

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

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ  
ҰЛТТЫҚ ҒЫЛЫМ АКАДЕМИЯСЫ

әл-Фараби атындағы Қазақ ұлттық университетінің

# Х А Б А Р Л А Р Ы

---

---

## ИЗВЕСТИЯ

НАЦИОНАЛЬНОЙ АКАДЕМИИ НАУК  
РЕСПУБЛИКИ КАЗАХСТАН  
Қазақстан Республикасының Ғылым  
Академиясының Алматыдағы  
Әл-Фараби атындағы Қазақ ұлттық  
университетінің

## N E W S

OF THE ACADEMY OF SCIENCES  
OF THE REPUBLIC OF KAZAKHSTAN  
al-Farabi Kazakh National University

SERIES

PHYSICO-MATHEMATICAL

1 (341)

JANUARY – MARCH 2022

PUBLISHED SINCE JANUARY 1963

PUBLISHED 4 TIMES A YEAR

ALMATY, NAS RK

---

---

*NAS RK is pleased to announce that News of NAS RK. Series physico-mathematical 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 chemistry and technologies in the Emerging Sources Citation Index demonstrates our dedication to providing the most relevant and influential content of chemical sciences to our community.*

*Қазақстан Республикасы Ұлттық ғылым академиясы «ҚР ҰҒА Хабарлары. Физика және информатика 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. Web of Science зерттеушілер, авторлар, баспашылар мен мекемелерге контент тереңдігі мен сапасын ұсынады. ҚР ҰҒА Хабарлары. Химия және технология сериясы Emerging Sources Citation Index-ке енуі біздің қоғамдастық үшін ең өзекті және беделді химиялық ғылымдар бойынша контентке адалдығымызды білдіреді.*

*НАН РК сообщает, что научный журнал «Известия НАН РК. Серия физика и информационные технологии» 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 в Emerging Sources Citation Index демонстрирует нашу приверженность к наиболее актуальному и влиятельному контенту по химическим наукам для нашего сообщества.*

### **Бас редактор:**

**МҰТАНОВ 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

### **Редакция алқасы:**

**ҚАЛИМОЛДАЕВ Мақсат Нұрәділұлы** (бас редактордың орынбасары), физика-математика ғылымдарының докторы, профессор, ҚР ҰҒА академигі, ҚР БҒМ ҒК «Ақпараттық және есептеу технологиялары институты» бас директорының кеңесшісі, зертхана меңгерушісі (Алматы, Қазақстан) Н=7

**БАЙГУНЧЕКОВ Жұмаділ Жаңабайұлы** (бас редактордың орынбасары), 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 Hemando**, профессор, Ядролық ғылымдар институты (Мехико, Мексика) Н=28

**ЖҮСПОВ 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

**МИХАЛЕВИЧ Александр Александрович**, техника ғылымдарының докторы, профессор, Беларусь ҰҒА академигі (Минск, Беларусь) Н=2

**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-математикалық 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/>*

© Қазақстан Республикасының Ұлттық ғылым академиясы, 2022

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

### Главный редактор:

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

### Редакционная коллегия:

**КАЛИМОЛДАЕВ Максат Нурадилович**, (заместитель главного редактора), доктор физико-математических наук, профессор, академик НАН РК, советник генерального директора «Института информационных и вычислительных технологий» КН МОН РК, заведующий лабораторией (Алматы, Казахстан) Н=7

**БАЙГУНЧЕКОВ Жумадил Жанабаевич**, (заместитель главного редактора), доктор технических наук, профессор, академик НАН РК, Институт кибернетики и информационных технологий, кафедра прикладной механики и инженерной графики, университет Сатпаева (Алматы, Казахстан) Н=3

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

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

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

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

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

**МИХАЛЕВИЧ Александр Александрович**, доктор технических наук, профессор, академик НАН Беларуси (Минск, Беларусь) Н=2

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

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

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

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

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

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

«Известия НАН РК. Серия физика-математическая».

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/>*

© Национальная академия наук Республики Казахстан, 2022

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

#### **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

#### **Editorial board:**

**KALIMOLDAYEV Maksat Nuradilovich** (Deputy Editor-in-Chief), doctor in Physics and Mathematics, Professor, Academician of NAS RK, Advisor to the General Director of the Institute of Information and Computing Technologies of SC MES RK, Head of the Laboratory (Almaty, Kazakhstan) H=7

**BAYGUNCHEKOV Zhumadil Zhanabayevich**, (Deputy Editor-in-Chief), 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

**MIKHALEVICH Alexander Alexandrovich**, Doctor of Technical Sciences, Professor, Academician of NAS of Belarus (Minsk, Belarus) H=2

**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 physico-mathematical.**

**ISSN 2518-1726 (Online),**

**ISSN 1991-346X (Print)**

Owner: RPA «National Academy of Sciences of the Republic of Kazakhstan» (Almaty). The certificate of registration of a periodical printed publication in the Committee of information of the Ministry of Information and Social Development of the Republic of Kazakhstan No. 16906-Ж, issued 14.02.2018

Thematic scope: *series 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/>*

© National Academy of Sciences of the Republic of Kazakhstan, 2022

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



NEWS

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

ISSN 1991-346X

Volume 1, Number 341 (2022), 88–95

<https://doi.org/10.32014/2022.2518-1726.120>

МРНТИ 81.93.29

УДК 004.056.5

**О.А. Усатова<sup>1</sup>, А.Ш. Баракова<sup>2\*</sup>**

<sup>1</sup>Ақпараттық және есептеуіш технологиялар институты, Алматы, Қазақстан;

<sup>2</sup>Әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан.

E-mail: [balia\\_79@mail.ru](mailto:balia_79@mail.ru)

**ҚАЗІРГІ ЗАМАНҒЫ ВЕБ-РЕСУРСТАРДЫ ҚОРҒАУ ЖҮЙЕЛЕРІН ТАЛДАУ**

**Аннотация.** Мақалада веб-ресурстарды зиянкестердің әрекеттерінен қорғау мәселелеріне шолу ұсынылған. Берілген ақпаратты қорғауға әсер ететін веб-ортаның ерекшеліктері келтірілген, веб – қызметтің базалық құрылымы сипатталған және ықтимал қауіптер жүйеленген және талданған сонымен қатар веб - сервистердің анықталған осалдықтарын жою бойынша шаралар әзірленген. Бұл тақырыптың өзектілігі мен маңыздылығы жүйелердің қауіпсіздігі саласындағы жоғары талпынысқа қарамастан көптеген жүйелер соның ішінде сайттарға жасалатын зиянкестердің есебінен сайттардың бұзылуына ұшырауы мүмкін. Қазіргі заманғы ақпараттық жүйелердің көпшілігі веб-сайттар түрінде жасалады сондықтан қауіпсіздікке ерекше назар аудару қажет. Бұл жұмыстың мақсаты веб-сайттарға жасалатын шабуылдардың кешенді қорғау әдістеріне қатысты мәселелерді зерттеу болып табылады. Мақалада веб сайттармен интернет тораптарындағы мәліметтерге жасалатын қаіптердің қауіпсіздіктің негізгі аспектілері және веб сайттардың сақтық шаралары қарастырылады. Ақпаратты қорғау және құпиялылықты сақтау мысалдары және де арнайы сайтты қорғаудың жолдары келтірілген. Қауіпсіздік параметрлерін таныстыру параметрлері келтірілген. Зерттеу нысаны ретінде [www.aliyaschool.kz](http://www.aliyaschool.kz) сайтының қорғаныс мәліметтері ұсынылған. Веб-сервистердегі ақпараттарды қорғаудың негізгі стандарттары мен спецификасы көрсетілген. Веб әзірлеушілердің және кез - келген веб-ресурстың ақпаратын ұрлықтан қорғау және оның мазмұнын өзгерту немесе жою кезінде салдарын анықтау мен алдын - алу жолдары көрсетілген. Интернет желісінде коммерциялық құндылығы бар контентті (мәтіндік) заңсыз алу проблемасы бар. Жеңудің жалғыз нұсқасы - оны көпшілікке қорғау. Егер бұл мүмкін болмаса оны техникалық және заңды түрде қорғау қажет. Жұмыстың мақсаты - контентті рұқсатсыз алудың техникалық қорғау мүмкіндіктерін және оның дәрменсіздігін және құқықтық салада кейінгі қорғауды жеңілдететін көмекші құрал ретінде оның мүмкіндіктерін көрсету. Осалдықтарды анықтаға шолуды жүргізу негізінде және веб-қосымшаларды қорғаудың осындай әдістерін одан әрі дамыту әртүрлі әдістемелердің мүмкіндіктерін біріктіру жолымен жүруі мүмкін деген қорытынды жасауға болады.

**Түйін сөздер:** веб-сервис, сайт, санкцияланбаған қол жеткізу, ақпараттың құпиялылығы, қорғау жүйесі, аутентификация, сәйкестендіру, авторизация, қол жеткізу құқығын шектеу, желі, алмасу хаттамасы, шабуыл, оқыс оқиға.

**О.А. Усатова<sup>1</sup>, А.Ш. Баракова<sup>2\*</sup>**

<sup>1</sup>Институт информационных и вычислительных технологий, Алматы, Казахстан;

<sup>2</sup>Казахский национальный университет им. аль-Фараби, Алматы, Казахстан.

E-mail: [balia\\_79@mail.ru](mailto:balia_79@mail.ru)

**АНАЛИЗ СОВРЕМЕННЫХ СИСТЕМ ЗАЩИТЫ ВЕБ-РЕСУРСОВ**

**Аннотация.** Представлен обзор проблем защиты веб-ресурсов от действий злоумышленников, описана базовая структура Веб-сервиса, приведены особенности Веб-среды, влияющие на защиту предоставляемой информации, систематизированы и проанализированы возможные угрозы,

выработаны меры по устранению выявленных уязвимостей веб-сервисов. Актуальность данной тематики обусловлена тем, что, несмотря на высокий прогресс в области безопасности систем, все же многие системы, в том числе и сайты, могут быть подвергнуты взломам злоумышленников. Большинство современных информационных систем создаются в виде Web-сайтов, поэтому безопасности необходимо уделить особое внимание. Цель данной работы заключается в изучении вопросов, которые касаются методов комплексной защиты веб-сайта от хакерских атак. Рассматриваются основные аспекты безопасности и соблюдение мер предосторожности в веб-сайтах. Приведены примеры защиты информации и сохранения конфиденциальности. Приводится ознакомительная настройка параметров безопасности как объект исследования, на сайте [www.aliyaschool.kz](http://www.aliyaschool.kz) указаны защитные данные. Отражены основные стандарты и спецификации защиты информации в веб-сервисах. Задача разработчиков и любого веб-ресурса – уберечь информацию конфиденциального характера от хищения, последствия которого выражаются в изменении или уничтожении контента ресурса. В сети Интернет существует проблема незаконного заимствования (текстового) контента, имеющего коммерческую ценность. Единственный вариант преодоления – не размещать его в свободном доступе. Если это невозможно, необходимо технически и юридически защищать его. Цель работы – показать возможности технической защиты от несанкционированного воспроизведения контента, ее несостоятельность и ее возможности в качестве вспомогательного инструмента, облегчающего последующую защиту в правовом поле. На основании проведенного обзора можно сделать вывод, что дальнейшее развитие таких методов обнаружения уязвимостей и защиты веб-приложений может пойти по пути соединения возможностей различных методик

**Ключевые слова:** веб-сервис, сайт, несанкционированный доступ, конфиденциальность информации, система защиты, аутентификация, идентификация, авторизация, разграничение прав доступа, сеть, протокол обмена, атака, инцидент.

**О.А. Ussatova<sup>1\*</sup>, А.Ш. Barakova<sup>2</sup>**

<sup>1</sup>Institute of Information and Computational Technologies, Almaty, Kazakhstan;

<sup>2</sup>Al-Farabi Kazakh National University, Almaty, Kazakhstan.

E-mail: [balia\\_79@mail.ru](mailto:balia_79@mail.ru)

## ANALYSIS OF MODERN WEB RESOURCE PROTECTION SYSTEMS

**Abstract.** An overview of the problems of protecting web resources from the actions of intruders is presented, the basic structure of the Web service is described, the features of the Web environment affecting the protection of the information provided are given, possible threats are systematized and analyzed, measures are developed to eliminate the identified vulnerabilities of web services. The relevance of this topic is due to the fact that, despite the high progress in the field of system security, many systems, including websites, can still be hacked by intruders. Most modern information systems are created in the form of Web sites, so special attention should be paid to security. The purpose of this work is to study the issues that relate to the methods of comprehensive protection of the website from hacker attacks. The main aspects of security and compliance with precautions in websites are considered. Examples of information protection and confidentiality preservation are given. An introductory setting of security parameters as an object of research on the site is given [www.aliyaschool.kz](http://www.aliyaschool.kz) indicates the security data. The main standards and specifications of information protection in web services are reflected. The task of developers and any web resource is to protect confidential information from theft, the consequences of which are expressed in changing or destroying the content of the resource. There is a problem of illegal borrowing of (text) content with commercial value on the Internet. The only way to overcome it is not to place it in the public domain. If this is not possible, it is necessary to technically and legally protect it. The purpose of the work is to show the possibilities of technical protection against unauthorized reproduction of content, its inconsistency and its capabilities as an auxiliary tool that facilitates subsequent protection in the legal field. Based on the review, it can be concluded that the further development of such methods of vulnerability detection and protection of web applications may follow the path of combining the capabilities of various techniques.

**Key words:** web-service, website, unauthorized access, information confidentiality, security system, authentication, identification, authorization, access rights differentiation, network, exchange Protocol, attack, incident.

**Кіріспе.** Қазіргі заманғы ақпараттық жүйелердің басым көпшілігі веб-сайттар ретінде құрылады, сондықтан қауіпсіздікке ерекше назар аудару қажет. Операциялық жүйесі мен бағдарламалық қосымшасы бар құрылғы пайда болған соң, ол бірден тәртіп бұзушылардың қызығушылығын тудырады. Олар оны зерттей бастайды және оны бұзуға күш жұмсайды. Бүгінгі күні веб-сервистерді қорғау барлық ұйымдарды алаңдатады, себебі қасақана субъектілер оны рұқсатсыз пайдалану мақсатында жеке немесе заңды тұлға туралы кез келген ақпаратты алуға ұмтылады.

Бүгінде барлық ұйымдар (шағын бизнес секторының аздаған үлесін қоспағанда) өз бизнесін тек нақты нарық кеңістігінде ғана емес, қолжетімді веб-сервистер яғни интернет желісінде де жүргізеді. Веб сайттар арқылы клиенттерге, серіктестерге, әлеуетті клиенттерге тапсырыс беру, ынтымақтастық, өтінім беру, «жедел желі» туралы хабарлау, консалтинг және т.б. қызметтерін ұсына алады. [1]

Әлемдік және отандық экономиканы трансформациялаудың қазіргі кезеңі коммерциялық қызмет пен цифрлық технологиялар арасындағы интеграциялық процестерді күшейтуге ықпал етеді, олардың соңғысы бизнес субъектілерінің қарқынды дамуының басты факторы болып табылады. Осы үрдіс шеңберінде ақпараттық технологияларды дамыту, зияткерлік технологияларды әзірлеу, кәсіпорындардың бизнес-процестерін жетілдіру шеңберінде жоғары зияткерлік инновацияларды іс жүзінде қолдану және халық ретінде пайдаланылатын әлеуметтік желілерді дамыту сияқты процестер қадағаланады. [2]

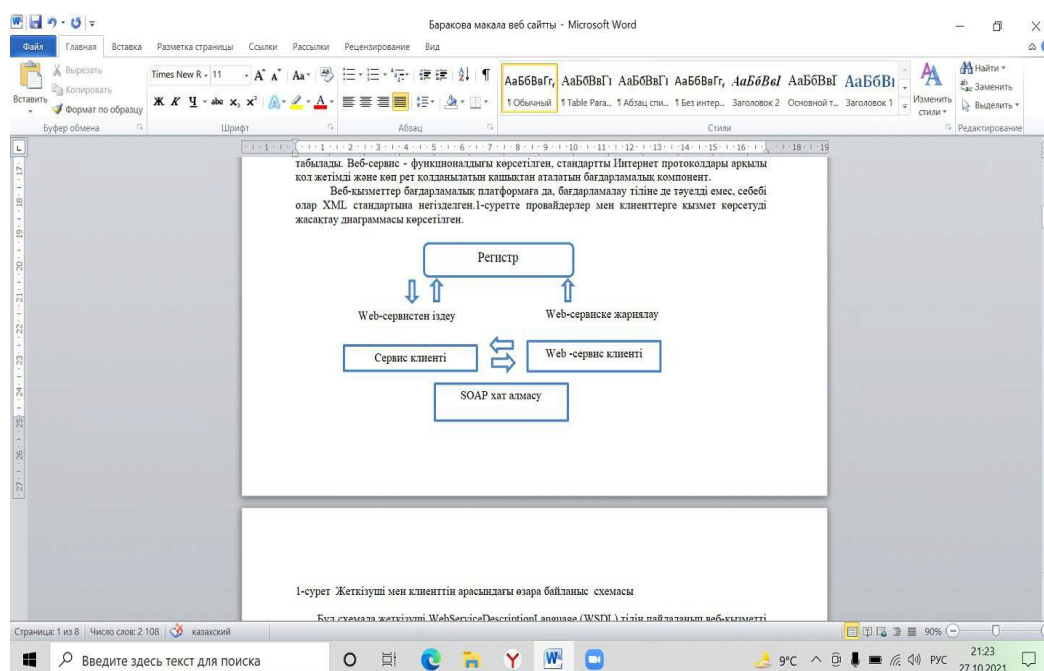
Соңғы процестердің бірі-ақпараттық деректерді жинау, өңдеу, талдау және сақтау бойынша ұйымдардың қызметін жетілдіретін ұйымның ақпараттық қауіпсіздігінің кешенді жүйесінің бөлігі ретінде цифрлық технологияларды дамыту.

**Зерттеу мақсаты.** Мақаланың мақсаты – ақпарат түрлі веб - ресурстар мен түрлі алаңдарда аутентификациялау кезінде алаяқтық операциялардың және жеке деректерді ұрлау жөніндегі заңсыз әрекеттердің объектісіне айналмауға негізделген

**Негізгі мақала материалы.** Веб-сервистің құрылымдық бөлімшесі - веб-сайт болып табылады. Ал веб-сервис - функционалдығы көрсетілген, стандартты протоколдар арқылы қолжетімді және көп рет қолданылатын, интернет арқылы қашықтықтан басқарыла аталатын бағдарламалық компонент.

Веб-сервис шеңберінде өзара іс-қимылды ұйымдастыру үшін қажетті кез келген ақпарат шабуылдаушыға қолжетімді болуы мүмкін. Демек, бүгінгі күні веб-қызметтерді қорғау проблемасы өте өзекті болып отыр. [3]

Веб-сервистер бағдарламалық платформаға да, бағдарламалау тіліне де тәуелді емес, себебі олар XML стандартына негізделген.1-суретте провайдерлер мен клиенттерге қызмет көрсетуді жасақтау диаграммасы көрсетілген.



1-сурет жеткізуші мен клиенттің арасындағы өзара байланыс схемасы



Бұл схемада жеткізуші веб Web Services Description Language (WSDL) тілін пайдаланып веб-қызметті сипаттайды және WSDL көмегімен құрылған құжатты Веб сервиске тіркеп, жариялайды. Ішкі құрылғылар мен тіркелімнің интерфейстері UDDI (Әмбебап сипаттама ашу және интеграциялау) стандартымен сипатталады. Құжат деректерінің мекен жайын пайдалана отырып клиент қажетті веб-сервистен табады. Содан кейін клиент провайдерден веб-қызметті алады, онымен SOAP хаттамасы. (SOAP ағылш. SimpleObjectAccessProtocol - нысандарға кірудің қарапайым хаттамасы) арқылы веб-сервистер өзара және сыртқы қосымшалармен сонымен қатар әр түрлі веб-сервистермен хабар алмасады. [4]

Жоғарыда көрсетілген диаграммада оларды қорғауға әсер ететін веб-сервис ортасының ерекшеліктері көрсетілген.

Сондай ерекшеліктерге мыналар кіреді:

- деректердің жоғары қолжетімділігі - веб-қызметтер шын мәнінде біртекті емес қосымшалардың қолжетімділігі мен тұтастығын арттыру үшін әзірленеді;
- басқа веб-сервистермен қосымшаларға байланысуға қандай да бір физикалық шекараларымен шектелмейді;
- мәліметтер алмасу интернет арқылы жалпыға қолжетімді өтеді, ол шабуылдаушыларға оларды ұстап қалу үшін алдыңғы қатарлы мүмкіндіктерді береді;
- көптеген деректер XML форматта беріледі;
- хабарларды топтық адрестеу мүмкіндігі, бұл уникастты беруге бағдарланған ақпараттық қауіпсіздік құралдарын қолдануды қиындатады;
- әлсіз аймаққа DoS-қа сәтті шабуыл жасаған жағдайда көптеген веб-қызметтерді бірден ажыратуға мүмкіндік беретін веб-сервистер архитектурасының аса осал компоненттерінің, атап айтқанда регистрлердің болуы; [5]
- веб-сервистерді іске асыруға адамның ең аз қатысуы - пайдаланушылардың көпшілігі үшін олар «қара» жәшіктер болып көрінеді.

Веб-сервистер - компьютерлерге интернет арқылы деректер алмасуға және бизнес-функциялар мен операцияларды орындауға мүмкіндік беретін XML тіліне негізделген халықаралық стандарттарға арналған жалпы термин. Веб-қызметтердің негізгі функциялары браузерлер арқылы компьютерлерге көзбен шолудан басқа қол жеткізу үшін ақпараттық қызметтер жасауға мүмкіншілік береді. Веб-сервистер айтарлықтай қуатты және жүйелі бөлімдер мен компаниялар шеңберінде өзара іс-қимылды қамтамасыз етуге қабілетті.

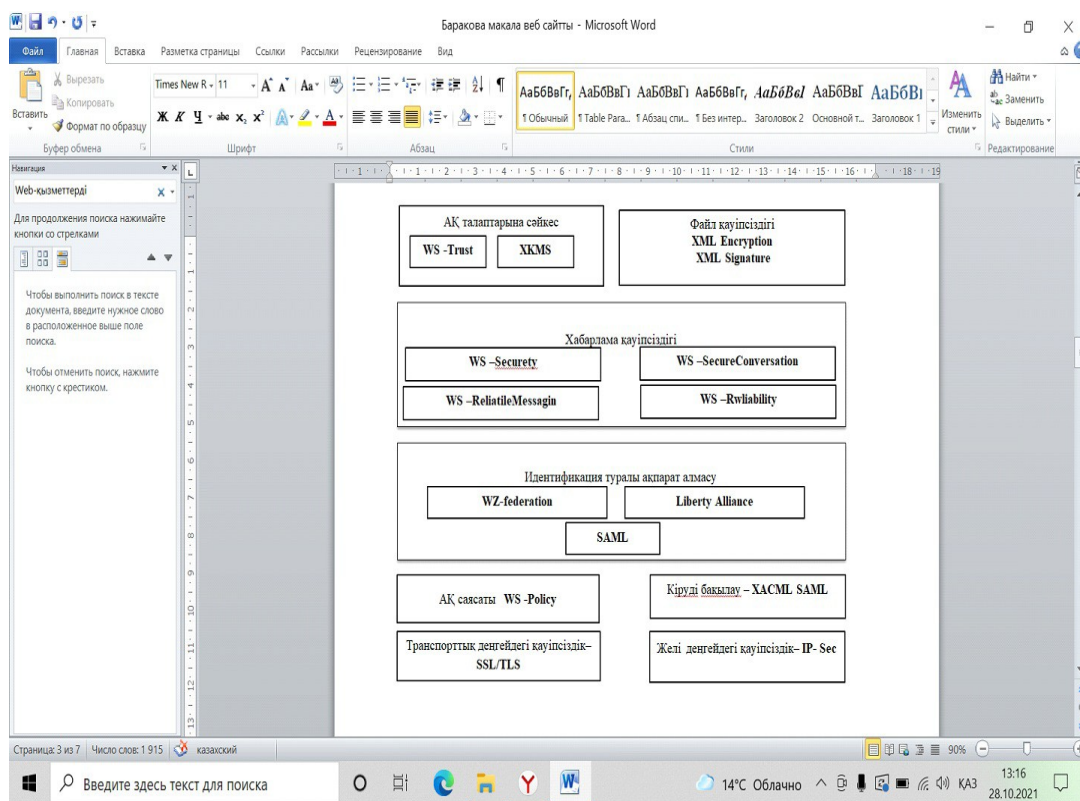
Веб-қызметтердің негізгі компоненттері мыналар болып табылады:

- қызмет көрсетілетін қосымшалар сервері;
- сервис интерфейсі;
- WSDL- дегі интерфейссті сипаттайтын деректер қоймасы немесе WSDL сипаттамасы бар анықтама керек себебі веб сервис клиенттері интерфейссті табу үшін
- веб-қызметті пайдаланғысы келетін веб-сервис клиенті;
- веб-сервис клиентіне қызметпен байланыс жасауға мүмкіндік беретін байланыс хаттамасы (объектіге қол жеткізудің қарапайым хаттамасы, яғни SOAP).

Веб-қызметті құрайтын «анықтамалардың» саны көп, бірақ әдетте қабылданған анықтама – W3C SOAP арқылы ақпаратты ашатын ақпараттық қызмет [6]. SOAP интерфейсінң клиенті осы ақпараттық қызметтерге қалай қол жеткізу керектігін білуі тиіс. Бұл қатынасты басқа W3C стандарты, Веб Services сипаттама тілі (WSDL) форматында сипаттауға болады. SOAP негізіндегі қызмет провайдерлері WSDL файлдарын жариялайды

Веб-сервистердің ақпараттық қауіпсіздігін қамтамасыз ету жалпыға бірдей қабылданған ақпараттық қауіпсіздік технологиялары - шифрлауды, цифрлық қолтаңбаларды, құпия сөзді қорғауды және т.б. пайдалануды көздейді. Веб-қызметтердің ақпараттық қауіпсіздік стандарттары ақпараттық қауіпсіздік веб-қызметтерінің нақты архитектурасына сәйкес келеді деп айтуға болады, бірақ бұл архитектураны іске асыру тетіктері өте дәстүрлі.

Қазіргі уақытта веб-сервистердің ақпараттық қауіпсіздігін қамтамасыз етудің бірқатар стандарттары мен спецификациялары әзірленді. 2-суретте веб-қызметтердің ақпараттық қауіпсіздігінің негізгі стандарттары мен техникалық сипаттамалары диаграммада көрсетіледі.



2 сурет Веб-сервистердегі ақпараттарды қорғаудың негізгі стандарттары мен спецификасы

Ең танымал стандарттардың бірі WS-Security болып табылады, ол SOAP хабар алмасу ортасындағы аутентификация және авторизация процестерін сипаттайды.

WS-Security пайдаланушының аутентификациясын логин/пароль жұбын, X.509 сертификатын немесе Kerberos хаттамасын пайдалана отырып қамтамасыз етеді. Осы технологияларда хабардың тұтастығын тексеруге мүмкіндік беретін сандық қолтаңба іске асырылады. Сондай-ақ, WS-Security қызметкерлері SOAP хабарламаларын шифрлауға, SOAP ортасында XML шифрлау стандартын пайдалану тетіктерін анықтауға мүмкіндік жасады. [7]

Веб-қызметтерді қорғау жан-жақты болуы тиіс: ақпараттық қауіптерден тек SOAP хабарламалары ғана емес, сонымен қатар Веб-қызметтер архитектурасының барлық басқа компоненттері де қорғалуы тиіс:

- олардың интерфейстері;
- сервистік анықтау құралдары (регистрлер) және т.б.

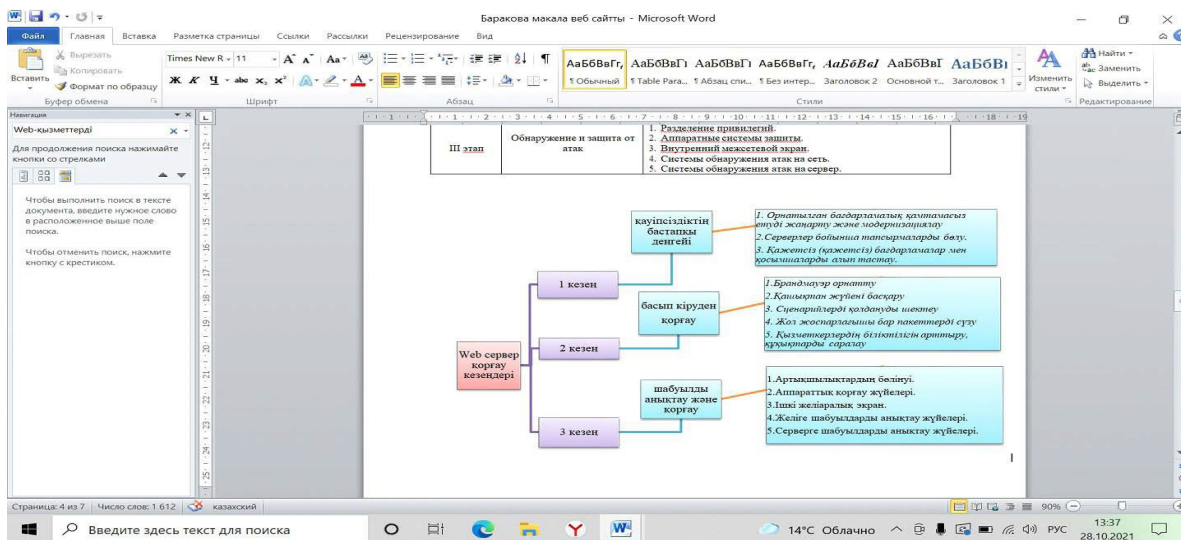
Бүгінде веб-сервистердің ақпараттық қауіпсіздігін стандарттау саласы үнемі дамып, жетілдіріліп отырады, осыған байланысты ақпаратты қорғаудың жоғары деңгейін қамтамасыз ету үшін стандарттар мен ерекшеліктердің соңғы нұсқаларын пайдалануды ұсынамыз. [8]

Ұйымдардың көпшілігі деректерінің көлеміне қарамастан, қауіпсіздіктің негізгі элементтерін қамтамасыз ете отырып, өз учаскелерінің дизайнына, функционалдығына және алға жылжуына көп көңіл бөлінеді. Соңғы кездері корпоративтік веб-сайттарды бұзған актілер жиілеп кетті, бұл әлсіз қорғауды, сондай-ақ бір немесе бірнеше серверлерді шамадан тыс жүктеу веб-серверлердің істен шығуына әкелуі мүмкін екенін көрсетеді.

Төменде шабуылдардың алдын алу немесе олардың салдарын жою мақсатында веб-серверлерді қорғау қадамдары көрсетілген. Сипатталған әдістерді қолдану өте қарапайым. Демек, кез келген ұйым оларды қабылдай алады.

Веб-серверлер интернеттің негізі болып табылады. Веб-серверлер үшін қауіпсіздік жүйенің елеулі бөлігі болып табылады. Серверлер пайдаланушылармен ақпарат алмасуға арналғандықтан осал болып табылады. Сондықтан хакерлер серверге немесе дерекқор кодына өзгерістер енгізе алады [9]. Веб-серверлерді қорғау үшін сайт әкімшілерінің, бағдарламашылар мен дизайнерлердің бірлескен жұмысы қажет. Сондай-ақ, бағдарламалық қамтамасыз етуді орнату қажет: антивирус, қолжетімділік құқықтарын тарату және т.б.

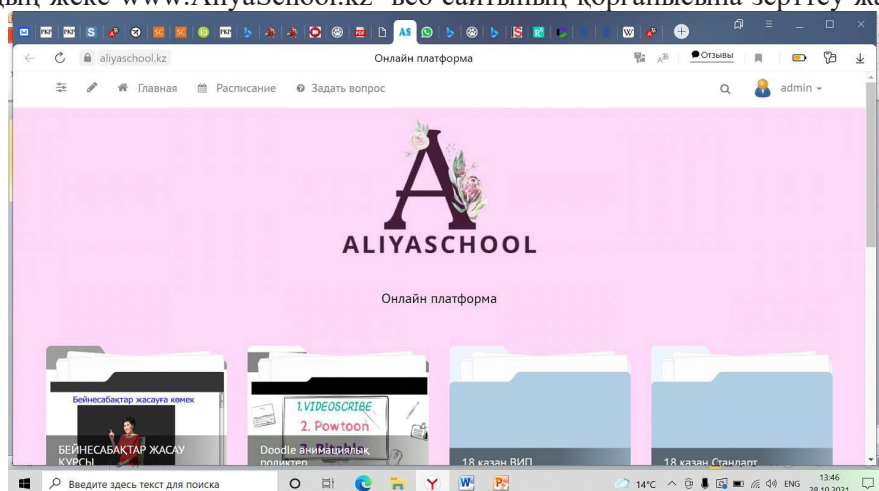
Веб-сервер қауіпсіздігінің 3 кезеңін ажыратқан дұрыс.



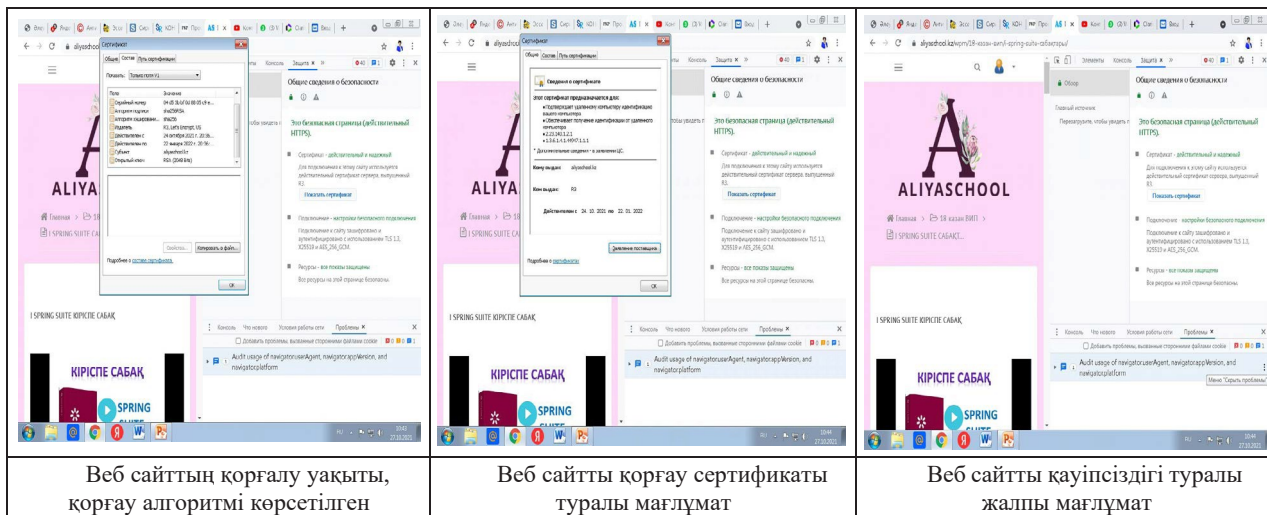
3 сурет веб-серверді қорғаудың кезеңдері

Бұл схемадан веб-серверді сапалы қорғауды қамтамасыз ету үшін сапалы бағдарламалық қамтамасыз етуді пайдалану қажет. [10] Сондай-ақ жүйені немесе жекелеген компоненттерді үнемі жаңартып отыру қажет. Веб-қызметтің қауіпсіздігін қамтамасыз ету үшін желі әкімшілері білікті болуы тиіс. Веб-сервер қауіпсіздігінің негізі веб-сайттарға қызмет көрсету болып табылады.

Автордың жеке [www.AliyaSchool.kz](http://www.AliyaSchool.kz) веб сайтының қорғанысына зерттеу жасаймыз



4 сурет [www.AliyaSchool.kz](http://www.AliyaSchool.kz) сайтының негізгі беті



Веб сайттың қорғалу уақыты, қорғау алгоритмі көрсетілген

Веб сайтты қорғау сертификаты туралы мағлұмат

Веб сайтты қауіпсіздігі туралы жалпы мағлұмат

5 сурет [www.AliyaSchool.kz](http://www.AliyaSchool.kz) веб – сайтының қорғау мәліметтері



Зерттелген [www.AliyaSchool.kz](http://www.AliyaSchool.kz) сайттан көретініміз қорғауға қолданылған алгоритм sha256RSA, Сертификат мерзімі 24.10.2021 жылдан 22.01.2022 жылға дейінгі аралықта, қорғалу хаттамасы HTTPS, TLS 1.3 сертификатымен қорғалғандығын көрсетеді. SHA – 2 (Secure Hash Algorithm 2) - хэш алгоритмдерінің ең танымал бірі. [11] SHA-2-бұл деректерді хэштеу идеясы бар алгоритмдер тобы. SHA-256 SHA-2 алгоритмінің әрекетін анықтайтын қосымша тұрақтыларды орнатады. Осындай тұрақтылардың бірі - шығыс өлшемі. “256” және “ 512 “ биттердегі тиісті шығыс өлшемдеріне жатады. Ал HTTPS (аббр. ағылшын тілінен. HyperText Transfer Protocol Secure) - қауіпсіздікті арттыру мақсатында шифрлауды қолдау үшін HTTP хаттамасын кеңейту. HTTPS жеке хаттама емес. Бұл SSL және TLS шифрланған транспорт механизмдері арқылы жұмыс істейтін қарапайым HTTP . Ол желілік қосылымды тыңдауға негізделген шабуылдардан қорғауды қамтамасыз етеді – шифрлар мен сервер сертификаты тексеріліп, оған сеніп тапсырылған жағдайда, сифферлік шабуылдардан және man-in-the-middle типті шабуылдардан қорғайды. [12]

**Қорытынды.** Қазіргі статистикаға қарасақ веб-қосымшаларға шабуылдардың үнемі өсіп келе жатқан көрсетеді – жүйенің бұзылу жағдайлары 80%-ы веб-қосымшадан басталады. Шабуыл құралдары мен әдістерінің көбеюі сайттың қол жетімділігін қамтамасыз ету, веб-қосымшаны немесе оның компоненттерін бұзу мен мазмұнды өзгертуден қорғау қиынға соғады. Техникалық мамандар мен әзірлеушілердің күш-жігеріне қарамастан, қорғаныс жағы веб-қосымшаның бұзылуынан кейін қорғаныс шараларын қолдана отырып, әдеттегідей ұстанымға ие болады. Веб-сайттар ашық қолжетімділікке, әрдайым сапалы жазылмаған кодқа, серверлік бөлікті баптауда қателіктердің болуына, сондай-ақ ақ қызметі тарапынан бақылаудың болмауына байланысты шабуылдарға ұшырайды, осылайша зиянкестерге сыни деректерге қолжетімділікті қамтамасыз етеді. [13]

Мақалада зиянкестер белсенді пайдаланатын неғұрлым кең таралған осалдықтар, сондай-ақ оларға қарсы іс-қимылдың тиімді әдістері қаралатын болады. Веб-сайттарды сапалы қорғауды қамтамасыз ету үшін сапалы бағдарламалық қамтыма пайдалану қажет. Сондай-ақ, жүйені немесе жеке компоненттерді үнемі жаңартып отыру қажет. Желі әкімшілері Веб-сайттың қауіпсіздігін қамтамасыз ету үшін тиісті біліктілікке ие болуы тиіс. Веб - сервистер қауіпсіздігінің негізін веб-сайттарға қызмет көрсету құрайды. Қорытындылай келе конфиденциальды ақпаратты қорғауда бағдарламалық қорғау жасақтамасын құралдарын пайдалану өте өзекті болып табылады. Өз сайтыңызды қорғау - маңызды міндеттердің бірі болып тұр қазіргі таңда. [14 ] Егер сіз оған ерекше назар аудармасаңыз сіз материалдық жағынан да, саяси жағынан да көптеген шығындарға дұшар боласыз. Осыған байланысты, бұл зиянкестердің Web-сайттарға шабуыл жасауға деген қызығушылығы қазір де қалыс қалмайды (егер барлық зиянды деп есептесек іс-әрекеттер заңмен жазаланады), әзірлеушілерге: ең алдымен оның қауіпсіздігі туралы ойланға тура келеді. Көптеген веб-сайттарды қорғау құралдары бар бірақ олар қандай болса Web-сайттар әлсіздік таныстуы мүмкін. Web-сайттарды әзірлеушілер мен әкімшілер ақпараттың сенімділік және қауіпсіздігіне өте жоғары деңгейде назар аударғаны дұрыс. [15] Қазіргі заманғы қорғау құралдарын енгізу ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі іс-шаралардың ажырамас бөлігі болып табылады.

#### Information about the authors:

**O.A. Usatova** – PhD, Institute of Information and Computing Technologies, [uoa\\_olga@mail.ru](mailto:uoa_olga@mail.ru), Almaty, Kazakhstan;

**A.Sh. Barakova** – PhD doctoral student, Al-Farabi Kazakh National University, [balia\\_79@mail.ru](mailto:balia_79@mail.ru), Almaty, Kazakhstan.

#### ӘДЕБИЕТТЕР

- [1] Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность и защита информации //Учебник , 2009г, с. 184 –186.
- [2] Бегимбаева Е., Усатова О., Бияшев Р., Нысанбаева С. Development of an automated system model of information protection in the cross-border exchange, // Cogent Engineering Journal, Birmingham, UK , №7, 2020 г., ISSN: 2331-1916, P.1-13; DOI:10.1080/23311916.2020.1724597 Процентиль важности: 69.
- [3] Крис Митчелл, Артем Конев. Обеспечение безопасности веб-сайтов.//Australia: SophosLabs. [Электронный ресурс]. URL:<http://help.yandex.ru/webmaster/protecting-sites/contents.xml>.
- [4] Simple Object Access Protocol (SOAP)1.1 [Электронный ресурс] URL: <http://www.w3.org/TR/2000/NOTE-SOAP-20000508>.
- [5] DDoS атаки и малый бизнес [Электронный ресурс]. URL: [http://bezshablona.ospfmon.com/2014/02/ddos\\_4866.html?m](http://bezshablona.ospfmon.com/2014/02/ddos_4866.html?m)
- [6] Запечников С.В. Информационная безопасность открытых систем. //М.: ГИТ, 2016. Т. 1. с.536-537
- [7] J. Holgersson and E. Soderstrom, “Web service security - vulnerabilities and threats within the context of WS-security,” The 4th Conference on Standardization and Innovation in Information Technology, 2005, pp. 138-146, DOI:10.1109/SIPT.2005.1563803.

- [8] Мерсер Д.//Создание надежных и полнофункциональных веб-сайтов, блогов, форумов, порталов и сайтов-сообществ. Вильямс – М., 2018. С.272-274.
- [9] Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие. М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2017. С.416 - 418.
- [10] Moldovyan A.A., Zima V.M., Moldovyan N.A. Security of global network technologies. The 2nd ed. 2014. 362 pp.
- [11] Прохоренко В., Чу К.-К. Р., Ашман Х. Контекстно-ориентированная модель защиты веб-приложений // Прикладная математика и вычисления. 2016. Том 285. С. 59-78.
- [12] <https://www.securitylab.ru/news/524358.php> .
- [13] А.М., Дафа-Аллах А., Эльханг А.А.М. Предлагаемая модель безопасности для веб-приложений и сервисов // Международная конференция по связи, управлению, вычислительной технике и электронике 2017 (ICCCCEE), — 2017. Стр. 1-6.
- [14] Дипа Г., Тилагам П. С. Защита веб–приложений от уязвимостей, связанных с внедрением и логикой: подходы и проблемы // Информационные и программные технологии. 2016. Том 74. С. 160- 180.
- [15] Верма А.К. Классификация атак SQL-инъекций с использованием нечеткого заражения // Достижения в области интеллектуальных систем и вычислений. 2018. Том. 518. С. 463-469.

#### REFERENCES

- [1] V.P. Melnikov, S.A. Kleimenov, A.M. Petrakov //”Information security and information protection”– 2009 - p. 184- 186. (In Russian).
- [1] Begimbayeva Yenlik, Ussatova Olga, Biyashev Rustem, Nyssanbayeva Saule. Development of an automated system model of information protection in the cross-border exchange // Cogent Engineering Journal, Birmingham, UK , №7, 2020 г.,ISSN: 2331-1916, P.1-13; DOI:10.1080/23311916.2020.1724597.
- [3] Chris Mitchell. Artem Konev. Ensuring the security of websites. // Australia: SophosLabs. [Electronic resource]. URL: <http://help.yandex.ru/webmaster/protecting-sites/ contents.xml>.
- [4] Simple Object Access Protocol (SOAP) 1.1 [Electronic resource]. URL <http://www.w3.org/TR/2000/NOTE-SOAP - 20000508>.
- [5] DDoS attacks and small business [Electronic resource]. URL: [http://bezshablona.ospfmon.com/2014/02/ddos\\_4866.html?m](http://bezshablona.ospfmon.com/2014/02/ddos_4866.html?m) (In Russian).
- [6] Zachepnikov S.V. Information security for open systems. //М.: GLT, 2016. Vol. 1. 536 p.
- [7] J. Holgersson and E. Soderstrom, “Web service security - vulnerabilities and threats within the context of WS-security,” The 4th Conference on Standardization and Innovation in Information Technology, 2005., 2005, p. 138-146, **DOI:** 10.1109/SIIT.2005.1563803.
- [8] Mercer D. Creation of reliable and fully functional websites, blogs, forums, portals and community sites. Williams - M., 2018. 272 p. (In Russian).
- [9] Shangin V.F. Information security of computer systems and networks: textbook. Moscow: ID FORUM, SICINFRA-M,2017.416p. (In Russian).
- [10] Moldovyan A.A., Zima V.M., Moldovyan N.A. Security of global network technologies. The 2nd ed. 2014. 362 pp.
- [11] Prokhorenko V., Choo K.-K. R., Ashman H. Context-oriented web application protection model // Applied Mathematics and Computation. 2016. Vol. 285. P. 59–78.
- [12] <https://www.securitylab.ru/news/524358.php>.
- [13] А.М., Дафа-Аллах А., Elhang A.A.M. Proposed security model for web based applications and services // International Conference on Communication, Control, Computing and Electronics Engineering 2017 (ICCCCEE), – 2017. P. 1–6.
- [14] Deepa G., Thilagam P. S. Securing Web applications from injection and logic vulnerabilities: Approaches and challenges // Information and Software Technology. 2016. Vol. 74. P. 160 – 180.
- [15] Verma A. K. Classification of SQL injection attacks using fuzzy tainting // Advances in Intelligent Systems and Computing. 2018. Vol. 518. P. 463 – 469.



## СОДЕРЖАНИЕ

### ИНФОРМАТИКА

<b>Ж.С. Абдимуратов, В.И. Дмитриченко, М.А. Джетписов, Е.Н. Жагыпаров</b> АДАПТАЦИЯ ЗАЩИТЫ РЕЛЕ ЭЛЕКТРОДВИГАТЕЛЯ ПРИ ПРОЕКТИРОВАНИИ ЦИФРОВЫХ ПОДСТАНЦИЙ В РЕСПУБЛИКЕ КАЗАХСТАН. ....	6
<b>Ж.С. Авкурова, Б.К. Абдураимова, С. Гнатюк, Л.М. Кыдыралина</b> МОДЕЛЬ ПАРАМЕТРОВ ДЛЯ РАННЕГО ВЫЯВЛЕНИЯ АРТ-АТАК И ИДЕНТИФИКАЦИИ НАРУШИТЕЛЕЙ БЕЗОПАСНОСТИ В КИБЕРПРОСТРАНСТВЕ. ....	17
<b>Т.С. Байшоланов, Ж.М. Алимжанова, Н. Байшолан, К.Е. Кубаев, К.С. Байшоланова</b> ОЦЕНКА СТОЙКОСТИ КРИПТОГРАФИЧЕСКИХ ШИФРОВ С ПОМОЩЬЮ АНАЛИЗА ШИФРТЕКСТОВ.....	26
<b>Ж.С. Есенгалиева, К.Н. Касылкасова, А.О. Касылкасова</b> АНАЛИЗ МЕДИЦИНСКИХ ПРИЛОЖЕНИЙ, СОЗДАННЫХ СПЕЦИАЛЬНО ДЛЯ БОРЬБЫ С COVID-19.....	34
<b>Ж.С. Иксебаева, К. Жетписов, Ж.М. Муратова</b> РАЗРАБОТКА КОНЦЕПТУАЛЬНОЙ МОДЕЛИ АВТОМАТИЧЕСКОЙ ПРОВЕРКИ ТЕХНИЧЕСКОЙ ДОКУМЕНТАЦИИ. ....	43
<b>В.А. Лахно, Б.С. Ахметов, М.Б. Ыдырышбаева, Ш. Сагындыкова</b> ПРИМЕНЕНИЕ СЕТИ БАЙЕСА СО СКРЫТЫМИ ВЕРШИНАМИ В СЕКТОРАЛЬНЫХ СППР ДЛЯ ЗАДАЧ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ. ....	50
<b>О.Ж. Мамырбаев, Д.О. Оралбекова, К. Алимхан, М. Othman, Б. Жумажанов</b> ПРИМЕНЕНИЕ ГИБРИДНОЙ ИНТЕГРАЛЬНОЙ МОДЕЛИ ДЛЯ РАСПОЗНАВАНИЯ КАЗАХСКОЙ РЕЧИ.....	58
<b>А.Р. Оразаева, Д.А. Тусупов, С.В. Павлов, Г.Б. Абдикеримова</b> ЭФФЕКТИВНОСТЬ ОБРАБОТКИ БИОМЕДИЦИНСКИХ ИЗОБРАЖЕНИЙ РАКА МОЛОЧНОЙ ЖЕЛЕЗЫ С ИСПОЛЬЗОВАНИЕМ ФИЛЬТРОВ.....	69
<b>Ж.М. Ташенова, Э.Н. Нурлыбаева, Ж.К. Абдугулова, Ш.А. Аманжолова</b> МЕТОДЫ БЕЗОПАСНОСТИ И ШИФРОВАНИЯ В ОБЛАЧНОЙ СИСТЕМЕ.....	77
<b>О.А. Усатова, А.Ш. Баракова</b> АНАЛИЗ СОВРЕМЕННЫХ СИСТЕМ ЗАЩИТЫ ВЕБ-РЕСУРСОВ. ....	88
<b>Г.С. Ыбыгаева, Н.Ф. Хайрова, К.Ж. Мухсина, Б.Ж. Жумажанов</b> ОБЗОР ПРОБЛЕМ ИСПОЛЬЗОВАНИЯ И ФОРМИРОВАНИЯ ЛИНГВИСТИЧЕСКИХ ОНТОЛОГИЙ. ....	96
<b>К.С. Чезимбаева, М.Ж. Батырова</b> ИЗУЧЕНИЕ ВЛИЯНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА НА СЕТЬ ПЕРЕДАЧИ ДАННЫХ (IOT) ДЛЯ МОДЕЛИРОВАНИЯ УМНОГО ДОМА. ....	107

## ФИЗИКА

<b>Г.Б. Абдраманова, О. Имамбек, А.М. Надир, М.Б. Мырзабаева</b> УПРУГОЕ РАССЕЙЯНИЕ ПРОТОНОВ НА ЯДРЕ ${}^3\text{He}$ ПРИ ПРОМЕЖУТОЧНЫХ ЭНЕРГИЯХ.....	117
<b>А.Е. Амантаева, Г.Р. Сүбебекова, А.Т. Агишев, С.А. Хохлов</b> ОПРЕДЕЛЕНИЕ ФУНДАМЕНТАЛЬНЫХ ПАРАМЕТРОВ КАТАКЛИЗМИЧЕСКОЙ ПЕРЕМЕННОЙ ЗВЕЗДЫ ПРОМЕЖУТОЧНОГО ПЕРИОДА V1239 HERCULES.....	124
<b>Т.Н. Исмагамбетова, М.Т. Габдуллин, Т.С. Рамазанов</b> СТРУКТУРНЫЕ И ТЕРМОДИНАМИЧЕСКИЕ СВОЙСТВА ДВУХКОМПОНЕНТНОЙ ПЛОТНОЙ ВОДОРОДНОЙ ПЛАЗМЫ. ....	131

## МАЗМҰНЫ

### ИНФОРМАТИКА

<b>Ж.С. Абдимуратов, В.И. Дмитриченко, М.А. Джетписов, Е.Н. Жагыпаров</b> ҚАЗАҚСТАН РЕСПУБЛИКАСЫНДАҒЫ ЦИФРЛЫҚ ҚОСАЛҚЫ СТАНЦИЯЛАРДЫ ЖОБАЛАУ КЕЗІНДЕ ҚОЗҒАЛТҚЫШТЫҢ РЕЛЕЛІК ҚОРҒАНЫСЫН БЕЙІМДЕУ .....	6
<b>Ж.С. Авкурова, Б.К. Абдураимова, Б. Гнатюк, Л.М. Қыдыралина</b> АРТ-ШАБУЫЛДАРДЫ ЕРТЕ АНЫҚТАУҒА ЖӘНЕ КИБЕРКЕҢІСТІКТЕГІ ҚАУІПСІЗДІК БҰЗУШЫЛАРЫН АНЫҚТАУҒА АРНАЛҒАН ПАРАМЕТРЛЕР МОДЕЛІ .....	17
<b>Т.С. Байшоланов, Ж.М. Алимжанова, Н. Байшолан, К.Е. Кубаев, К.С. Байшоланова</b> ШИФРМӘТІНДІ ТАЛДАУ АРҚЫЛЫ КРИПТОГРАФИЯЛЫҚ ШИФРЛАРДЫҢ ТҰРАҚТЫЛЫҒЫН БАҒАЛАУ .....	26
<b>Ж.С. Есенғалиева, К.Н. Касылқасова, А.О. Касылқасова</b> COVID-19-БЕН КҮРЕСУ ҮШІН АРНАЙЫ ЖАСАЛҒАН МЕДИЦИНАЛЫҚ ҚОСЫМШАЛАРДЫ ТАЛДАУ .....	34
<b>Ж.С. Иксебаева, К. Жетписов, Ж.М. Муратова</b> ТЕХНИКАЛЫҚ ҚҰЖАТТАМАНЫ АВТОМАТТЫ ТҮРДЕ ТЕКСЕРУДІҢ ТҰЖЫРЫМДАМАЛЫҚ МОДЕЛІН ӨЗІРЛЕУ .....	43
<b>В.А. Лахно, Б.С. Ахметов, М.Б. Ыдырышбаева, Ш. Сагындыкова</b> КИБЕРҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУ ҮШІН СЕКТОРАЛДЫ ШҚҚЖ - ДЕ ЖАСЫРЫН ТӨБЕЛЕРІ БАР БАЙЕС ЖЕЛІСІН ҚОЛДАНУ .....	50
<b>О.Ж. Мамырбаев, Д.О. Оралбекова, Қ. Әлімхан, М. Othman, Б. Жумажанов</b> ҚАЗАҚША СӨЙЛЕУДІ ТАҢУ ҮШІН ГИБРИДТІ ИНТЕГРАЛДЫҚ МОДЕЛЬДЕРДІ ҚОЛДАНУ .....	58
<b>А.Р. Оразаева, Д.А. Тусупов, С.В. Павлов, Г.Б. Абдикеримова</b> СҮТ БЕЗІ ҚАТЕРЛІ ІСІГІНІҢ БИОМЕДИЦИНАЛЫҚ КЕСКІНДЕРІН СҮЗГІЛЕРДІ ПАЙДАЛАНА ОТЫРЫП ӨНДЕУ ТИІМДІЛІГІ .....	69
<b>Ж.М. Ташенова, Э.Н. Нурлыбаева, Ж.К. Абдугулова, Ш.А. Аманжолова</b> БҰЛТТЫҚ ЖҮЙЕДЕГІ ҚАУІПСІЗДІК ЖӘНЕ ШИФРЛАУ ӘДІСТЕРІ .....	77
<b>О.А. Усатова, А.Ш. Баракова</b> ҚАЗІРГІ ЗАМАНҒЫ ВЕБ-РЕСУРСТАРДЫ ҚОРҒАУ ЖҮЙЕЛЕРІН ТАЛДАУ .....	88
<b>Г.С. Ыбығтаева, Н.Ф. Хайрова, К.Ж. Мухсина, Б.Ж. Жумажанов</b> ЛИНГВИСТИКАЛЫҚ ОНТОЛОГИЯНЫ ҚОЛДАНУ ЖӘНЕ ҚАЛЫПТАСТЫРУ МӘСЕЛЕЛЕРІНЕ ШОЛУ .....	96
<b>К.С. Чезимбаева, М.Ж. Батырова</b> АҚЫЛДЫ ҮЙДІ МОДЕЛЬДЕУ ҮШІН ДЕРЕКТЕР ЖЕЛІСІНЕ (IOT) ЖАСАНДЫ ИНТЕЛЛЕКТ ӨСЕРІН ЗЕРТТЕУ .....	107

## ФИЗИКА

<b>Г.Б. Абдраманова, О. Имамбек, Ә.М. Нәдір, М.Б. Мырзабаева</b> АРАЛЫҚ ЭНЕРГИЯЛАРДАҒЫ ПРОТОНДАРДЫҢ $^3\text{He}$ ЯДРОСЫНАН СЕРПІМДІ ШАШЫРАУЫ .....	117
<b>А.Е. Амангаева, Г.Р. Сүбебекова, А.Т. Агишев, С.А. Хохлов</b> АРАЛЫҚ ПЕРИОДАҒЫ V 1239 HERCULES КАТАКЛИЗМАЛЫҚ АЙНЫМАЛЫ ЖҰЛДЫЗЫНЫҢ ІРГЕЛІ ПАРАМЕТРЛЕРІН АНЫҚТАУ .....	124
<b>Т.Н. Исмагамбетова, М.Т. Габдуллин, Т.С. Рамазанов</b> ЕКІ КОМПОНЕНТТІ ТЫҒЫЗ СУТЕГІ ПЛАЗМАСЫНЫҢ ҚҰРЫЛЫМДЫҚ ЖӘНЕ ТЕРМОДИНАМИКАЛЫҚ ҚАСИЕТТЕРІ .....	131

---

## CONTENTS

### COMPUTER SCIENCE

<b>Zh.S. Abdimuratov, V.I. Dmitrichenko, M.A. Jetpisov, Y.N. Zhagyparov</b> ADAPTATION OF ELECTRIC MOTOR RELAY PROTECTION WHEN DESIGNING DIGITAL SUBSTATIONS IN THE REPUBLIC OF KAZAKHSTAN .....	6
<b>Zh. Avkurova, B. Abduraimova, S. Gnatyuk, L.M. Kydyralina</b> MODEL OF PARAMETERS FOR EARLY DETECTION OF APT ATTACKS AND IDENTIFICATION OF SECURITY INTRUDERS IN CYBERSPACE. ....	17
<b>T.S. Baisholanov, Zh.M. Alimzhanova, N. Baisholan, K.E. Kubayev, K.S. Baisholanova</b> EVALUATION OF THE STRENGTH OF CRYPTOGRAPHIC CIPHERS USING CIPHERTEXT ANALYSIS. ....	26
<b>Zh. Yessengaliyeva, K. Kassylkassova, A. Kassylkassova</b> ANALYSIS OF MEDICAL APPLICATIONS DESIGNED SPECIFICALLY TO COMBAT COVID-19. ....	34
<b>Zh.S. Ixebayeva, K. Jetpisov, Zh.M. Muratova</b> DEVELOPMENT OF A CONCEPTUAL MODEL FOR AUTOMATIC VERIFICATION OF TECHNICAL DOCUMENTATION. ....	43
<b>V.A. Lakhno, B.S. Akhmetov, M.B. Ydyryshbayeva, Sh. Sagyndykova</b> APPLICATION OF A BAYESIAN NETWORK WITH HIDDEN VERTICES IN SECTORAL DSS FOR CYBERSECURITY TASKS. ....	50
<b>O.Zh. Mamyrbayev, D.O. Oralbekova, K. Alimhan, M. Othman, B. Zhumazhanov</b> APPLICATION OF HYBRID END TO END MODELS FOR KAZAKH SPEECH RECOGNITION. ....	58
<b>A.R. Orazayeva, J.A. Tussupov, S.V. Pavlov, G.B. Abdikerimova</b> EFFICIENCY OF PROCESSING BIOMEDICAL IMAGES OF BREAST CANCER USING FILTERS. ....	69
<b>Zh. Tashenova, E. Nurlybaeva, Zh. Abdugulova, Sh. Amanzholova</b> CLOUD SECURITY AND ENCRYPTION METHODS. ....	77
<b>O.A. Ussatova, A.Sh. Barakova</b> ANALYSIS OF MODERN WEB RESOURCE PROTECTION SYSTEMS. ....	88
<b>G.S. Ybytayeva, N.F. Khairova, K.Zh. Mukhsina, B.Zh. Zhumazhanov</b> PROBLEMS OF USING AND FORMING LINGUISTIC ONTOLOGIES: AN OVERVIEW .....	96
<b>K.S. Chezimbayeva, M.Z. Batyrova</b> STUDYING THE IMPACT OF ARTIFICIAL INTELLIGENCE ON THE DATA NETWORK (IOT) FOR SIMULATION OF A SMART HOME. ....	107



## PHYSICS

**G.B. Abdramanova, O. Imambek, F.B. Belisarova**

ELASTIC PROTON SCATTERING BY  $^3\text{He}$  NUCLEI AT INTERMEDIATE ENERGIES. ....117

**A.E. Amantayeva, G.R. Subebekova, A.T. Agishev, S.A. Khokhlov**

DETERMINATION OF THE FUNDAMENTAL PARAMETERS OF CATAclysmic  
VARIABLE PERIOD GAP STAR V1239 HERCULES. ....124

**T.N. Ismagambetova, M.T. Gabdullin, T.S. Ramazanov**

STRUCTURAL AND THERMODYNAMIC PROPERTIES OF A TWO-COMPONENT  
DENSE HYDROGEN PLASMA. ....131

## **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](http://publicationethics.org/files/u2/New_Code.pdf)). To verify originality, your article may be checked by the Cross Check originality detection service <http://www.elsevier.com/editors/plagdetect>.

The authors are obliged to participate in peer review process and be ready to provide corrections, clarifications, retractions and apologies when needed. All authors of a paper should have significantly contributed to the research.

The reviewers should provide objective judgments and should point out relevant published works which are not yet cited. Reviewed articles should be treated confidentially. The reviewers will be chosen in such a way that there is no conflict of interests with respect to the research, the authors and/or the research funders.

The editors have complete responsibility and authority to reject or accept a paper, and they will only accept a paper when reasonably certain. They will preserve anonymity of reviewers and promote publication of corrections, clarifications, retractions and apologies when needed. The acceptance of a paper automatically implies the copyright transfer to the National Academy of Sciences of the Republic of Kazakhstan.

The Editorial Board of the National Academy of Sciences of the Republic of Kazakhstan will monitor and safeguard publishing ethics.

Правила оформления статьи для публикации в журнале смотреть на сайтах:

**[www.nauka-nanrk.kz](http://www.nauka-nanrk.kz)**

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

**ISSN 2518-1726 (Online),**

**ISSN 1991-346X (Print)**

Редакторы: *М.С. Ахметова, А. Ботанқызы, Д.С. Аленов, Р.Ж. Мрзабаева*

Верстка на компьютере *Г.Д. Жадыранова*

Подписано в печать 10.03.2022.

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

9,0 п.л. Тираж 300. Заказ 1.