ISSN 2518-170X (Online),
ISSN 2224-5278 (Print)

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ҰЛТТЫҚ ҒЫЛЫМ АКАДЕМИЯСЫ
Satbayev University

ХАБАРЛАРЫ

ИЗВЕСТИЯ

НАЦИОНАЛЬНОЙ АКАДЕМИИ НАУК
РЕСПУБЛИКИ КАЗАХСТАН
Satbayev University

N E W S

OF THE ACADEMY OF SCIENCES
OF THE REPUBLIC OF KAZAKHSTAN
Satbayev University

SERIES
OF GEOLOGY AND TECHNICAL SCIENCES

3 (447)

MAY – JUNE 2021

THE JOURNAL WAS FOUNDED IN 1940

PUBLISHED 6 TIMES A YEAR

ALMATY, NAS RK

NAS RK is pleased to announce that News of NAS RK. Series of geology and technical sciences scientific journal has been accepted for indexing in the Emerging Sources Citation Index, a new edition of Web of Science. Content in this index is under consideration by Clarivate Analytics to be accepted in the Science Citation Index Expanded, the Social Sciences Citation Index, and the Arts & Humanities Citation Index. The quality and depth of content Web of Science offers to researchers, authors, publishers, and institutions sets it apart from other research databases. The inclusion of News of NAS RK. Series of geology and technical sciences in the Emerging Sources Citation Index demonstrates our dedication to providing the most relevant and influential content of geology and engineering sciences to our community.

Қазақстан Республикасы Ұлттық ғылым академиясы «ҚР ҰҒА Хабарлары. Геология және техникалық ғылымдар сериясы» ғылыми журналының Web of Science-тің жаңаланған нұсқасы Emerging Sources Citation Index-те индекстелуге қабылданғанын хабарлайды. Бұл индекстелу барысында Clarivate Analytics компаниясы журналды одан әрі the Science Citation Index Expanded, the Social Sciences Citation Index және the Arts & Humanities Citation Index-ке қабылдау мәселесін қарастыруда. Webof Science зерттеушілер, авторлар, баспашылар мен мекемелерге контент тереңдігі мен сапасын ұсынады. ҚР ҰҒА Хабарлары. Геология және техникалық ғылымдар сериясы Emerging Sources Citation Index-ке енуі біздің қоғамдастық үшін ең өзекті және беделді геология және техникалық ғылымдар бойынша контентке адалдығымызды білдіреді.

НАН РК сообщает, что научный журнал «Известия НАН РК. Серия геологии и технических наук» был принят для индексирования в Emerging Sources Citation Index, обновленной версии Web of Science. Содержание в этом индексировании находится в стадии рассмотрения компанией Clarivate Analytics для дальнейшего принятия журнала в the Science Citation Index Expanded, the Social Sciences Citation Index и the Arts & Humanities Citation Index. Web of Science предлагает качество и глубину контента для исследователей, авторов, издателей и учреждений. Включение Известия НАН РК. Серия геологии и технических наук в Emerging Sources Citation Index демонстрирует нашу приверженность к наиболее актуальному и влиятельному контенту по геологии и техническим наукам для нашего сообщества.

«ҚР ҰҒА Хабарлары. Геология және техникалық ғылымдар сериясы».
ISSN 2518-170X (Online),
ISSN 2224-5278 (Print)
Меншіктенуші: «Қазақстан Республикасының Ұлттық ғылым академиясы» РҚБ (Алматы қ.).
Қазақстан Республикасының Ақпарат және қоғамдық даму министрлігінің Ақпарат комитетінде 29.07.2020 ж. берілген **№ KZ39VPY00025420** мерзімдік басылым тіркеуіне қойылу туралы куәлік.
Тақырыптық бағыты: *геология және техникалық ғылымдар бойынша мақалалар жариялау.*
Мерзімділігі: жылына 6 рет.
Тиражы: 211 дана.
Редакцияның мекен-жайы: 050010, Алматы қ., Шевченко көш., 28, 219 бөл., тел.: 272-13-19, 272-13-18
http://www.geolog-technical.kz/index.php/en/

Типографияның мекен-жайы: «Аруна» ЖК, Алматы қ., Муратбаева көш., 75.

«Известия НАН РК. Серия геологии и технических наук».
ISSN 2518-170X (Online),
ISSN 2224-5278 (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 **№ KZ39VPY00025420,** выданное 29.07.2020 г.
Тематическая направленность: *публикация статей по геологии и техническим наукам.*
Периодичность: 6 раз в год.
Тираж: 211 экземпляров.
Адрес редакции: 050010, г. Алматы, ул. Шевченко, 28, оф. 219, тел.: 272-13-19, 272-13-18
http://www.geolog-technical.kz/index.php/en/

Адрес типографии: ИП «Аруна», г. Алматы, ул. Муратбаева, 75.

News of the National Academy of Sciences of the Republic of Kazakhstan. Series of geology and technology sciences.
ISSN 2518-170X (Online),
ISSN 2224-5278 (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. KZ39VPY00025420,** issued 29.07.2020.
Thematic scope: *publication of papers on geology and technical sciences.*
Periodicity: 6 times a year.
Circulation: 211 copies.
Editorial address: 28, Shevchenko str., of. 219, Almaty, 050010, tel. 272-13-19, 272-13-18, http://www.geolog-technical.kz/index.php/en/

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

I**NEWS**
OF THE NATIONAL ACADEMY OF SCIENCES OF THE REPUBLIC OF
KAZAKHSTAN **SERIES OF GEOLOGY AND TECHNICAL SCIENCES**
ISSN 2224-5278
Volume 3, Number 447 (2021), 100-103 **https://doi.org/10.32014/2021.2518-170X.69**

SSN 2224-5278
UDC 621.395.019
IRSTI 47.00.00

M.A. Khizirova[1], K.S. Chezhimbayeva[1], A.D. Mukhamejanova[1], Zh.D. Manbetova[1], B. Ongar[2]
[1]Almaty University of Power Engineering and Telecommunications named after Gumarbek Daukeev, Almaty, Kazakhstan.
[2]Logistics and Transport Academy, Almaty, Kazakhstan.
E-mail: hizirova73@mail.ru

USING OF VIRTUAL PRIVATE NETWORK TECHNOLOGY FOR SIGNAL TRANSMISSION IN CORPORATE NETWORKS

Abstract. This paper discusses some modes of signal transmission for corporate systems using the technology of virtual private networks VPN. A very important property of tunnels is the ability to differentiate different types of traffic and assign them the necessary service priorities. In this work, research has been carried out and comparative characteristics of signal transmission modes using virtual networks have been obtained to identify the effectiveness of the network in various modes of organizing a virtual network, and to optimize a virtual network in order to identify an effective method for organizing a VPN. Also, the work analyzes the specifics of the work of corporate information systems and networks intended for their maintenance, showed that for building a corporate network it is advisable to use virtual private network (VPN) technology, which makes it possible to ensure the fulfillment of the basic requirements for the security and quality of customer service and applications and the current state and direction of development of VPN technology when creating new generation corporate networks, while highlighting the main tasks that need to be addressed when creating a network. Some features of setting up an IPSec VPN server for corporate networks are considered.

Key words: corporate networks, VPN (Virtual Private Network), tunneling, traffic, point-to-point connection, server, router

Introduction. The transmission of corporate data over a public network such as Internet is often a threat to the security of an enterprise network, which is especially important for corporate systems. In addition, for corporate networks, the quality of user service, the provision of a given set of services and guarantees, which is not always easy to provide in public networks, are important.

To solve these problems, the technology of virtual private networks VPN (Virtual Private Network) can be used. This technology transforms connections in public packet networks into secure channels with guaranteed bandwidth, providing security and a wide range of services at an acceptable cost of the established connections. Therefore, this technology is in demand by many enterprises and organizations that do not have their own network resources, primarily corporate organizations due to its cost-effectiveness, availability and security.

The relevance of this issue lies in the peculiarities of large geographically distributed corporate networks: in the use of global connections and the integration of individual local networks of branches of an enterprise and computers of its remote employees with a central local network; serving a large number of heterogeneous users. All these features make it expedient to develop networks using VPN technology, which allows combining security requirements for the provided system services. However, its effective application requires the solution of a number of special problems associated with the choice of the structure of the network, the organization of the work of users and networks, ensuring the required level of data protection and the required characteristics of transmission and processing of information [1,2].

To date, there is a fairly rich practical experience in creating large corporate networks based on VPN technology, however, theoretical substantiation of the proposed solutions is required. As a rule, in each specific case, its own original solutions are required, due to the specifics of the network and the corporation, which must be evaluated using sufficiently universal methods and models.

Ensuring an appropriate level of information exchange security can be achieved through the complex use of organizational, technical, hardware-software and cryptographic protection means, as well as the implementation of continuous control over the effectiveness of the implemented information security measures.

Virtual networking which based on internet has several advantages:

- it provides scalable support for remote access to local network resources, allowing mobile users to communicate over local telephone lines with ISPs and thus enter their corporate network;
- when organizing remote access for users to a local network, the need for modem pools is eliminated, and remote access traffic can be managed in the same way as any other Internet traffic;
- costs for information exchange through an open external environment are reduced.

Experimental part. The ubiquity of IP-based networks, their versatility and cost effectiveness make these networks a more attractive VPN foundation for most businesses and organizations. In addition, QoS (Quality of Service) protocols and technologies such as RSVP, DiffServ and MPLS are beginning to be widely implemented in dedicated IP networks. According to many experts, VPN is one of the most important technologies that enterprises are using and will use in the near future. The significance of this technology for any enterprise, and even more so for budgetary organizations, is primarily due to the economic benefits that are associated with its implementation. Infonetics Research estimates that a VPN can save a company between 20% and 40% for site-to-site and 60% to 80% savings for remote users respectively. Tasks are considered here which arise when creating a network and analyze the modes of signal transmission. At its core, VPN (Virtual Private Networks) has many of the properties of a leased line, but it is deployed within a public network such as the Internet. With the tunneling technique, data packets are broadcast over the public network as over a normal point-to-point connection. A kind of tunnel is established between each pair of "transmitter-receiver of data" - a secure logical connection that allows encapsulating data from one protocol in packets of another. A very important property of tunnels is the ability to differentiate different types of traffic and assign them the necessary service priorities. [2,3,4,5]. These properties are considered in this research.

Let us compare the characteristics of the modes of signal transmission using virtual networks to determine the effectiveness of the network under various modes of organizing a virtual network, and to optimize the virtual network in order to identify an effective method for organizing a VPN.

Experiment results. The research was carried out by the method of network analysis using WireShark and TCPdump programs. The network analysis will be carried out by assessing bandwidth, connection speed, security, and the effect of frame and packet size on network performance, and the effect of a broadcast storm on network health.

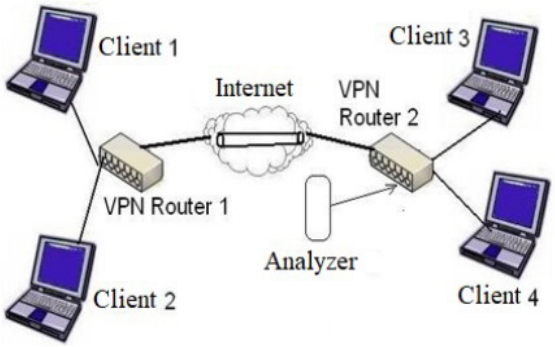

Figure 1 - Diagram of the organization of the experiment

The experimental setup is shown in Figure 1, where two VPN routers are installed and they are connected to each other by an Internet channel with a bandwidth of 18 Mbit / s, then a VPN tunnel is organized between them. Clients connect to two routers. Using the network analyzer programs (WireShark, TCPdump) configured for Router 2, we scan and analyze the VPN network in three different modes of operation of the Point to Point Tunneling Protocol VPN server (PPTP0):

1 Mode.

PPTP clients located in the WAN segment of the router connected to the router, after which standard speed tests were performed. Testing was carried out with one PPTP client. Test results are shown below. Figure 2 shows the results of the PPTP server network for the first client (1-client), where the following paths are indicated:

- LAN path → WAN - where traffic goes from the LAN segment computer to the PPTP client in the WAN segment;
- LAN path - this traffic goes from the PPTP client in the WAN segment to the computer in the LAN segment fdx path - full duplex - traffic goes in both directions.

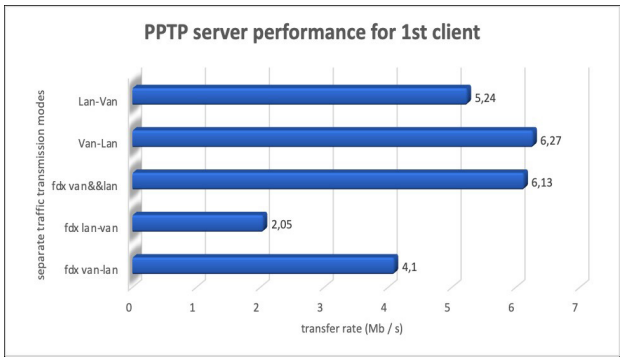

Figure 2 - PPTP server performance for the 1st client

Along the abscissa axis, transfer rate (Mb / s),

Separate traffic transmission modes along the ordinate.

The transfer results reflect the maximum speed: 6.27 Mbps is not slow enough compared to the speed

without using a VPN, especially when you consider that traffic is not encrypted.

2 mode.

L2TP (L2TP (Layer 2 Tunneling Protocol) VPN Server: Setting up an L2TP VPN server does not fundamentally differ from setting up a PPTP VPN server and encryption is also not supported. Performance testing was carried out in the same way as when testing the PPTP VPN server.

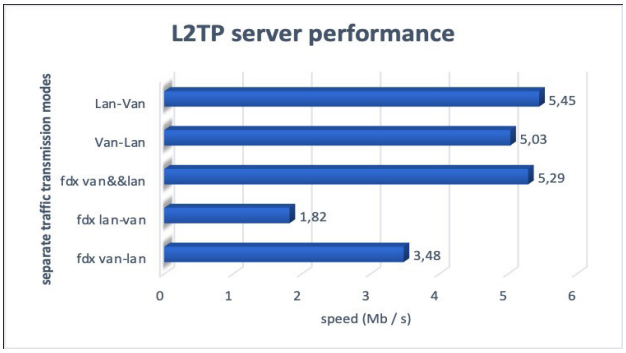

Figure 3 - L2TP server performance, 1 client, - speed (Mb / s) on the abscissa, - individual traffic transmission modes on the ordinate

Maximum speed: 5.45 Mbps - not slow enough when you consider that encryption is not supported.

3 mode.

IPSec VPN server: Some of the specifics of configuring an IPSec VPN server is that when static keys are set, you can use DES and 3DES encryption, and with dynamic key exchange, the configuration interface does not allow you to select the type of encryption, later it turned out that during dynamic key exchange, traffic encrypted using the AES algorithm.

Definitions:

– router - Internet router Level One FBR-1411TX;

– Gentoo - a computer with Gentoo Linux 2.6.11 installed;

– fdx - full duplex mode;

– along the abscissa axis, the speed (Mb / s);

– on the ordinate axis separate traffic transmission modes.

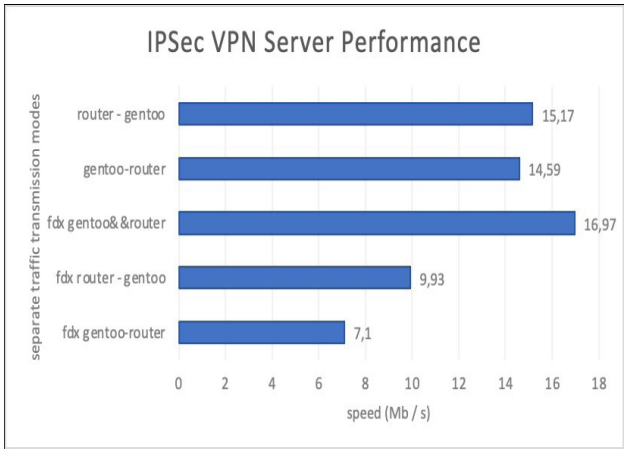

Figure 4 - Performance of IPSec VPN server, 1 tunnel, AES encryption

Maximum speed: 16.97 Mbps - sufficient speed for organizing a VPN, especially when compared with the operation of PPTP and L2TP VPN servers, which use slower speeds and no encryption.

Conclusion. An analysis of the specifics of the operation of corporate information systems and networks intended for their maintenance has shown that for building a corporate network it is advisable to use virtual private network (VPN) technology, which allows ensuring the fulfillment of the basic requirements for security and quality of customer service and applications.

The analysis of the current state and direction of development of VPN technology made it possible to draw a conclusion about the prospects of its application in the creation of corporate networks of a new generation, while highlighting the main tasks to be solved when creating a network.

Comparative characteristics of signal transmission modes using virtual networks are obtained to identify the effectiveness of the network in various modes of organizing a virtual network, and to optimize a virtual network in order to identify an effective method for organizing a VPN.

М.А. Хизирова[1], К.С. Чежимбаева[1], А.Д. Мухамеджанова[1], Ж.Д. Манбетова[1], Б. Онгар[2]
[1]Ғұмарбек Даукеев атындағы Алматы энергетика және байланыс университеті,
Алматы, Қазақстан.
[2]Логистика және көлік академиясы, Алматы, Қазақстан.
E-mail: hizirova73@mail.ru

КОРПОРАТИВТІК ЖЕЛІЛЕРДЕ СИГНАЛ БЕРУ ҮШІН ВИРТУАЛДЫ ЖЕКЕ VPN (VIRTUAL PRIVATE NETWORK) ТЕХНОЛОГИЯСЫН ҚОЛДАНУ

Аннотация. Бұл жұмыста виртуалды жеке желілер VPN (Virtual Private Network) технологиясын қолдана отырып корпоративті жүйелер үшін сигнал берудің кейбір режимдері қарастырылған. Туннельдердің өте маңызды қасиеті - бұл трафиктің әртүрлі түрлерін ажырата білу және оларға қажетті қызмет көрсету басымдықтарын тағайындау. Жұмыста виртуалды желіні ұйымдастырудың әр түрлі режимдерінде желінің тиімділігін анықтау үшін және виртуалды желіні оңтайландыру үшін виртуалды желілерді қолдана отырып сигнал беру режимдерінің салыстырмалы сипаттамалары алынды және виртуалды желіні тиімді түрде анықтады. VPN ұйымдастыру әдісі. Сондай-ақ,

жұмыста корпоративті ақпараттық жүйелер мен оларға қызмет көрсетуге арналған желілер жұмысының ерекшеліктері талданды, корпоративті желіні құру үшін виртуалды жеке желі (VPN) технологиясын қолданудың орынды екендігі көрсетілді, бұл базалық жүйенің орындалуын қамтамасыз етеді, тұтынушыларға қызмет көрсету мен қосымшалардың қауіпсіздігі мен сапасына қойылатын талаптар, жаңа буын корпоративті желілерді құру кезінде VPN технологиясының қазіргі жағдайы мен даму бағыты, сонымен бірге желіні құру кезінде шешілуі керек негізгі міндеттерді атап өту керек. Корпоративтік желілер үшін IPSec VPN серверін орнатудың кейбір ерекшеліктері қарастырылады.

Түйін сөздер: корпоративтік желілер, виртуалды жеке желілер VPN (виртуалды жеке желі), туннельдеу, трафик, нүктеден нүктеге қосылу, сервер, маршрутизатор

М.А. Хизирова[1], К.С. Чежимбаева[1], А.Д. Мухамеджанова[1], Ж.Д. Манбетова[1], Б. Онгар[2]
[1]Алматинский университет энергетики и связи имени Гумарбека Даукеева, Алматы, Казахстан.
[2]Академия логистики и транспорта, Алматы, Казахстан.
E-mail: hizirova73@mail.ru

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ ВИРТУАЛЬНЫХ ЧАСТНЫХ СЕТЕЙ VPN (VIRTUAL PRIVATE NETWORK) ДЛЯ ПЕРЕДАЧИ СИГНАЛОВ В КОРПОРАТИВНЫХ СЕТЯХ

Аннотация. В данной работе рассмотрены некоторые режимы передачи сигналов для корпоративных систем при использовании технологии виртуальных частных сетей VPN (Virtual Private Network). Очень важным свойством туннелей является возможность дифференциации различных типов трафика и назначения им необходимых приоритетов обслуживания. В работе проведены исследования и получены сравнительные характеристики режимов передачи сигналов с помощью виртуальных сетей для выявления эффективности работы сети при различных режимах организации виртуальной сети, и для оптимизации виртуальной сети с целью выявления эффективного метода организации VPN. Также в работе проведены анализы специфики работы корпоративных информационных систем и сетей, предназначенных для их обслуживания, показал, что для построения корпоративной сети целесообразно применять технологию виртуальных частных сетей (VPN), которая позволяет обеспечить выполнение основных требований по безопасности и качеству обслуживания клиентов и приложений и современного состояния и направлении развития VPN- технологии при создании корпоративных сетей нового поколения, при этом выделены основные задачи, требующие решения при создании сети. Рассмотрены некоторые особенности настройки IPSec VPN-сервера для корпоративных сетей.

Ключевые слова: корпоративные сети, виртуальные частные сети VPN (Virtual Private Network), туннелирование, трафик, двухточечное соединение, сервер, роутер.

Information about authors:
Muhabbat Khizirova, PhD, associate professor, Almaty University of Power Engineering and Telecommunications named after Gumarbek Daukeev, Almaty, Kazakhstan; hizirova73@mail.ru, https://orcid.org/0000-0002-2242-7756
Katipa Chezhimbayeva, candidate of technical sciences, associate professor, Almaty University of Power Engineering and Telecommunications named after Gumarbek Daukeev, Almaty, Kazakhstan; chezhimbayeva@aues.kz; https://orcid.org/0000-0002-1039-1629
Almira Mukhamejanova1, doctoral student Almaty University of Power Engineering and Telecommunications named after Gumarbek Daukeev, almira_md@mail.ru, https://orcid.org/0000-0003-3063-1340
Zhanat Manbetova, doctoral student Almaty University of Power Engineering and Telecommunications named after Gumarbek Daukeev, Almaty, Kazakhstan; zmanbetova@inbox.ru; https://orcid.org/0000-0002-6716-4646
Bulbul Ongar, PhD, associate professor, Logistics and Transport Academy, ongar_bulbul@mail.ru, https://orcid.org/0000-0002-8333-8343

References

[1] Daffi D. Quality support in virtual networks // Networks. – 2001 y. – №09. – p.10-15.
[2] Brown SVirtual private networks. – M.: Lory, 2001 y. – p. 508.
[3] Sallivan K. VPN technology progress. PCWEEK/RE, №2, 26 January 2003 y. – p. 225.
[4] Shtainke S. VPN between local networks. LAN/ Network Solutions Journal. October 2001 y., Part 4, №10. – p. 109.
[5] Yakimova, IA Mathematical model of processing IP packets in the VPNMPLS network router [Text] / IA Yakimova, VE Toiskin, VA Tsimbal, SV Ryabtsev, TA Isaeva / / International conf. "Radio-electronic devices and systems for infocommunication technologies" (RES-2014); Reports; Series: scientific. conf. ded. Radio Day / Ros. scientific and technical total radio engineering., electron. and communication to them. A.S. Popov. –M. : LLC "BRIS-M", 2014. - Issue. LXIX. -FROM.- p.199-203.

МАЗМҰНЫ-СОДЕРЖАНИЕ-CONTENTS

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.geolog-technical.kz/index.php/en/

ISSN 2518-170X (Online),
ISSN 2224-5278 (Print)

Редакторы: *М. С. Ахметова, Р. Ж. Мрзабаева, Д. С. Аленов*
Верстка на компьютере *В.С. Зикирбаева*

Подписано в печать 15.06.2021.
Формат 60x881/8. Бумага офсетная. Печать – ризограф.
4,6 п.л. Тираж 211. Заказ 3.

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