

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

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ҰЛТТЫҚ ҒЫЛЫМ АКАДЕМИЯСЫНЫҢ
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 университетінің

NEWS

OF THE NATIONAL ACADEMY OF SCIENCES
OF THE REPUBLIC OF KAZAKHSTAN
Al-Farabi Kazakh
National University

**SERIES
PHYSICO-MATHEMATICAL**

2(330)

MARCH – APRIL 2020

PUBLISHED SINCE JANUARY 1963

PUBLISHED 6 TIMES A YEAR

ALMATY, NAS RK

Б а с р е д а к т о р ы
ф.-м.ғ.д., проф., ҚР ҰҒА академигі
Ғ.М. Мұтанов

Р е д а к ц и я а л қ а с ы:

Жұмаділдаев А.С. проф., академик (Қазақстан)
Кальменов Т.Ш. проф., академик (Қазақстан)
Жантаев Ж.Ш. проф., корр.-мүшесі (Қазақстан)
Өмірбаев У.У. проф., корр.-мүшесі (Қазақстан)
Жүсіпов М.А. проф. (Қазақстан)
Жұмабаев Д.С. проф. (Қазақстан)
Асанова А.Т. проф. (Қазақстан)
Бошкаев К.А. PhD докторы (Қазақстан)
Сұраған Д. корр.-мүшесі (Қазақстан)
Quevedo Hernando проф. (Мексика),
Джунушалиев В.Д. проф. (Қырғыстан)
Вишневский И.Н. проф., академик (Украина)
Ковалев А.М. проф., академик (Украина)
Михалевич А.А. проф., академик (Белорусь)
Пашаев А. проф., академик (Әзірбайжан)
Такибаев Н.Ж. проф., академик (Қазақстан), бас ред. орынбасары
Тигиняну И. проф., академик (Молдова)

«ҚР ҰҒА Хабарлары. Физика-математикалық сериясы».

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

Меншіктенуші: «Қазақстан Республикасының Ұлттық ғылым академиясы» РҚБ (Алматы қ.).

Қазақстан республикасының Мәдениет пен ақпарат министрлігінің Ақпарат және мұрағат комитетінде
01.06.2006 ж. берілген №5543-Ж мерзімдік басылым тіркеуіне қойылу туралы куәлік.

Мерзімділігі: жылына 6 рет.

Тиражы: 300 дана.

Редакцияның мекенжайы: 050010, Алматы қ., Шевченко көш., 28; 219, 220 бөл.; тел.: 272-13-19; 272-13-18,
<http://physics-mathematics.kz/index.php/en/archive>

© Қазақстан Республикасының Ұлттық ғылым академиясы, 2020

Типографияның мекенжайы: «NurNaz GRACE», Алматы қ., Рысқұлов көш., 103.

Главный редактор
д.ф.-м.н., проф. академик НАН РК
Г.М. Мутанов

Редакционная коллегия:

Джумадильдаев А.С. проф., академик (Казахстан)
Кальменов Т.Ш. проф., академик (Казахстан)
Жангаев Ж.Ш. проф., чл.-корр. (Казахстан)
Умирбаев У.У. проф., чл.-корр. (Казахстан)
Жусупов М.А. проф. (Казахстан)
Джумабаев Д.С. проф. (Казахстан)
Асанова А.Т. проф. (Казахстан)
Бошкаев К.А. доктор PhD (Казахстан)
Сураган Д. чл.-корр. (Казахстан)
Quevedo Hernando проф. (Мексика),
Джунушалиев В.Д. проф. (Кыргызстан)
Вишневский И.Н. проф., академик (Украина)
Ковалев А.М. проф., академик (Украина)
Михалевич А.А. проф., академик (Беларусь)
Пашаев А. проф., академик (Азербайджан)
Такибаев Н.Ж. проф., академик (Казахстан), зам. гл. ред.
Тигиняну И. проф., академик (Молдова)

«Известия НАН РК. Серия физика-математическая».

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

Собственник: РОО «Национальная академия наук Республики Казахстан» (г. Алматы).

Свидетельство о постановке на учет периодического печатного издания в Комитете информации и архивов
Министерства культуры и информации Республики Казахстан №5543-Ж, выданное 01.06.2006 г.

Периодичность: 6 раз в год.

Тираж: 300 экземпляров.

Адрес редакции: 050010, г. Алматы, ул. Шевченко, 28; ком. 219, 220; тел.: 272-13-19; 272-13-18,

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

© Национальная академия наук Республики Казахстан, 2020

Адрес типографии: «NurNaz GRACE», г. Алматы, ул. Рыскулова, 103.

Editor in chief

doctor of physics and mathematics, professor, academician of NAS RK

G.M. Mutanov

Editorial board:

Dzhumadildayev A.S. prof., academician (Kazakhstan)
Kalmenov T.Sh. prof., academician (Kazakhstan)
Zhantayev Zh.Sh. prof., corr. member. (Kazakhstan)
Umirbayev U.U. prof., corr. member. (Kazakhstan)
Zhusupov M.A. prof. (Kazakhstan)
Dzhumabayev D.S. prof. (Kazakhstan)
Asanova A.T. prof. (Kazakhstan)
Boshkayev K.A. PhD (Kazakhstan)
Suragan D. corr. member. (Kazakhstan)
Quevedo Hernando prof. (Mexico),
Dzhunushaliyev V.D. prof. (Kyrgyzstan)
Vishnevskiy I.N. prof., academician (Ukraine)
Kovalev A.M. prof., academician (Ukraine)
Mikhalevich A.A. prof., academician (Belarus)
Pashayev A. prof., academician (Azerbaijan)
Takibayev N.Zh. prof., academician (Kazakhstan), deputy editor in chief.
Tiginyanu I. prof., academician (Moldova)

News of the National Academy of Sciences of the Republic of Kazakhstan. Physical-mathematical series.

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 periodic printed publication in the Committee of information and archives of the Ministry of culture and information of the Republic of Kazakhstan N 5543-Ж, issued 01.06.2006.

Periodicity: 6 times a year.

Circulation: 300 copies.

Editorial address: 28, Shevchenko str., of. 219, 220, Almaty, 050010, tel. 272-13-19; 272-13-18,

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

© National Academy of Sciences of the Republic of Kazakhstan, 2020

Address of printing house: «NurNaz GRACE», 103, Ryskulov str, Almaty.

NEWS

OF THE NATIONAL ACADEMY OF SCIENCES OF THE REPUBLIC OF KAZAKHSTAN
PHYSICO-MATHEMATICAL SERIES

ISSN 1991-346X

<https://doi.org/10.32014/2020.2518-1726.17>

Volume 2, Number 330 (2020), 75 – 79

УДК 621.391.26

M. Amreyev, B. Yakubov, R. Safin, M. Yakubova

Almaty University of Power Engineering and Telecommunication, Almaty, Kazakhstan.
E-mail: max.amreev@gmail.com, 1968ybm@mail.ru, raf.safin@mail.ru, mubor194@gmail.com

**IMPROVING THE QUALITY AND RELIABILITY OF SIGNAL
TRANSMISSION AND RECEPTION IN MULTISERVICE NETWORKS»»**

Abstract. This article describes the entire complete cycle of signal transmission and reception from the terminal device on the transmitting side to the terminal device on the receiving side, due to the fact that the reliability and quality of information transmission and reception in public access networks depend on many different parameters. The article describes the process of converting a signal from an analog form to a digital one. For this purpose, the so-called encoding of the graphic signal is used. To get a rich palette of colors, different intensities were set for the base colors. During the experiment, an IP video camera was used and digital traffic was prepared to transmit it over multiservice or open networks. The Novus IP video camera uses a web interface. During the initial installation, in order to access the camera interface, you must assign an IP address, subnet mask, and Ethernet adapter gateway to the PC. To ensure greater protection of information, it is necessary to apply encryption, which will increase the reliability of the process of transmitting and receiving information. Today, cryptography is one of the most used ways to ensure the confidentiality and authenticity of information. There are symmetric and asymmetric cryptosystems. In the symmetric encryption process, the same key is used for both encryption and decryption. Asymmetric systems use public and private keys that are mathematically related to each other. The DHCP-installer program was used and the distribution of IP addresses was obtained by agreeing to its terms. First, you need to configure the DHCP server. The DHCP Protocol is commonly used in most cases used in TCP/IP networks. In addition to the IP address, DHCP can also tell the client additional parameters that are necessary for normal network operation and these are called DHCP options. Today, there is a modern and high-speed Wi-Fi router that supports the wireless communication standard 802.11 a/b/g/n/ac. The router, in turn, transmits private information through any built-in interfaces. After high-speed transmission of traffic, the receiving side must perform the reverse encryption procedure-decryption, in order to get the original signal. As a result of the experiment on the equipment, we come to the conclusion that the studied parameters such as reliability, quality and secrecy of the transmitted information depend on the technical characteristics of the real equipment that was used in the experiment.

Key words: signal, IP-video camera, format, encryption, decryption, broadcast, receiving, quality, reliability, traffic.

Today, the reliability and quality of data transmission and reception in public access networks depend on many different parameters such as:

- 1) The operation of routers.
- 2) The quality of converting the source signal from one format to another (for example, digitization in IP cameras, etc.).
- 3) The use of various types of hiding information itself (for example, encryption).
- 4) Network service quality.

It means that the relevance of this task is undeniable. This article will cover the entire complete cycle of signal transmission and reception, starting from the terminal device on the transmitting side to the terminal device on the receiving side.

At the beginning, the process of converting a signal from an analog form to a digital one will be briefly considered. For this purpose, we will use the so-called encoding of the graphic signal. The screen resolution and color depth determines image quality. The number of colors (K) displayed on the display screen depends on the number of bits (N) allocated in video memory for each pixel:

$$K=2^N. \tag{1}$$

Where N is the value of the bit depth.

To achieve a intense palette of colors, the base colors can be set to different intensities. For instance, if the color depth is 24 bits, 8 bits (RGB) are allocated for each color, i.e. $K = 2^8 = 256$ intensity levels are possible for each color. One bit of video memory is occupied by information about one pixel on a black-and-white screen (without halftones). Figure 1 depicts an example of this transformation [1, 3].

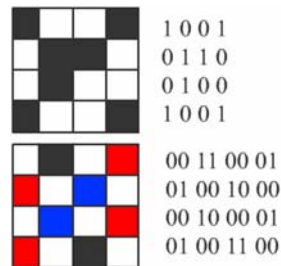


Figure 1 - Example of converting pixels (image points) to a bit sequence

For the experiment, an IP video camera "NOVUS NVIP-TC2400D / MPX1. 3-II" was used, which was installed on a laboratory stand designed for the study and research of analogue CCTV systems, on the left end wall of the laboratory table № 1 (figure 2) [2].



Figure 2 - Appearance of the laboratory table №1

The Novus IP video camera uses a web interface. During the initial installation, in order to access the camera interface, IP address, subnet mask, and Ethernet adapter gateway to the PC have to be assigned. In the address bar of the Internet browser, select the IP address: IP-адрес: 192.168.0.83.

Subnet mask: 255.255.255.0
 sluice: 192.168.0.200

After all the pre-settings described above on endpoints such as IP video cameras, digital traffic was prepared for transmission over multiservice or open networks. To better protect information, you can now use encryption, which will increase the reliability of the process of transmitting and receiving information.

Today, cryptography is one of the most used ways to ensure the confidentiality and authenticity of information. There are symmetric and asymmetric cryptosystems.

In the symmetric encryption process, the same key is used for both encryption and decryption.

Asymmetric systems use public and private keys that are mathematically related to each other. Information is encrypted using a public key that is shared, and decrypted using a private key that is known only to the recipient of the message.

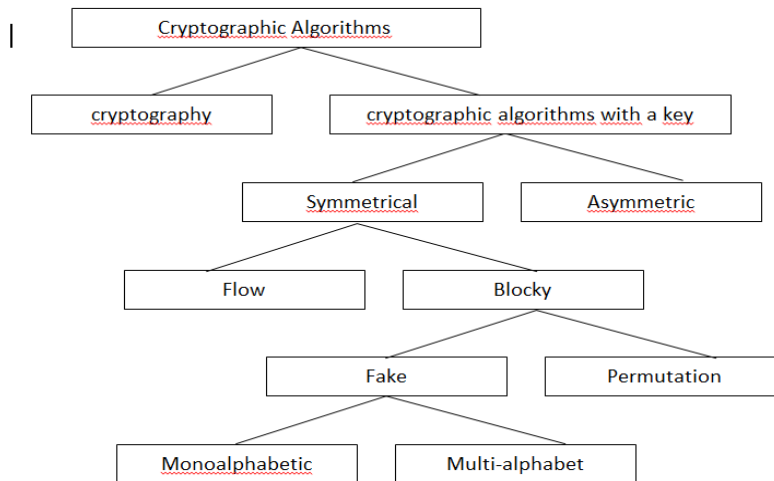


Figure 3 – General classification of cryptographic algorithms

After selecting and applying the encryption algorithm, the traffic is ready to transfer the already encrypted information over the communication channels. To do this, let's briefly consider how packet traffic is transmitted and received over communication networks [4].

First, it is needed to configure the Dhcp server. The Dhcp Protocol is commonly used in most cases used in TCP/IP networks.

In addition to the IP address, Dhcp can also tell the client additional parameters that are necessary for normal network operation and these are called Dhcp options.

There are the most frequently used options:

- The IP address of the default router;
- Subnet mask;
- DNS server address and
- DNS domain name.

Running the dhcp-installer program and agreeing to its terms, we get the distribution of IP addresses, which is shown in figure 4.

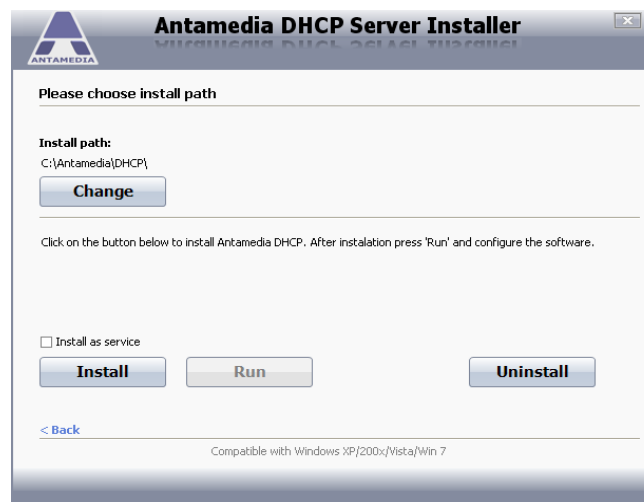


Figure 4 - Antamedia DHCP Server Installer window

Now the original signal is completely ready for transmission to the router, which in turn will transmit the closed information via any interfaces built into it, such as fiber, twisted pair or Wi-Fi, to the communication channels (figure 5) [5].



Figure 5 -ASUS RT-AC52U B1 router

Today, there are modern and high-speed Wi-Fi router which supports wireless standards 802.11 a/b/g/n/ac, and can operate in 2 frequency bands such as 2.4 GHz and 5 GHz. Therefore, there is a possibility of traffic with high speed is 733 Mbit/s, which will significantly affect the figure as processing time and packet delay, in addition to Wi-Fi interface it enables connection of copper source and optical fiber [5].

After the high-speed traffic on the receiver side, it was necessary to carry out the opposite procedure of encryption – decryption, in order to obtain the original signal. In this case, the IP video image.

Conclusion. After conducting an experiment on the equipment, it can be seen that the studied parameters such as reliability, quality and secrecy of the transmitted information depend on the technical characteristics of the real equipment that was used in the experiment and the use of an encryption system that generally improves the quality of service in multi-service public access networks.

М. Амреев, Б. Якубов, К. Сафин, М. Якубова

Ғұмарбек Даукеев атындағы Алматы энергетика және байланыс университеті, Алматы, Қазақстан

МУЛЬТИСЕРВИСТІК ЖЕЛІДЕ ТАРАТУ ЖӘНЕ ҚАБЫЛДАУ КЕЗІНДЕ СИГНАЛДЫҢ САПАСЫ МЕН СЕНІМДІЛІГІН АРТТЫРУ

Аннотация. Бұл мақалада тарату мен қабылдаудың барлық аяқталған циклі қарастырылады, таратушы жақтан терминалды құрылғыдан қабылдау жағындағы терминалды құрылғыға, өйткені ақпараттың сенімділігі мен сапасы көпшілікке арналған желілерде әртүрлі параметрлерге байланысты болады. Мақалада сигналды аналогтық форматтан сандық түрге түрлендіру процесі сипатталған. Ол үшін графикалық сигналды кодтау деп аталатын әдіс қолданылады. Түстердің бай палитрасын алу үшін негізгі түстерге әр түрлі қарқындылық берілді. Тәжірибе барысында IP бейнекамерасы қолданылды және сандық трафик мультисервистік немесе ашық желілер арқылы берілуге дайындалған. Novus IP бейнекамерасы веб-интерфейсті қолданады. Алғашқы орнатудан кейін камераның интерфейсіне кіру үшін компьютерге IP мекенжайын, ішкі желі маскасын және Ethernet адаптерінің шлюзін тағайындау керек. Ақпараттың үлкен қорғалуын қамтамасыз ету үшін ақпаратты беру және қабылдау процесінде сенімділікті арттыратын шифрлауды қолдану қажет. Бүгінгі таңда криптография ақпараттың құпиялылығы мен шынайылығын қамтамасыз етудің ең көп қолданылатын әдістерінің бірі болып табылады. Симметриялық және асимметриялық криптожүйелер бар. Симметриялық шифрлау процесінде бірдей кілт шифрлау үшін де, шифрлау үшін де қолданылады. Асимметриялық жүйелерде бір-бірімен математикалық байланысқан ашық және жеке кілттер қолданылады. DHCP-installer бағдарламасы қолданылды және оның шарттарына сәйкес IP адресстердің таралуы алынды. Алдымен сіз DHCP серверін конфигурациялауыңыз керек. DHCP көбінесе TCP / IP желілерінде қолданылады. IP мекенжайынан басқа, DHCP клиентке желіде қалыпты жұмыс істеу үшін қажет болатын қосымша параметрлерді айта алады және оларды Dhcp опциялары деп атайды. Бүгінгі таңда 802.11a / b / g / n / ac сымсыз байланыс стандартын қолдайтын заманауи және жоғары жылдамдықты Wi-Fi маршрутизаторы бар. Маршрутизатор өз кезегінде жабық ақпаратты оған салынған кез-келген интерфейс арқылы жібереді. Трафикті жоғары жылдамдықпен бергеннен кейін, қабылдаушы жағында бастапқы сигналды алу үшін кері шифрлау процедурасын орындау керек - шифрлау. Жабдықта жүргізілген эксперимент нәтижесінде алынған мәліметтердің сенімділігі, сапасы және құпиясы сияқты зерттелген параметрлер экспериментте қолданылған нақты жабдықтың техникалық сипаттамаларына байланысты деп тұжырымдаймыз.

Түйін сөз: сигнал, IP-бейнекамера, формат, шифрлау, тарату, кабылдау, сапа, сенімділік, трафик.

М. Амреев, Б. Якубов, К. Сафин, М. Якубова

Алматинский университет энергетики и связи имени Гумарбека Даукеева, Алматы, Казахстан

УЛУЧШЕНИЕ КАЧЕСТВА И НАДЕЖНОСТИ СИГНАЛА ПРИ ПЕРЕДАЧЕ И ПРИЕМЕ В МУЛЬТИСЕРВИСНЫХ СЕТЯХ

Аннотация. В данной статье рассмотрен весь законченный цикл по передаче и приему сигнала, начиная от оконечного устройства с передающей стороны до оконечного устройства на приемной стороне, в связи с тем, что надежность и качество при передаче и приеме информации в сетях общего доступа зависят от множества различных параметров. Описан процесс преобразования сигнала с аналоговой формы в цифровую. Для этого использовано так называемое кодирование графического сигнала. Для получения богатой палитры цветов базовым цветам были заданы различные интенсивности. При проведении эксперимента использовалась IP-видеокамера и был подготовлен цифровой трафик для передачи его по мультисервисным или открытым сетям. Для использования IP-видеокамеры Novus используется веб-интерфейс. При первоначальной установке, для того чтобы получить доступ к интерфейсу камеры, необходимо назначить IP-адрес, маску подсети и шлюз Ethernet-адаптера на ПК. Для большего обеспечения защиты информации необходимо применить шифрование, что повысит надежность при самом процессе передачи-приема информации. На сегодняшний день криптография является одним из наиболее используемых способов обеспечения конфиденциальности и подлинности информации. Существуют симметричные и асимметричные криптосистемы. В процессе симметричного шифрования и для шифрования, и для дешифрования используется один и тот же ключ. В асимметричных системах используются открытый и закрытый ключи, связанные друг с другом математически. Использовалась программа DHCP-installer и, соглашаясь с ее условиями, была получена раздача IP – адресов. Вначале надо настроить DHCP-сервер. Протокол DHCP является часто используемым в большинстве случаев используемым в сетях TCP/IP. Кроме IP-адреса, DHCP также может сообщить клиенту дополнительные параметры, которые необходимы для нормальной работы в сети и они называются опциями DHCP. На сегодняшний день имеется современный и скоростной Wi-Fi роутер, который поддерживает стандарт беспроводной связи 802.11a/b/g/n/ac. Маршрутизатор в свою очередь передает закрытую информацию через любые встроенные в нем интерфейсы. После высокоскоростной передачи трафика, на приемной стороне необходимо провести обратную процедуру шифрованию – дешифрование, для того что бы получить исходный сигнал. В результате проведения эксперимента на оборудовании, приходим к заключению, что исследуемые параметры, такие как надежность, качество и скрытость передаваемой информации зависят от технических характеристик реального оборудования, которое было использовано в эксперименте.

Ключевые слова: сигнал, IP-видеокамера, формат, шифрование, дешифрование, трансляция, прием, качество, надежность, трафик.

Information about authors:

Amreyev M. B., doctor's degree, Almaty University of Power Engineering and Telecommunication, email: max.amreev@gmail.com, <https://orcid.org/0000-0002-4874-1161>;

Yakubov B. M., doctor's degree, Almaty University of Power Engineering and Telecommunication, email: 1968ybm@mail.ru, <https://orcid.org/0000-0002-1297-705X>;

Safin R. T., Senior lecturer of the Department «TCSS», Almaty University of Power Engineering and Telecommunication, email: raf.safin@mail.ru, <https://orcid.org/0000-0003-1583-0034>;

Yakubova M.Z., Ph.D. professor of department «TCSS», Almaty University of Power Engineering and Telecommunication, email: mubor194@gmail.com, <https://orcid.org/0000-0001-7665-5976>

REFERENCES

- [1] Sergienko A.B. Digital signal processing. SPbu. 202-608 p.
- [2] Artyukhin V.V., Artyukhin A.V. Digital television, radio broadcasting and video surveillance systems. «AUPET». Almaty, 2011. 32 p.
- [3] Novakovski S.V. Digital television. M. ECO -Trends, 2008. 375 p.
- [4] Ryabko B.Y., Fionov A.N. Fundamentals of modern cryptography for information technology professionals. M. Science world, 2004. 170 p.
- [5] Olipher B., Olipher N. «Computer network. Principles, technologies, and protocols» (5th edition). 2016. 992p.

Publication Ethics and Publication Malpractice in 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). 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)

Редакторы: *М. С. Ахметова, Г. Б. Халидуллаева, Д. С. Аленов*
Верстка на компьютере *А.М. Кульгинбаевой*

Подписано в печать 05.04.2020.

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

11 п.л. Тираж 300. Заказ 2.

Национальная академия наук РК
050010, Алматы, ул. Шевченко, 28, т. 272-13-18, 272-13-19