ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ҰЛТТЫҚ ҒЫЛЫМ АКАДЕМИЯСЫНЫҢ

ХАБАРШЫСЫ

ВЕСТНИК	THE BULLETIN
НАЦИОНАЛЬНОЙ АКАДЕМИИ НАУК РЕСПУБЛИКИ КАЗАХСТАН	OF THE NATIONAL ACADEMY OF SCIENCES OF THE REPUBLIC OF KAZAKHSTAN

1944 ЖЫЛДАН ШЫҒА БАСТАҒАН
ИЗДАЕТСЯ С 1944 ГОДА
PUBLISHED SINCE 1944

6

АЛМАТЫ		ҚАРАША
АЛМАТЫ	2018	НОЯБРЬ
ALMATY		NOVEMBER

NAS RK is pleased to announce that Bulletin of NAS RK 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 Bulletin of NAS RK in the Emerging Sources Citation Index demonstrates our dedication to providing the most relevant and influential multidiscipline content to our community.

Қазақстан Республикасы Ұлттық ғылым академиясы "ҚР ҰҒА Хабаршысы" 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. Web of Science зерттеушілер, авторлар, баспашылар мен мекемелерге контент тереңдігі мен сапасын ұсынады. ҚР ҰҒА Хабаршысының Emerging Sources Citation Index-ке енуі біздің қоғамдастық үшін ең өзекті және беделді мультидисциплинарлы контентке адалдығымызды білдіреді.

НАН РК сообщает, что научный журнал «Вестник НАН РК» 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 Вестника НАН РК в Emerging Sources Citation Index демонстрирует нашу приверженность к наиболее актуальному и влиятельному мультидисциплинарному контенту для нашего сообщества.

Типографияның мекенжайы: «Аруна» ЖК, Алматы қ., Муратбаева көш., 75.

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

Address of printing house: ST "Aruna", 75, Muratbayev str, Almaty

BULLETIN OF NATIONAL ACADEMY OF SCIENCES
OF THE REPUBLIC OF KAZAKHSTAN

Y. Zh. Aitkhozhayeva[1], A. A. Ziro[1], Zh. A. Zhaibergenova[1], A. G. Baltabay[2]

[1]Kazakh National Research Technical University named after K. I. Satpayev (Satbayev University),
Almaty, Kazakhstan,
[2]School of Control and Computer Engineering, North China Electric Power University, Beijing, China.
E-mail: ait_djam@mail.ru, ziro.aasso@gmail.com, zhanshuak@gmail.com, aliya250892@gmail.com

PENETRATION TESTING

Abstract. Detection of vulnerabilities is an important composite component of both internal and external audit of information security systems. Potential internal vulnerabilities can be revealed by testing for penetration. At the same time, both the commercial and being in the free access instruments of penetration test are used differently. The review of recognized methodologies (standards) of conducting testing for penetration is made. The list of free distribution kits of instruments of penetration test is provided. One of the widespread attacks is BackDoor allowing to receive control over the attacked system. With the help of the utility of Msfvenom which is a part of a free distribution kit of penetration test Kali Linux with methodology of PTES the attack of BackDoor by implementation of an exploit is successfully realized. Control over the attacked virtual machine was as a result received.

Keywords: vulnerabilities, penetration testing methodology, BackDoor attacks.

Introduction. Now there was the standard international practice of support of the mode of the information security (IS), one of the stages of which is audit of the IS systems. Existence of management system of IS (Information Security Management), and in particular audit of management system of IS (Risk Management), is an indispensable condition of the organization of the IS mode at the enterprise.

IS audit is carried out by a team of security experts of enterprise systems and experts in the field of management. One of the methods in case of the active audit of information security systems is testing for penetration. Testing for penetration - the valuation method of safety of computer systems or networks simulars of the attack of the malefactor (ethic hacking - ethical hacking). Testing for penetration is an integral part of the analysis of security of any information resource. The authorized search of vulnerabilities of protection system is execute and their subsequent use for penetration into subject to protection. The purpose of penetration test is independent assessment and the expert opinion on a status of security of the critical information. The recommendations about closing (elimination) of the found vulnerabilities are whenever possible formulated. As a result, security concerns which need to be solved urgently come to light. There is a certification of CHE (Certified Ethical Hacker) for experts in the field of conducting testing for penetration which is recognized around the world today and confirms existence of appropriate level of knowledge. The certified examination of EC-Council CEH approved by the U.S. Department of Defense is one of recognized for experts of IT safety. State structures of the USA require existence of this certificate for certain positions of IS that once again emphasizes importance of penetration test as instrument of the active audit.

Methods. There are several recognized techniques (standards) of conducting penetration test: Payment Card Industry Data Security Standard – PCI DSS (Penetration Test Guidance, methodology of Special Interest Group PCI Security Standards Council), OSSTMM (Open Source Security Testing Methodology Manual), NIST Special Publications 800-115 Technical Guide to Information Security Testing and Assessment (NIST methodology, CSRC subdividing), Study A Penetration Testing Model (BSI methodology, the German subdividing of Federal Office for Information Security), ISSAF (Information System Security Assessment Framework, methodology of Open Information Systems Security

Group), OWASP Testing Guide (methodology of Open Web Application Security Project), PTES Technical Guidelines (Penetration Testing Execution Standard), methodology of Deloitte [1-8].

The offered methodologies differ on steps of conducting testing, types of testing for penetration, detailing of testing objects, determination of testing procedures, the description of utilities for conducting testing, a formulating, structure, a detail of description of a technique and purposes of penetration testing.

PCI DSS is oriented on a penetration testing for the organizations which processing, storing and transferring data of card owners. OSSTMM is one of the first techniques of complex testing of information security of the organization. In methodology of NIST different recommendations about testing types are described, there is in the separate document an operation methodology with a fire-wall (NIST SP 800-41 Guideline on Firewalls and Firewall Policy). The detailed methodology of BSI provides both technical and organizational aspects of testing, and legal aspects. ISSAF describes assessment of safety of fire-walls, routers, anti-virus systems and many other things. Methodologies of PTES and OWASP are well structured therefore they are widely used when testing for penetration. PTES is model which was used in the system of a penetration testing Rapid7 Metasploit.

Tools. Penetration test is subdivided on external and internal. External infrastructure penetration test is an analysis of perimeter from the Internet. The expert makes attempts, trying to compromise available network services and to develop the attack which main goal is to get in system. Internal infrastructure penetration test is a simulation of action of the insider. As the insider the infected node in a network can appear.

In turn external penetration test is conditionally divided into categories: network scanners, scanners in web scripts, exploits, automation of injections, debugger. There are both separate programs, and distribution kits (commercial and free) for conducting testing for penetration.

Usually distribution kits represent the processed versions existing Linux distribution kits.

The most known of them which are in the free access [9]:

- BlackArch Linux, a distribution kit is based on Arch Linux. Includes 1359 utilities for testing for penetration, it is intended for professionals, maintains architecture of i686 and x86_64;

- Parrot Security OS, is based on Debian Linux, the easy and effective testing tool on penetration, idle time in mastering;

- BackBox, is based on Ubuntu Linux, is convenient for private use, and has rather good functionality for daily use;

- Pentoo, is based on Gentoo Linux, contains a set of security-utilities;

- Network Security Toolkit, is based on Fedora Linux, intended for the analysis of safety of a network, gives simple access to a wide set of the opened network applications, many of which are included in one hundred the best security aids recommended by the website insecure.org;

- DEFT Linux, is founded on Lubuntu, has the convenient graphic interface, includes antiviruses, the systems of information search in a browser cache, network scanners and utilities for detection of rootkits, tools for search of the hidden data on a disk;

- Samurai Web Security Framework is intended for testing for penetration of different web applications. It is delivered in the form of an image of the virtual machine which contains the most popular Open Source of the utility for information collection and carrying out different attacks to web applications;

- Santoku Linux, is based on Ubuntu Linux. It is intended for the analysis of mobile devices and applications: carrying out the analysis of safety, extraction of data, the reverse engineering, forensic, also contains development tools. It is provided only for the X64 platform;

- WifiSlax, is based on Slackware Linux, intended for check of safety of the WiFi networks systems and carrying out the criminalist analysis. It is used for audit of Wi-Fi of networks as the majority of popular utilities for the analysis of security of wireless networks are included in it, maintains the majority creates network interface cards;

- Kali Linux, is based on Debian Linux, includes more than 600 security-utilities (Wireshark, Nmap, Armitage, Aircrack, Burp Suite, etc.) and multilingual support. There are several types of this distribution kit for different platforms: x86 and ARM systems, systems of virtualization, mobile platforms (Kali Net hunter).

Results. Kali Linux – the most popular and advanced distribution kit for conducting testing for penetration and security audit today [10]. The special kernel of Kali Linux is protected from injections that allows to book audit of wireless networks safely. Kali Linux maintains a large number of wireless devices, is compatible to USB and other wireless devices.
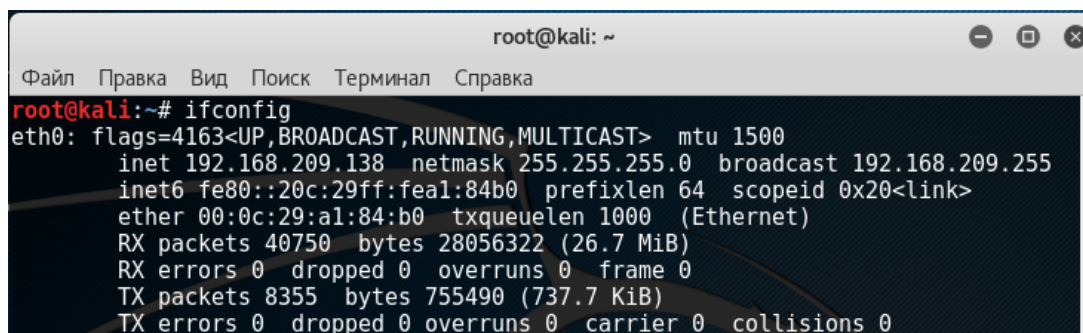
In [11] risks and threats of virtualization and results of detection of vulnerabilities of the virtual machines by port scanning by means of the utility of Wireshark from the Kali Linux distribution kit were presented.

Also the utility of Msfvenom is a Kali Linux part by means of which it is possible to realize the attack of BackDoor, having created an exploit. Successfully realized attack of BackDoor allows to implement on the attacked computer the small program through which it is possible to collect confidential data, to control far off an operating system and the computer in general, to use the cracked computer for scanning of a network, carrying out network attacks of network hacking. Usually in case of this attack two programs are used. The program of control is installed on the computer of the tester and controls other program which is illegally set on the attacked computer.

The exploit uses vulnerabilities of the attacked system to violation of its safety. There is an open database of exploits (The Exploit Database) and the appropriate vulnerable software. The basis is created and supported for testers on penetration and researchers of vulnerabilities. There are also closed databases in which the most interesting exploits are collected. Access to them can be or paid, or for a certain circle of people. To one of examples can serve the tool for testing for penetration – Metasploit Exploitation Framework. It contains a big basis of exploits. There are two Metasploit versions, free and paid. There are websites on search of exploits, such as The Exploit Database, WPScan Vulnerability Database (a fresh basis of exploits for WordPress) and Packet Storm (the most different fresh exploits).

With the help of the utility of Msfvenom which is a part of a free distribution kit of penetration test Kali Linux with methodology of PTES the attack of BackDoor was organized. As attacked the virtual machine was used. With the help of Msfvenom the special program - an exploit (exploit) with the .exe format is created. Implementation of this program in the attacked computer, gives to the malefactor access to the virtual machine and means of the user.

During creation of an exploit it is necessary to specify the IP address of the attacking machine, the port and the place of saving the file of an exploit in the attacking machine. To learn the IP address, it is possible to use the ifconfig command. This command will issue information on a configuration of the attacking machine, including the IP address - 192.168.209.138 (figure 1).


```
root@kali: ~

Файл  Правка  Вид  Поиск  Терминал  Справка

root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.209.138  netmask 255.255.255.0  broadcast 192.168.209.255
        inet6 fe80::20c:29ff:fea1:84b0  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:a1:84:b0  txqueuelen 1000  (Ethernet)
        RX packets 40750  bytes 28056322 (26.7 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8355  bytes 755490 (737.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Figure 1 – Configuration of hacking machine

We use data retrieved during creation of an exploit: we specify the IP address of the attacking machine (192.168.209.138), the port (5566), the place of saving and file name of an exploit (attack.exe). The exploit is created on the x86 platform, file size 73802 bytes (figure 2).

After creation of an exploit we will send it to the virtual machine Windows 7 via the Internet. For example, through e-mail, explaining attacked that it is the useful program.

Further on the attacking machine we will launch metasploit framework (figure 3).

Then we register the IP address of the attacking machine and on what port there will be a connection with the implemented exploit (figure 4).

Attacked launches an exploit by the machine, thinking that it is the useful program.
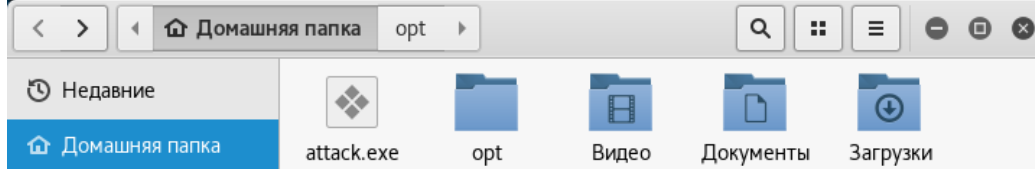
Figure 2 – Creation of exploit

Figure 3 – Start of metasploit framework

Figure 4 – Configuration of linking with exploit

Figure 5 – Link with exploit

Figure 6 – Messages from exploit

By this time by the attacking machine it is necessary to open a session of connection with an exploit (figure 5).

Now the virtual machine under monitoring of the attacking machine (figure 6).

Conclusion. Innovation, organization, and sophistication - these are the tools of cyber attackers as they work harder and more efficiently to uncover new vulnerabilities [12]. With the help of testing for penetration it is possible to be ahead of malefactors, having revealed and having eliminated vulnerabilities before real cyber-attack. Now penetration test is a mandatory component of both internal and external audit. Free products of penetration testing are easy to use. They allow identifying vulnerabilities on the channel, network and transport levels, having built-in expert systems. When solving problems at the application level, these products unusable. In this case necessary to use commercial solutions (commercial versions Nessus and Rapid 7 NeXpose, Xspider 7, Retina Nenwork Security Scanner, SAINT and etc.) [13-16]. Commercial products of the penetration testing use more advanced technologies and have extended capabilities compared to free ones. This provides additional opportunities in assessing risks and threats. Penetration testing should be performed on both the channel, network and transport layers, and at the application level.

REFERENCES

[1] Information Supplement: Penetration Testing Guidance (2015). [Penetration Test Guidance Special Interest Group PCI Security Standards Council] 40 p. [https://www.pcisecuritystandards.org/documents/Penetration_Testing_Guidance_March_2015. pdf] (In Eng.).

[2] Herzog P. (2006). OSSTMM – The Open Source Security Testing Methodology Manual. USA, New York. 129 p. [http://www.isecom.org/research/osstmm.html] (In Eng.).

[3] Scarfone K, Souppaya M., Cody A., Orebaugh A. (2008). NIST Special Publications 800-115 Technical Guide to Information Security Testing and Assessment. USA, Gaithersburg. 80 p. [http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf] (In Eng.).

[4] BSI-Study A Penetration Tesing Model. Germany, Bonn. 111 p. [https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/Penetration/penetration_pdf.pdf?__blob=publicati onFile] (In Eng.).

[5] Rathore B., Brunner M., Dilaj M., Herreragh O., Brunati P., Subramaniam R., Raman S., Chavan U. (2006). ISSAF – Information System Security Assesment Framework. 1264 p. [http://www.oissg.org/issaf02/issaf0.1-5.pdf] (In Eng.).

[6] OWASP Testing Guide [https://www.owasp.org/index.php/OWASP_Testing _Project] (In Eng.).

[7] Penetration Testing Execution Standard Technical Guidelines [http://www.penetration test-standard.org/index.php/Main_Page] (In Eng.).

[8] Deloitte. Test of networks and systems on resistance to cracking (pentest),or penetration test [Test setey i system na ustoychivost' ko vzlomu (penetration test), ili test na proniknovenie] (2017) [https://www2.deloitte.com/content/dam/Deloitte/by/Documents/risk/ Penetration-test-A4-RUS. pdf] (In Rus.).

[9] The best distributions for penetration testing [Luchshie distributivy dlya provedeniya testirovaniya na pronicnovenie] (2016). [Penetration testit] [https://habrahabr.ru/company/ pentestit/blog/276477] 23 Mar 2018 (In Russ.).

[10] Official Kali Linux Documentation (2014). [Kali] [https://www.docs.kali.org/kali-linux-documentation] (In Eng.).

[11] Aytkhozhaeva E.Zh., Ziro A.A., Zhaibergenova Zh.A. (2017). Virtualization safety [Computer Modelling and New Technologies]. ISSN 1407-5806 21 (2) 48-53 (In Eng.).

[12] Internet Security Threat Report (ISTR) (2018) [Symantec 2018] Mar 2018. Vol. 23. 87 p. [https://img03.en25.com/Web/Symantec/%7B4424960b-b98b-4945-bbe2-1cc8c7c44 edd%7D_RPT_ISTR23-FINAL_EN.pdf?aid=elq] (In Eng.).

[13] Lopez L. (2016). Nessus Tenable Vs. Nexpose By Rapid7 [Gb Advisors] [Http://Www.Gb-Advisors.Com/Tech-Blog/Nessus-Tenable-Vs-Nexpose-By-Rapid7] (In Eng.).

[14] Leonov A.V. (2017). Rapid7 Nexpose in 2017 [Information Security Automation] [Https://Avleonov.Com/2017/04/06/Rapid7-Nexpose-In-2017] (In Eng.).

[15] Retina Nenwork Security Scanner (2017). [Beyondtrust] [Https://Www.Beyondtrust.Com/Resources/Data-Sheet/Retina-Network-Security-Scanner/] (In Eng.).

[16] Saint Security Suite (2017). [Saint Corporation] [Http://Www.Saintcorporation. Com/Security-Suite] (In Eng.).

Е. Ж. Айтхожаева¹, А. А. Зиро¹, Ж. А. Жайбергенова¹, А. Ғ. Балтабай²

¹Қ. И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті, Алматы, Қазақстан,
²Солтүстік Қытай электроэнергетикалық университеті, Пекин, ҚХР

ЕНУГЕ ТЕСТІЛЕУ

Аннотация. Осалдықтарды анықтау – ақпараттық қауіпсіздік жүйелерінің ішкі және сыртқы аудитінің маңызды құрамдас бөлігі болып табылады. Әлеуетті ішкі осалдықтарды енуге тестілеу арқылы анықтауға болады (pentest). Бұл ретте, әртүрлі коммерциялық, сондай-ақ пентесттің еркін қол жетімді құралдары пайдаланылады. Енуге тестілеу жүргізудің танылған әдістемелеріне (стандарттарына) шолу жүргізілді. Пентест құралдарының тегін дистрибутивтерінің тізімі келтірілген. Кең тараған шабуылдардың бірі – шабуылға ұшыраған жүйені бақылауға мүмкіндік беретін BackDoor шабуылы. Пентесттің тегін дистрибутиві Kali Linux құрамына кіретін Msfvenom утилитасының көмегімен PTES әдісітемесі бойынша эксплоитты енгізу арқылы BackDoor шабуылы іске асырады. Нәтижесінде, шабуылданған виртуалды машина бақылауға алынды.

Түйін сөздер: осалдықтар, енуге тестілеу әдістемелері, BackDoor шабуылдары.

Е. Ж. Айтхожаева¹, А. А. Зиро¹, Ж. А. Жайбергенова¹, А. Г. Балтабай²

¹Казахский национальный исследовательский технический университет им. К. И. Сатпаева,
Алматы, Казахстан,
²Северо-китайский электроэнергетический университет, Пекин, КНР

ТЕСТИРОВАНИЕ НА ПРОНИКНОВЕНИЕ

Аннотация. Выявление уязвимостей является важной составной компонентой как внутреннего, так и внешнего аудита систем информационной безопасности. Потенциальные внутренние уязвимости могут быть выявлены тестированием на проникновение (пентест). При этом используются различные как коммерческие, так и находящиеся в свободном доступе инструменты пентеста. Сделан обзор признанных методологий (стандартов) проведения тестирования на проникновение. Приводится перечень бесплатных дистрибутивов инструментов пентеста. Одной из распространенных атак является атака BackDoor, позволяющая получить контроль над атакуемой системой. С помошью утилиты Msfvenom, входящей в состав бесплатного дистрибутива пентеста Kali Linux, по методологии PTES реализована атака BackDoor путем внедрения эксплоита. В результате был получен контроль над атакуемой виртуальной машиной.

Ключевые слова: уязвимости, методологии тестирования на проникновение, атаки BackDoor.

Information about authors:

Aitkhozhayeva Yevgeniya – associated professor of the Department of Information Security, Candidate of Technical Sciences, Kazakh National Research Technical University named after K. I. Satpayev, Almaty, Kazakhstan; ait_djam@mail.ru; https://orcid.org/0000-0002-5961-8556

Ziro Aasso – Master of Technical Sciences, senior-lector of the Department of Information Security, Kazakh National Research Technical University named after K. I. Satpayev, Almaty, Kazakhstan; ziro.aasso@gmail.com; https://orcid.org/0000-0002-5952-877X

Zhaibergenova Zhanshuak – Master of Technical Sciences, tutor of the Department of Information Security, Kazakh National Research Technical University named after K. I. Satpayev, Almaty, Kazakhstan; zhanshuak@gmail.com; https://orcid.org/0000-0002-4775-8877

Baltabay Aliya – Master of Military Sciences, master student at North China Electric Power University, Beijing, China; aliya250892@gmail.com; https://orcid.org/0000-0002-9145-0992

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.