

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 Нұрсұлтан 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**

**WOICIK 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 Aldazarovna**, 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), 154-169  
<https://doi.org/10.32014/2023.2518-1726.175>

УДК 004.8, 004.9

© **Sh. Mussiraliyeva**, **M. Shaizat**, **A. Beketova**, **Y. Abayuly**,  
**A. Manassova**\*, 2023

Al-Farabi Kazakh National University, Kazakhstan, Almaty.  
E-mail: [manassova.akerke4493@gmail.com](mailto:manassova.akerke4493@gmail.com)

### IDENTIFICATION OF SUSPICIOUS TRANSACTIONS IN THE BITCOIN NETWORK

**MUSSIRALIYEVA Shynar** — Candidate of Physical and Mathematical Sciences. Head of the Department «Information System» of Al-Farabi Kazakh National University.

E-mail: [mussiraliyevash@gmail.com](mailto:mussiraliyevash@gmail.com), <http://orcid.org/0000-0001-5794-3649>;

**SHAIZAT Medet Zhanbolatovich** — doctoral student of the Department of Information Systems of Al-Farabi Kazakh National University.

E-mail: [m10.invictus@gmail.com](mailto:m10.invictus@gmail.com), <http://orcid.org/0000-0002-1651-8205>;

**BEKETOVA Ayman Kayyrbekovna** — senior lecturer of the Department of Information Systems of Al-Farabi Kazakh National University.

E-mail: [aiman.beketova@gmail.com](mailto:aiman.beketova@gmail.com), <http://orcid.org/0000-0003-4931-0563>;

**ABAYULY Yerulan** — doctoral student of the Department of Information Systems of Al-Farabi Kazakh National University.

E-mail: [a.erulan.97@gmail.com](mailto:a.erulan.97@gmail.com), <http://orcid.org/0000-0003-2248-3819>;

**MANASSOVA Akerke** — doctoral student of the Department of Information Systems of Al-Farabi Kazakh National University.

E-mail: [manassova.akerke4493@gmail.com](mailto:manassova.akerke4493@gmail.com), <http://orcid.org/0000-0001-8709-4617>.

**Abstract.** This article talks about one of the most popular cryptocurrencies today - bitcoin. The principles of bitcoin and blockchain technologies are considered, where the pros and cons of bitcoin are listed. The focus of the work is on the analysis of the use of cryptocurrencies, namely bitcoin for illegal and criminal purposes. Particular attention is paid to identifying a set of signs to identify suspicious activity in the bitcoin network. The article provides a practical example of a real case of illegal transactions in the bitcoin network, associated with fraudulent user actions. During research work reviewed and analyzed many scientific publications and articles, and from these studies, signs were identified that are key attributes when evaluating a Bitcoin transaction for suspicious or questionable transactions. Based on these features, an input dataset of 15 attributes with about 100,000 transactions

was formed for further use in creating a model that will evaluate bitcoin transactions for suspicion. After the formation of the dataset, models were created and trained to identify suspicious transactions in the bitcoin network based on several machine learning algorithms, such as random forest, k-nearest neighbors, decision tree. The article also provides comparisons of the results of machine learning algorithms, and in addition, chosen the best algorithm that showed the highest accuracy.

**Keywords:** Cryptocurrency, blockchain, bitcoin, suspicious transactions, features

© Ш.Ж. Мусиралиева, М.Ж. Шайзат, А.К. Бекетова, Е. Абайұлы,  
А.Б. Манасова\*, 2023

Әл-Фараби атындағы Қазақ ұлттық университеті, Қазақстан, Алматы.

E-mail: manassova.akerke4493@gmail.com

## БИТКОИН ЖЕЛІСІНДЕГІ КҮДІКТІ ТРАНЗАКЦИЯЛАРДЫ АНЫҚТАУ

**Аңдатпа.** Бұл мақалада қазіргі кездегі ең танымал криптовалютаның бірі Биткоин туралы мәліметтер айтылады. Биткоин мен блокчейн технологияларының жұмыс принциптері қарастырылады, оның ішінде Bitcoin-нің артықшылықтары мен кемшіліктері көрсетілген. Жұмыстың негізгі бағыты криптовалюталарды, атап айтқанда биткоинді заңсыз мақсаттарда пайдалануды талдауға бағытталған. Биткоин желісіндегі күдікті әрекеттерді анықтау үшін белгілер жинағын анықтауға ерекше назар аударылған. Мақалада пайдаланушының алаяқтық әрекеттерімен байланысты биткоин желісіндегі заңсыз транзакциялардың нақты жағдайының практикалық мысалы келтірілген. Зерттеу жұмысы барысында көптеген ғылыми жарияланымдар мен мақалалар қаралды және талданды және осы зерттеулерден күдікті немесе күмәнді транзакциялар үшін Bitcoin транзакциясын бағалау кезінде негізгі атрибуттар болып табылатын белгілер анықталды. Осы белгілердің негізінде, күдікті биткоин транзакцияларды бағалайтын модельді құруда одан әрі пайдалану үшін 100 000-ға жуық транзакциясы бар 15 атрибуттан тұратын кіріс деректер жинағы (датасет) жасалды. Деректер жинағы қалыптасқаннан кейін кездейсоқ орман, k-ең жақын көршілер, шешім ағашы сияқты бірнеше машиналық оқыту алгоритмдеріне негізделген биткоин желісіндегі күдікті транзакцияларды анықтау үшін модельдер жасалды және оқытылды. Сонымен қатар, мақалада машиналық оқыту алгоритмдерінің салыстырмалы талдауының нәтижелері, сондай-ақ жоғары дәлдікті қамтамасыз ететін алгоритм таңдалған.

**Түйін сөздер:** Криптовалюта, блокчейн, биткоин, күдікті транзакциялар, белгілер

© Ш.Ж. Мусиралиева, М.Ж. Шайзат, А.К. Бекетова, Е. Абайұлы,  
А.Б. Манасова\*, 2023

Казахский национальный университет имени аль-Фараби,  
Алматы, Казахстан.

E-mail: manassova.akerke4493@gmail.com

## **О МЕТОДЕ ИДЕНТИФИКАЦИИ ПОДОЗРИТЕЛЬНЫХ ТРАНЗАКЦИЙ В БИТКОИН СЕТИ**

**Аннотация.** Статья посвящена актуальному направлению научных исследований — анализу биткоин транзакций. В ней рассматриваются принципы и характер работы биткоина и блокчейн-технологий, перечисляются преимущества и недостатки биткоина. В работе внимание акцентируется на анализе использования криптовалют, а именно биткоина в незаконных и преступных целях. Особое внимание уделяется идентификации подборки признаков для определения подозрительной деятельности в сети биткоина. В статье приводится практический пример реального кейса незаконных транзакций в биткоин сети, связанный с мошенническими действиями пользователя. В ходе исследовательской работы были проведены обзор и анализ множества научных публикаций и статьи, а из этих исследований были выявлены признаки, которые являются ключевыми атрибутами при оценке Биткоин транзакции на предмет подозрительных или сомнительных операций. На основе этих признаков был сформирован входной датасет из 15 атрибутов и около 100 000 транзакциях для дальнейшего использования в создании модели, которая будет оценивать биткоин транзакции на предмет подозрительности. После формирования датасета были созданы и обучены модели для идентификации подозрительных операций в биткоин сети на основе нескольких алгоритмов машинного обучения, такие как случайный лес, Метод k-ближайших соседей, дерево решений. Кроме этого, в статье приведены результаты сравнительного анализа алгоритмов машинного обучения, а также выбран алгоритм, обеспечивающий высокую точность.

**Ключевые слова:** блокчейн, криптовалюта, биткоин, подозрительные транзакции, характеристики блокчейна

### **Введение**

В настоящее время развитие современных технологий привели к появлению цифровых валют, одной из которых является криптовалюта. Криптовалюта — цифровая платежная система, в которой не участвуют традиционные финансовые институты такие как банки (<https://www.kaspersky.ru>). Существуют много видов криптовалют, самый известный из них биткоин. Биткойн — первая в мире успешная криптовалюта, которая появилась на свет в 2009 году (Nakamoto и т.д., 2022). Биткоин — это децентрализованная

система, которая функционирует на базе программного протокола и основана на концепции прямого обмена между участниками.

Биткоин создавался как цифровая платежная система с открытым исходным кодом. Главная ценность этой системы в том, что в ней впервые удалось создать самодостаточную, надежную и децентрализованную систему для переводов (<https://forklog.com>).

Биткойны математически генерируются путем выполнения набора сложных задач с хешем числа с использованием процедуры, известной как «добыча» (<https://www.kaspersky.ru>). Люди, которые «добывают» биткойны называются «Майнерами». Майнеры обрабатывают журнал и подтверждают, что транзакции являются законными. Текущее среднее время, необходимое для проверки транзакции Биткоина, составляет около шести минут. Примерно половина всех транзакций подтверждается за это или меньшее количество времени (<https://phemex.com>).

Все транзакции в сети биткоина записываются в распределенный реестр данных — блокчейн. Блокчейн — это революционная технология, которая представила новые концепции безопасного обмена данными. Эта современная технология состоит из цепочки блоков, которая позволяет надежно хранить все совершенные транзакции с использованием общих и распределенных сетей (Салах и т.д., 2019).

Транзакции биткоин — это процесс перевода криптовалюты от одного кошелька другому кошельку с использованием технологии блокчейн. Транзакция представляет собой связанную с друг-другом цепочку блоков с данными обо всех перемещениях биткойнах между кошельками (<https://finswin.com>).

Блок — непрерывно записываемые файлы в сети Биткоин, которые содержат информацию о совершенных транзакциях.

В каждом из блоков содержится такая информация:

История проведенных ранее операций;

Информация о совершаемой транзакции (<https://www.researchgate.net>).

Каждый блок имеет одинаковую структуру как показано на рисунке 1, он состоит из заголовка, содержащего собственный хеш-код и хеш предшествующего, а также перечня транзакций, среди которых первая — с указанием награды майнера.



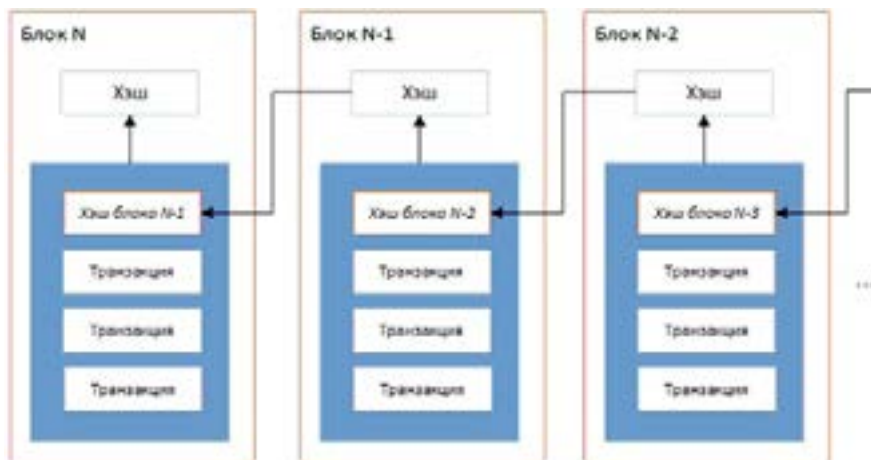


Рис. 1 – Структура блока

Транзакция начинается после её создания в кошельке и подписанием пользователем на основе закрытого ключа с цифровой подписью. Приватный ключ или закрытый ключ — это криптографическая защищенная часть данных с функцией, аналогичной паролю в учетной записи электронной почты. В Биткоин-транзакциях кроме закрытого ключа также используются публичный ключ. Публичный ключ или открытый ключ — это зашифрованные фрагменты данных, которые действуют аналогично адресам электронной почты (<https://www.bitcoin.com>). Участники Биткоин сети используют публичные ключи для отправки и получения криптовалют. Адрес Биткоин-кошелька это хэшированная версия публичного ключа. Когда биткоины отправляется другому пользователю, перевод содержит информацию о публичном ключе отправителя и публичном ключе получателя.

В сущности, биткоин транзакция состоит из трех частей:

Входные данные

Сумма транзакции

Выходные данные

Входные данные относятся к информации о балансе адреса отправителя до текущей выполняемой транзакций.

Когда пользователь отправляет один биткоин, система должна убедиться, что у него есть один полный биткоин, который он может отправить другому пользователю. Если все предыдущие транзакции на адрес пользователя были исходящими переводами, и он никогда не получал никаких средств, он не может ничего отправить. Таким образом, входные данные гарантируют, что перевод происходит с адреса, где необходимая сумма для перевода. Когда транзакция будет добавлена в блок, сумма в кошельке отправителя будет обновлена.

Вторая часть, сумма транзакции. Это относится к сумме, которую отправитель хочет перевести получателю.

Третий ключевой компонент, выходные данные, включают в себя информацию о распределении суммы перевода на адрес получателя. Доступная сумма в кошельке получателя обновляется, и эта обновленная информация позже будет использоваться в качестве входных данных для будущей транзакции с использованием этого адреса (Condos и т.д., 2016).

Блокчейн технологий обладают следующими особенностями:

В блокчейне хранятся только записи о событиях — транзакциях, то есть метаданные, а не сами данные. Сначала все записи валидируются на подлинность и подтверждаются при помощи криптографии, только после этого подаются в блокчейн. Записи хранятся в блоках, которые цепляются друг за друга, как звенья одной цепочки, а не в табличном виде, как классические базы данных. При этом каждый следующий блок включает зашифрованные данные о предыдущем. Информацию хранящуюся в блокчейн, нельзя модифицировать, менять, обновлять или удалять, не нарушив целостность всей цепочки (<https://www.seeneco.com>).

У биткойна низкие транзакционные издержки, что воспроизведен во многих его встроенных функциях. Как уже было сказано, биткойн — децентрализованная платёжная система, которая позволяет пользователям производить разные операции с биткойнами друг с другом без посредника или контролирующего органа, например, в случае с фиатными деньгами — это банки. Отсутствие посредника между покупателем и продавцом делает платежи более дешевыми, а обрабатывание транзакции более быстрым по сравнению с фиатными деньгами. Однако все эти особенности криптовалют, в частности биткойна также привлекают разного рода недобросовестных пользователей, которые используют сеть для разного рода преступной деятельности, например, по отмыванию денег или финансированию экстремизма или терроризма и обеспечила им преимущества перед законом (Ларин, 2018).

Самым главным и важным подходом в традиционных способах по борьбе с отмыванием денег или разного рода незаконными финансовыми операциями является контроль и наблюдение регулятора за посредниками, то есть за финансовыми организациями (банками), которые являются мостом между участниками финансовой операций, и имеют право мониторить и проверять сомнительные транзакции, а в случае чего отменять транзакции и замораживать деньги для тщательного изучения участников сделки и их цели (<https://www.seeneco.com>).

Поскольку в Биткойн сети отсутствуют такого рода посредники, то традиционная стратегия борьбы с отмыванием денег или с незаконными деньгами почти не работает (Ларин, 2018). Как было уже сказано несмотря на то, что каждая транзакция хранится в открытом доступе и может быть

прослежена, не существует прямой ссылки на конкретного человека или организацию, совершившую транзакцию.

Кроме этого, совершение транзакций в биткойнах значительно легче и гибче, чем традиционные средства, используемые для незаконной деятельности, а именно транзакция фиатных денег. Бумажные купюры несут с собой физическое ограничение в виде веса и размера, а миллионы биткойнов могут храниться на стандартном USB-устройстве и можно отправить любому пользователю в мире в течение очень короткого времени (Chuen и т.д., 2015). Также платежи Биткойн можно разбивать на более мелкие транзакций, что очень облегчает обход мер регулирования (Ajello, 2015).

### **Материал и методы исследования**

Многие люди считают, что Биткойн гарантирует полную анонимность, но на практике это не так, так как является псевдоанонимной сетью. История всех транзакции биткойнов доступны для публичного просмотра блокчейне, потому что блокчейн — это публичный реестр информации (<https://phemex.com>). Используя онлайн-обозреватели Биткойна, такие как платформа [blockchain.com](https://blockchain.com), любой желающий может просматривать всю историю транзакции любого кошелька, а также отслеживать эти транзакции и анализировать. Но, по сути, даже имея доступ к полной истории транзакции кошелька это ничего не рассказывает о личности пользователя.

Для того, чтобы продемонстрировать это на практическом примере был выбран случай, произошедший в сентябре 2018 года, когда хакеры получили несанкционированный доступ к горячему кошельку биржи Zaif и украли 5966 BTC (<https://incrypted.com>). Для анализа был выбран инструмент Crystal.

Все входящие адреса принадлежали Zaif. Как показано на рисунке 2, похищенные средства в биткойнах хакер отправил на адрес: *FmwHh6pgkf4meCMoqo8fHH3GNRF571f9w*.



Рис.2 - Перевод средств с кошельков Zaif на адрес хакера

Как видно на рисунке 3, адрес 1FmwHh6pgkf4meCMoqo8fHh3GNRF571f9w содержит 9 исходящих транзакций, таким образом, отслеживание применялось для каждой из них.

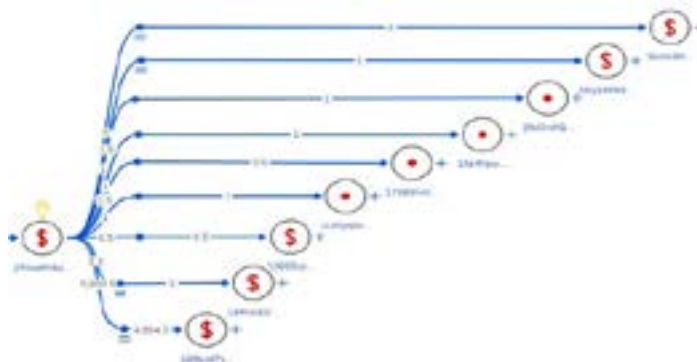


Рис. 3 – Исходящие транзакций по адресу 1FmwHh6pgkf4meCMoqo8fHh3GNRF571f9w

Как показано на рисунке 4, многие биткоины были разделены на относительно небольшие суммы (0.5 и 1 биткоин) и отправлены в течении очень короткого времени как видно на рисунке 5, на другие адресаты, у которых нет историй и не было больше никаких активностей за последние 4 года, что говорит о том, что это кошельки-однодневки.



Рис. 4 - Разбиения биткоинов на небольшие суммы

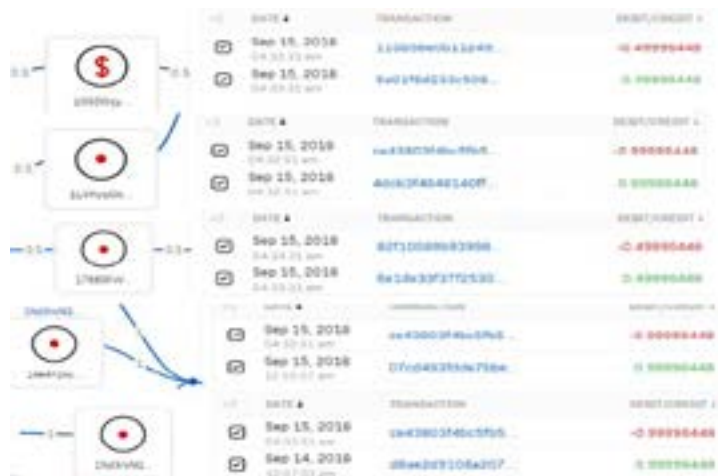


Рис. 5 - Кошельки-однодневки. Время и дата транзакций.

Проведя множество операций, описанные выше, были обнаружены больше 5 тысяч кошельков куда были переведены часть украденных средств. По итогам исследования было определено, что часть похищенных средств была отправлена на вывод через криптовалютную биржу Binance, другая часть — разбита на мелкие суммы и распределена на многочисленные адреса через игровые сервисы, миксеры и другие криптобиржи (<https://forklog.com>). Как было видно на этом примере, этому случаю характерны многие признаки, которые являются ключевыми атрибутами при оценке биткоин транзакции на предмет подозрительности.

*Идентификация подборки признаков для определения подозрительной операции.*

Этот раздел содержит подборку признаков подозрительной деятельности в сфере криптовалюты, а именно в сети биткоина или возможных попыток уклониться от разоблачения правоохранительными органами. В ходе исследовательской работы, в рамках которой проведены обзор и анализ научных публикаций и статьи, обзор литературы и из исследований открытых источников были выявлены и определены следующие признаки (факты, кейсы), которые являются ключевыми атрибутами (помогают) при оценке Биткоин транзакции на предмет подозрительных или сомнительных операций:

Операций перевода или обмена криптовалюты, как и аналогично в случае с фиатными деньгами, путем разбиения на небольшие суммы либо на суммы, не превышающие пороговых значений, установленных для обязательной регистрации операций или для передачи сообщений. А если говорить более подробно, то разбиение большого количество биткоинов на множество небольшое количество биткоинов и перевод биткоинов на последующие адресаты. Разделение связано с тем, что существуют разного рода правил от

Межправительственной комиссии по финансовому мониторингу (ФАТФ), например, одна из них называется «Travel Rule». Travel Rule, также известное как Рекомендация 16 ФАТФ, направлено на прекращение отмывания денег за счет сведения к минимуму анонимности крупных транзакций в криптовалюте. Правило путешествий уже давно применяется к фиатным транзакциям, и в 2018 году ФАТФ заявила, что страны должны также применять это правило к криптовалютным компаниям и обязать Провайдеры услуг в сфере виртуальных активов (ПУВА) получать, хранить и обмениваться информацией об отправителях и получателях криптовалютных переводов с другими ПУВА и выше 1000 долларов США (<https://www.coindesk.com>). Кроме этого, многие криптобиржи позволяют пользователям снимать до 1 биткоинов, то есть небольшие суммы денег, без прохождения строгого контроля.

Множество операции разбиения большого количество биткоинов на десятки и сотни транзакции, совершаются путем использования кошельков, у которых зачастую нет никаких истории, то есть, биткоин кошельки открывшиеся недавно или уже считающиеся спящими, другими словами, их можно называть кошельками-однодневками или транзитными кошельками. Если не все, то большинство биткоин кошельков такого типа, используются всего 2 раза. Первый раз для получения биткоинов (денег), второй раз для отправления полученных биткоинов (денег) на другой кошелек. После проведения таких операции биткоин кошельки перестают использоваться. Так как у одного пользователя может быть множество биткоин-кошельков;

Перевод биткоинов (денег) происходит в пожарном порядке по разным кошелькам и в очень короткие сроки, например, в пределах 30 минут или 1 часа;

Полученная сумма и отправленная сумма плюс комиссия является одинаковой суммой. Потому что, люди проводящие такие транзакции знают, что больше не будут использовать эти кошельки, поэтому переводят всю сумму (биткоин);

Разделенные биткоины после короткой цепочки транзакции примерно (5–6 транзакции) биткоины собираются заново в одном кошельке;

Обмен биткоина на другие виды криптовалют, с дополнительными расходами на комиссию за транзакции, но с сокрытием следа;

Внесение биткоина в криптобиржу, а затем немедленный вывод с биржи без проведения дополнительных операций, как покупку чего-либо или перевода на другой кошелек.

Все вышеперечисленные признаки были выявленные в ходе анализа более десятков практических примеров, взятых из научных публикаций и статей. Сразу хочется отметить, наличие одного из признаков не дает основание считать транзакцию как незаконную или преступную. Часто подозрение на возможную преступную деятельность вызывает именно наличие нескольких признаков в транзакциях, не имеющей логичного обоснования с точки зрения

поведения обычного пользователя. Наличие признаков должно служить толчком к проведению дальнейшего мониторинга и детального анализа.

*Формирование и описание датасета.* Следующий этап после идентификации основных признаков подозрительных транзакций для биткоинов, работа с данными: поиск и сбор данных, анализ и обработка собранных данных, формирование входных признаков датасета для обучения модели.

В рамках исследовательской работы, был создан датасет содержащий около 5 тысяч незаконных транзакций путем изучения известных случаев, связанных с кражей биткойнов, отмыванием биткойнов и т.д. Один из примеров был описан в предыдущем примере, это кража биткоинов, произошедший в сентябре 2018 года, когда хакеры получили несанкционированный доступ к горячему кошельку биржи Zaif и украли 5966 биткоинов (<https://incrypted.com>). Кроме этого, с целью увеличения количества транзакций в наборе данных был исследован известный набор данных в сфере биткойн транзакций «EllipticDataSet», крупнейший в мире набор данных с помеченными транзакциями. Набор данных включает 200 000 транзакций на общую сумму 6 миллиардов долларов. Этот набор данных был создан с целью, чтобы сообщества могла использовать собранные данные для выявления финансовых преступлений в криптовалютах (<https://www.kaggle.com>).

Эллиптический набор данных сопоставляет биткойн-транзакции с реальными объектами, принадлежащими к законным категориям (биржи, поставщики кошельков, майнеры, законные услуги и т.д.), а не с незаконными (мошенничество, вредоносное ПО, террористические организации, программы-вымогатели, схемы Понци и т.д.), а также неизвестных, процентное соотношение: 2% были помечены как незаконные, 21% как законные, а 77% как неизвестные.

Было сделано важное наблюдение о том, что набор данных Elliptic является несбалансированным (4545 «незаконных» и 42019 «законных» транзакций). Поэтому следующей задачей было, не только найти значение для вышеперечисленных элементов транзакций, но и попытка определения транзакций как законной или незаконной для неизвестных транзакций.

*Для достижения поставленной цели был написан парсер для автоматического сбора данных на языке программирования «Python» для 200 тысяч биткойн транзакций путем обращения к платформам Crystal, и Blockchain, Датасет состоял из 207472 транзакций, из которых 107949 были помечены как неопределенные, 32938 помечены как подозрительные транзакций, а 66585 помечены как чистые транзакций. Было решено в наборе данных, который будет использован в обучении модели, убрать все неизвестные транзакций, после этого в датасете остались 99523 транзакций. Из них 32938 помечены как подозрительные, а 66585 помечены как чистые.*

В таблице 1 можно увидеть 15 ключевых признаков для последующего использования в алгоритмах для обучения модели, которая оценивает транзакции на предмет подозрительности.

Название атрибута	Тип данных	Описание
TRANSACTION	STRING	Уникальный идентификатор, используемый для идентификации конкретной транзакции
BLOCK_HASH	STRING	Хэш блока
BLOCK_HEIGHT	INTEGER	Высота блока
CONFIRMATIONS	INTEGER	Подтверждения транзакции в сети
COUNT_IN	INTEGER	Общее количество полученных транзакций
COUNT_OUT	INTEGER	Общее количество отправленных транзакций
FIAT RATE	FLOAT	Деньги в USD на момент транзакций
INPUTS	STRING	Адреса, отправившие BTC
OUTPUTS	STRING	Адреса, получившие BTC
POOL_TIME	TIMESTAMP	Время подтверждения транзакции
TOTAL_IN	NUMERIC	Общее количество отправленных BTC
TOTAL_OUT	NUMERIC	Общее количество полученных BTC
SIZE	INTEGER	Общий размер этой транзакции
WEIGHT	INTEGER	Вес этой транзакции
RISK_SCORE	BOOLEAN	Оценка транзакций на предмет подозрительности

### Результат

После подготовки датасета, следующим этапом стало обучение модели. Для обучения модели было использовано несколько алгоритмов машинного обучения, таких как случайный лес, деревья решений, логистическая регрессия. Разделение на обучающие и тестовые образцы основано на соотношении 80% к 20%. В результате для обучения было использовано 79 618 случайных элементов, а для теста — 19905.

В рисунке 5 был выбран алгоритм случайный лес. Случайный лес показывает очень хороший результат. Точность около 84 процентов. А в рисунке 6 деревья решения показывает хороший результат, но не как случайный лес. Точность модели составил 79%, что является хорошим результатом.

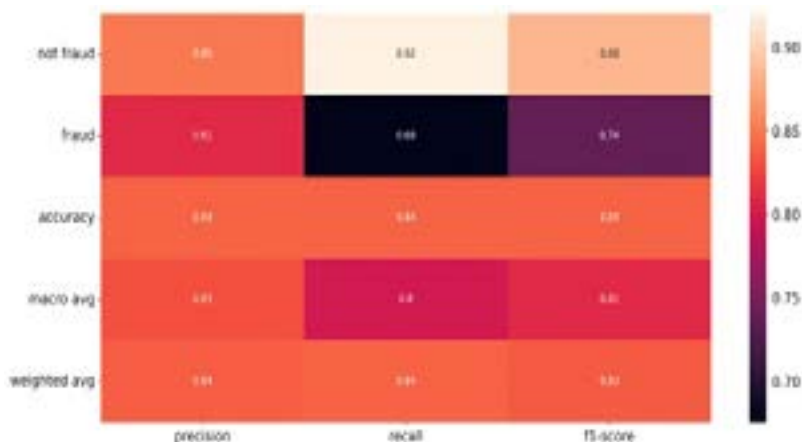


Рис.5 - Отчет о классификации для алгоритма случайного леса



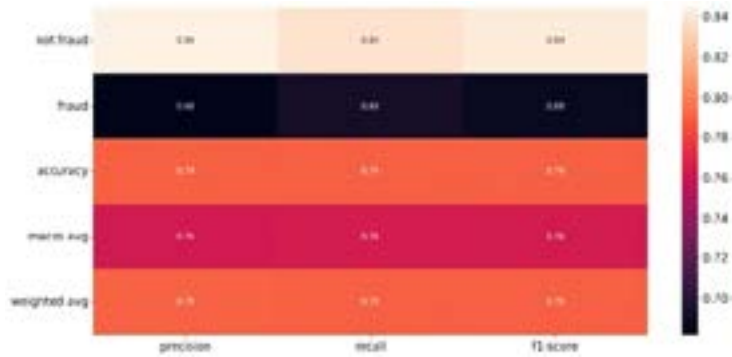


Рис. 6 - Отчет о классификации для алгоритма деревьев решений

Алгоритм k-ближайших соседей показывает наихудший результат среди функциональных алгоритмов, 71 процент также подходит для определения транзакции.

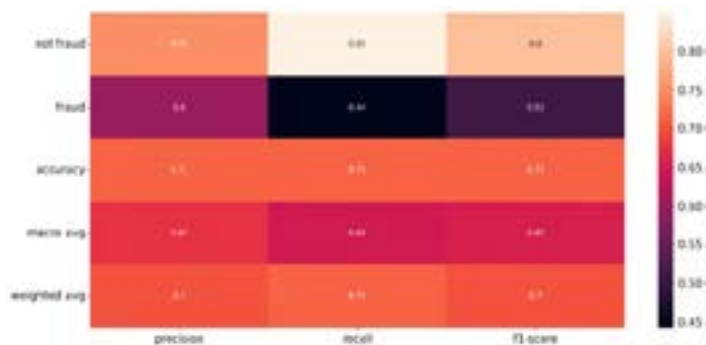


Рис. 7 - Отчет о классификации для алгоритма k-ближайших соседей

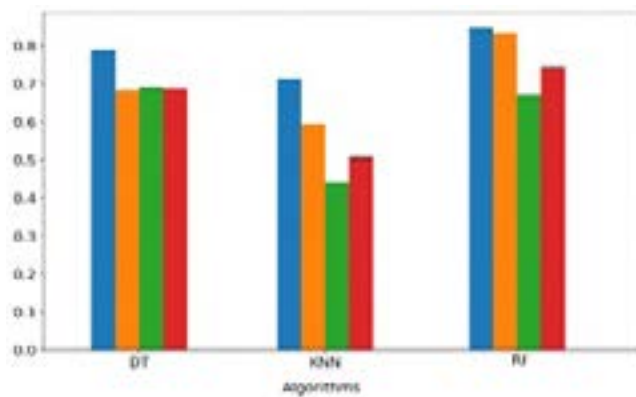


Рис. 8 - Сравнение алгоритмов

Таблица 2. Результаты и сравнение ключевых метрик.

№	Name	Accuracy	Precision	Recall	F1-score
1	DecisionTree	0.789249	0.681771	0.691323	0.686514
2	KNN	0.713618	0.595658	0.442302	0.507651
3	RandomForest	0.844966	0.833677	0.669027	0.742332

Как видно на рисунке 8 и в таблице 2, алгоритм «RandomForest» имеет лучшие показатели по всем метрикам по сравнению с остальными алгоритмами машинного обучения, кроме метрики «Recall», где лучше показатели у алгоритма «DecisionTree». Поэтому модель обученная на алгоритме случайного леса был выбран для дальнейшего использования.

### Обсуждение

На основе выявленных признаков был создан датасет содержащий около 5 тысяч незаконных транзакций путем изучения известных случаев, связанных с кражей биткойнов, отмытием биткойнов и т.д., чтобы избежать несбалансированности датасета. А также исследован набор данных «Elliptic DataSet». Путем объединения 2-х наборов данных был сформирован один основной датасет. Кроме этого, был написан парсер для автоматического сбора данных на языке программирования «Python» для 200 тысяч биткойн транзакций путем обращения к платформам Crystal и Blockchain. Созданы и обучены 3 модели для идентификаций транзакций на предмет подозрительности с использованием 3-х разных алгоритмов машинного обучения. Каждая из моделей обучалась примерно на почти 100 тысячах данных с 15 параметрами. В итоге была выбрана модель с самой высокой точностью, которая была построена на основе случайного леса и показала точность в 84%, что является хорошим результатом. В дальнейшем этот модель будет еще улучшаться и обучаться на более объемных датасетах. Будут исследоваться новые случаи, связанные с мошенническими и незаконными действиями пользователей, выявляться ранее неизвестные признаки подозрительных транзакций, а объем датасета будет увеличиваться.

### Заключение

В рамках проведенной работы были рассмотрены принципы и характеристики работы блокчейн технологий и биткойна, как они появляется, какими особенностями обладают, а также как они используются в преступных и незаконных целях. Кроме этого, были проанализированы множества литературы и научных статьи, выявлены и определены признаки (факты, кейсы), которые помогают при оценке Биткойн транзакции на предмет подозрительных или сомнительных операций. Был приведен практический пример анализа незаконных транзакции, создана модель для бинарной классификации нелегальных и легальных транзакций.

#### ЛИТЕРАТУРЫ

An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends [https://www.researchgate.net/publication/318131748\\_An\\_Overview\\_of\\_Blockchain\\_Technology\\_Architecture\\_Consensus\\_and\\_Future\\_Trends](https://www.researchgate.net/publication/318131748_An_Overview_of_Blockchain_Technology_Architecture_Consensus_and_Future_Trends).

Ajello N., 2015 — *Ajello N.* Fitting a Square Peg in a Round Hole: Bitcoin, Money Laundering, and the Fifth Amendment Privilege Against Self-Incrimination // *Brooklyn Law Review*. 2015. Volume 80. Issue 2.

Chuen D.L., 2015 — *Chuen D.L.* Handbook of Digital Currency. Bitcoin, Innovation, Financial instruments, And Big Data. USA, Academic Press, 2015.

Crypto Firms Can't Outrun the Travel Rule. <https://www.coindesk.com/layer2/2022/01/12/crypto-firms-cant-outrun-the-travel-rule/> (дата обращения: 06.10.2022).

Condos J., Sorrel W.H. & Donegan S.L., 2016 — *Condos J., Sorrel W.H. & Donegan S.L.* Blockchain Opportunities. Vermont. Retrieved from <https://legislature.vermont.gov/assets/Legislative-Reports/blockchain-technology-report-final.pdf>

Elliptic Data Set. Bitcoin Transaction Graph. <https://www.kaggle.com/ellipticco/elliptic-data-set> (дата обращения: 06.10.2022).

Nakamoto S., 2022 — *Nakamoto S.* Bitcoin: A Peer-to-Peer Electronic Cash System. <http://bitcoin.org/bitcoin.pdf> (дата обращения: 05.09.2022).

Взломали биржу Zaif. <https://incrypted.com/exchange-zaif-was-hacked/> (дата обращения: 23.09.2022).

Как отслеживаются транзакции в сети биткоина? <https://forklog.com/cryptorium/kak-otslezhivayutsya-tranzaksii-v-seti-bitkoina/> (дата обращения: 07.09.2022).

Как проверить и отследить транзакцию в сети биткоин <https://finswin.com/kripto/btc/tranzakcii-bitcoin.html>

Как осуществляются биткойн-транзакции <https://www.bitcoin.com/ru/get-started/how-bitcoin-transactions-work/> Ларин Д. С.Возможность использования биткоинов в отмывании денег. 2018, ГРНТИ 06.73.02

Салах К., Рехман М., Низамуддин Н., Аль-Фукаха А., 2019 — *Салах К., Рехман М., Низамуддин Н., Аль-Фукаха А.* Блокчейн для ИИ: обзор и открытые исследовательские задачи. *IEEE Access* 2019, 7. 10127–10149.

Что такое криптовалюта и как она применяется? <https://www.kaspersky.ru/resource-center/definitions/what-is-cryptocurrency> (дата обращения: 05.09.2022).

Что такое биткоин и как он работает? <https://forklog.com/cryptorium/chto-takoe-bitcoin> (дата обращения: 09.09.2022).

Что такое Биткоин транзакции: Как проверить транзакцию биткоин? <https://phemex.com/ru/academy/what-is-bitcoin-transaction>.

Что такое Блокчейн (Blockchain)? Технология распределенного реестра простыми словами. <https://www.seeneco.com/ru/blog/chto-takoe-blokchejn> (дата обращения: 11.09.2022).

Что такое Биткоин транзакции: как проверить транзакцию биткоин? <https://phemex.com/ru/academy/what-is-bitcoin-transaction/>(дата обращения: 27.09.2022).

#### REFERENCE

An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends [https://www.researchgate.net/publication/318131748\\_An\\_Overview\\_of\\_Blockchain\\_Technology\\_Architecture\\_Consensus\\_and\\_Future\\_Trends](https://www.researchgate.net/publication/318131748_An_Overview_of_Blockchain_Technology_Architecture_Consensus_and_Future_Trends).

Ajello N., 2015 — *Ajello N.* Fitting a Square Peg in a Round Hole: Bitcoin, Money Laundering, and the Fifth Amendment Privilege Against Self-Incrimination // *Brooklyn Law Review*. 2015. Volume 80. Issue 2.

Chuen D.L., 2015 — *Chuen D.L.* Handbook of Digital Currency. Bitcoin, Innovation, Financial instruments, And Big Data. USA, Academic Press, 2015.

Crypto Firms Can't Outrun the Travel Rule. <https://www.coindesk.com/layer2/2022/01/12/crypto-firms-cant-outrun-the-travel-rule/> (date of application: 06.10.2022).

Condos J., Sorrel W.H. & Donegan S.L., 2016 — *Condos J., Sorrel W.H. & Donegan S.L. Blockchain Opportunities*. Vermont. Retrieved from <https://legislature.vermont.gov/assets/Legislative-Reports/blockchain-technology-report-final.pdf>

Elliptic Data Set. Bitcoin Transaction Graph. <https://www.kaggle.com/ellipticco/elliptic-data-set> (date of application: 06.10.2022).

How are transactions tracked on the Bitcoin network? <https://forklog.com/cryptorium/kak-otslezhivayutsya-tranzaktsii-v-seti-bitkoina/> (date of application:07.09.2022).

How to check and track a transaction on the Bitcoin network. <https://finswin.com/kripto/btc/tranzakcii-bitkoin.html> (date of application:10.10.2022).

How are Bitcoin transactions carried out? <https://www.bitcoin.com/ru/get-started/how-bitcoin-transactions-work/> (date of application:10.10.2022).

Larin D.S., 2018 — *Larin D.S. The possibility of using bitcoins in money laundering*. 2018. GRNTI 06.73.02

Nakamoto S., 2022 — *Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System*. <http://bitcoin.org/bitcoin.pdf> (date of application:05.09.2022).

The Zaif exchange was hacked. <https://incrypted.com/exchange-zaif-was-hacked/> (date of application: 23.09.2022).

Salah K., Rehman M., Nizamuddin N., Al-Fuqaha A., 2019 — *Salah K., Rehman M., Nizamuddin N., Al-Fuqaha A. Blockchain for AI: Review and Open Research Tasks*. IEEE Access 2019, 7. 10127–10149.

What is cryptocurrency and how is it applied? <https://www.kaspersky.ru/resource-center/definitions/what-is-cryptocurrency> (date of application:05.09.2022).

What is Bitcoin and how does it work? <https://forklog.com/cryptorium/chto-takoe-bitkoin> (date of application: 09.09.2022).

What are Bitcoin Transactions?: How to verify a Bitcoin transaction? <https://phemex.com/ru/academy/what-is-bitcoin-transaction> (date of application: 27.09.2022).

What is Blockchain? Distributed registry technology in simple words. <https://www.seeneco.com/ru/blog/chto-takoe-blokchein> (date of application:11.09.2022).

What are Bitcoin Transactions: How to verify a Bitcoin transaction? <https://phemex.com/ru/academy/what-is-bitcoin-transaction/>(date of application:27.09.2022).

## 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 МЕДИАРИПЕ ЖӘНЕ SVM АРҚЫЛЫ ҚАЗАҚ ҰМ 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. Tokkuliyeva</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.