsewhere, that its publication is approved by all authors and tacitly or explicitly by the responsible authorities where the work was carried out, and that, if accepted, it will not be published elsewhere in the same form, in English or in any other language, including electronically without the written consent of the copyright-holder. In particular, translations into English of papers already published in another language are not accepted.

No other forms of scientific misconduct are allowed, such as plagiarism, falsification, fraudulent data, incorrect interpretation of other works, incorrect citations, etc. The National Academy of Sciences of the Republic of Kazakhstan follows the Code of Conduct of the Committee on Publication Ethics (COPE), and follows the COPE Flowcharts for Resolving Cases of Suspected Misconduct ([http://publicationethics.org/files/u2/New\\_Code.pdf](http://publicationethics.org/files/u2/New_Code.pdf)). To verify originality, your article may be checked by the Cross Check originality detection service <http://www.elsevier.com/editors/plagdetect>.

The authors are obliged to participate in peer review process and be ready to provide corrections, clarifications, retractions and apologies when needed. All authors of a paper should have significantly contributed to the research.

The reviewers should provide objective judgments and should point out relevant published works which are not yet cited. Reviewed articles should be treated confidentially. The reviewers will be chosen in such a way that there is no conflict of interests with respect to the research, the authors and/or the research funders.

The editors have complete responsibility and authority to reject or accept a paper, and they will only accept a paper when reasonably certain. They will preserve anonymity of reviewers and promote publication of corrections, clarifications, retractions and apologies when needed. The acceptance of a paper automatically implies the copyright transfer to the National Academy of Sciences of the Republic of Kazakhstan.

The Editorial Board of the National Academy of Sciences of the Republic of Kazakhstan will monitor and safeguard publishing ethics.

Правила оформления статьи для публикации в журнале смотреть на сайтах:

**[www.nauka-nanrk.kz](http://www.nauka-nanrk.kz)**

**<http://physics-mathematics.kz/index.php/en/archive>**

**ISSN 2518-1726 (Online),**

**ISSN 1991-346X (Print)**

Заместитель директора отдела издания научных журналов НАН РК *Р. Жалиқызы*

Редакторы: *М.С. Ахметова, Д.С. Аленов*

Верстка на компьютере *Г.Д. Жадыранова*

Подписано в печать 30.03.2023.

Формат 60x881/8. Бумага офсетная. Печать – ризограф.

15,5 п.л. Тираж 300. Заказ 1.