

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
Әл-Фараби атындағы
Қазақ ұлттық университетінің

NEWS

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

SERIES
PHYSICS AND INFORMATION TECHNOLOGY

2 (346)

APRIL – JUNE 2023

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

QUEVEDO Nemandó, 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**

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 Жәбағаұлы, 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), Наноқұрылымды 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/>

© Қазақстан Республикасының Ұлттық ғылым академиясы, 2023

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

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), **Н=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), **Н=5**

РЕДАКЦИОННАЯ КОЛЛЕГИЯ:

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

БАЙГУНЧЕКОВ Жумадил Жанабаевич, 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**

РАМАЗАНОВ Глеккабул 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 Нурғали Жабагаевич, 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 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/>

© Национальная академия наук Республики Казахстан, 2023
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**

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-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, 2023

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 2. Number 346 (2023). 96–107
<https://doi.org/10.32014/2023.2518-1726.187>

UDC 543; 543.62

© **A.Sh. Barakova***, **O.A.Usatova**, **A.S.Orynbaeva**, 2023
Al-Farabi Kazakh National University, Almaty, Kazakhstan.
E-mail: balia_79@mail.ru

DIGITAL RESOURCES ON WEBSITES MODEL OF PROTECTION BY STEGANOGRAPHY

Barakova Aliya Sharizatovna — PhD student, Al-Farabi Kazakh National University. Almaty, Kazakhstan

E-mail: balia_79@mail.ru. ORCID: <https://orcid.org/0000-0002-0904-745X>;

Ussatova Olga Aleksandrovna — PhD, Gumarbek Daukeev Almaty University of energy and communications,
Almaty, Kazakhstan

E-mail: uoa_olga@mail.ru. ORCID: <https://orcid.org/0000-0002-5276-6118>;

Orynbaeva Ainur Serikovna — Senior Lecturer, Astana Medical University. Astana, Kazakhstan
E-mail: ainur_tas@mail.ru.

Abstract. This article provides an overview of ways and methods to prevent pirates from copying, processing, distributing and making digital resources public, and using digital creations for personal gain. To improve the quality of research and analysis, the steganography method is set as the goal. Finally, this review contains discussion, Research, Critical Analysis and a detailed summary, so that you can easily understand the development of steganography of media information such as image, video, audio. Steganography is a method of hiding data in a file, such as an image, audio, video, etc. and this data is reliably transmitted from the sender to the recipient. This method serves as a better way to protect the message than cryptography, which hides the content of the message. The original message is hidden so that the changes that occurred in the file are not noticed. To hide confidential information, you can use reliable steganography methods that are more complex than others, they all have their strengths and weaknesses. The absolute invisibility of confidential information is supported by various applications, while others require a large secret message to be hidden. This article discusses an overview of video, image, audio steganography, its use and methods to meet the need for privacy on the internet.

Key words: steganography, cryptography, confidential information, digital image, video, audio

© А.Ш. Баракова*, О.А. Усатова, А.С. Орынбаева, 2023
эл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан.
E-mail: balia_79@mail.ru

ВЕБ САЙТТАРДАҒЫ САНДЫҚ РЕСУРСТАРДЫ СТЕГАНОГРАФИЯ ӘДІСІМЕН ҚОРҒАУДЫҢ МОДЕЛІ

Баракова Алия Шаризатқызы — PhD докторанты, эл-Фараби атындағы Қазақ ұлттық университеті. Алматы, Қазақстан

E-mail: balia_79@mail.ru. ORCID: <https://orcid.org/0000-0002-0904-745X>;

Усатова Ольга Александрқызы — PhD, Ғұмарбек Дәукеев атындағы Алматы энергетика және байланыс университеті, Алматы, Қазақстан

E-mail: uoa_olga@mail.ru. ORCID: <https://orcid.org/0000-0002-5276-6118>;

Орынбаева Айнур Серикқызы — Аға оқытушы, Астана медицина университеті. Астана, Қазақстан

E-mail: ainur_tas@mail.ru.

Аннотация. Бұл мақалада қарақшылардың сандық ресурстарды көшіру, өңдеу, тарату және көпшілікке жария ету, сандық туындыларды жеке пайда табу үшін пайдаланудың алдын алу жолдары мен әдістеріне шолу жасалады. Зерттеу мен талдаудың сапасын жақсарту үшін стеганография әдісін алға мақсат етіп қойылады. Соңында, бұл шолуда талқылау, зерттеу, сыни талдау және егжей-тегжейлі түйіндеме бар, осылайша сурет, видео, аудио сияқты меди ақпараттардың стеганографиясының дамуын оңай түсінуге болады. Стеганография — бұл файлдағы деректерді жасыру әдісі, мысалы, сурет, аудио, видео және т.б. және бұл деректер жіберушіден алушыға сенімді түрде беріледі. Бұл әдіс хабарламаның мазмұнын жасыратын криптографияға қарағанда хабарламаны қорғаудың жақсы әдісі ретінде қызмет етеді. Бастапқы хабарлама файлда болған өзгерістер байқалмайтындай етіп жасырылады. Құпия ақпаратты жасыру үшін басқаларға қарағанда күрделі болып табылатын сенімді стеганография әдістерін қолдануға болады, олардың барлығының күшті және әлсіз жақтары бар. Құпия ақпараттың абсолютті көрінбейтіндігіне әртүрлі қосымшалар қолдау көрсетеді, ал басқалары үлкен құпия хабарламаны жасыруды талап етеді. Бұл мақалада видео, сурет, аудио стеганографиясына шолу, оны пайдалану және интернеттегі құпиялылық қажеттілігін қанағаттандыру әдістері қарастырылады.

Түйін сөздер: стеганография, криптография, құпия ақпарат, сандық сурет, видео, аудио

Мүдделер қақтығысы: Авторлар осы мақалада мүдделер қақтығысы жоқ деп мәлімдемейді.

© А.Ш. Баракова *, О.А. Усатова, А.С. Орынбаева, 2023

Казахский национальный университет им. аль-Фараби, Алматы, Казахстан.

E-mail: balia_79@mail.ru

РАЗРАБОТКА МОДЕЛИ ЗАЩИТЫ ЦИФРОВЫХ WEB РЕСУРСОВ С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ СТЕГАНОГРАФИИ

Баракова Алия Шаризатовна — докторант PhD, Казахский национальный университет им. Аль-Фараби. Алматы, Казахстан

E-mail: balia_79@mail.ru. ORCID: <https://orcid.org/0000-0002-0904-745X>;

Усатова Ольга Александровна — PhD, Алматинский университет энергетики и связи имени Гумарбека Даукеева, Алматы, Казахстан

E-mail: uoa_olga@mail.ru. ORCID: <https://orcid.org/0000-0002-5276-6118>;

Орынбаева Айнур Сериковна — старший преподаватель, медицинский университет Астана. Астана, Казахстан

E-mail: ainur_tas@mail.ru.

Аннотация. В данной статье представлен обзор способов и средств предотвращения от атак злоумышленника: копирования, редактирования, распространения и публикации цифровых ресурсов общественности, а также предотвращение использования цифрового контента в личных целях. Для повышения качества исследования и анализа в качестве цели выдвигается метод стеганографии. Данный обзор включает в себя обсуждение, исследование, критический анализ и подробный обзор, чтобы можно было легко понять развитие стеганографии для медиаинформации, такой как изображения, видео и аудио. Стеганография — это метод сокрытия данных в файле, таких как изображение, аудио-, видео-, которые безопасно передаются от отправителя к получателю. Данный метод является наиболее защищенным для передачи сообщения, чем криптография, которая кодирует информацию. Изменения в файле не доступны, так как исходное сообщение скрыто. Для сокрытия конфиденциальной информации могут использоваться разные методы стеганографии, которые имеют сильные и слабые стороны. Абсолютная невидимость конфиденциальной информации поддерживается различными приложениями, в то время как другие требуют сокрытия большого секретного сообщения. В этой статье представлен обзор методов стеганографии для защиты конфиденциальной информации в Интернете таких файлов, как видео, аудио и изображений.

Ключевые слова: стеганография, криптография, конфиденциальная информация, цифровое изображение, видео, аудио

Кіріспе

Цифрлық технологиялар мен интернеттің дамуымен мультимедиялық және цифрлық туындылар кескіндер, аудио, видео және басқа да цифрлық форматтар түрінде интернетте жарияланады және оларға авторлық құқықты

қорғау және ақпараттың тұтастығын қамтамасыз ету біртіндеп шешілуі керек өзекті мәселеге айнауда (Усатова, 2022). Сандық туындыларды көшіру, өңдеу, тарату және көпшілікке жария ету оңай болғандықтан, қарақшылар цифрлық туындылардың осы сипаттамаларын жеке пайда табу үшін авторлық құқық иелерінің заңды құқықтарын бұзу үшін пайдаланады.

Біз өз зерттеуімізде стеганографиялық әдістердің көбеюімен қатар, мақалаларда сурет, видео т.б. медиа ақпараттың кеңістіктік аймақтың стеганографиясына көбірек бағытталғанын байқадық. Әдебиеттік шолу жалпы стеганографияны жан-жақты талқылайтын әр әдісті енгізу процесіне бағытталған. Әдістерді ендіру процесінде ең көрнекті идея негізінде бірнеше санатқа бөлуге болады; сондықтан жаңа классификация ұсынылады. Ұсынылған жіктеу аудиостеганографияда ең көп қолданылатын тәсілдерді жалпылауға және түсінуге мүмкіндік береді. Содан кейін бұл зерттеу әрбір әдістің күшті және әлсіз жақтарын оның іске асыру мінез-құлқына негізделген сыни тұрғыдан қарастырады. Ендіру, медиа түрлері және бағалау орталары саласындағы басқа мәселелер де талқыланады.

Бірнеше жаңа әдістер маңызды аспект ретінде сенімділікті арттырады. Бұл стеганографиялық әдістердің дамуын әр түрлі етеді және әдетте әдістің мақсатын бір немесе екі аспектке бағыттайды. Қазіргі уақытта стеганография туралы мақалалар, әсіресе шолулар, стеганографияны оның мақсаттарына қарай сирек жіктейді. Осылайша, бұл шолулар стеганографиялық зерттеулердің мақсаттарына ықпал етеді. Зерттеу жұмысымызды деректерді жинаудан бастау алды. Ол әлемдік деңгейдегі бес дерекқорды қамтиды, атап айтқанда Web of Science, IEEE Xplore, ScienceDirect, Scopus және Springer, нәтижесінде барлығы 57 мақала қарастырылды. Әдебиеттік шолуда әр әдісті енгізу процесіне бағытталған яғни тәжірбиеден өткізілген. Әдістерді ендіру процесін бірнеше санатқа бөлуге болады. Стеганография әдісін зерттеу барысында сурет, видео, аудио т.б. медиа ақпараттарды қорғауға арналған бірнеше авторлардың жұмыстарын қарастырайық. Олар ұсынған ең көп қолданылатын тәсілдерді жалпылауға және түсінуге мүмкіндік береді. Содан кейін бұл зерттеу әрбір әдістің күшті және әлсіз жақтарын оның іске асыру мінез-құлқына негізделген сыни тұрғыдан қарастырады.

Әдебиеттік шолу

J. Bai тағы басқалары (Jiawang, 2022) өз зерттеу жұмыстарында авторлар видео деректердің қорғаудың жаңа әдісін ұсынған. Universal attack шабуылдарының әсерінен болатын зиянды видео деректерін жинауын болдырмау үшін видеоны терең хэштеу әдісін әзірледі. Бұл әдісті сценарийлерге деректерсіз таратады яғни видеоларды түпнұсқасыз да қорғауды қамтамасыз етеді. Әдістерін жүзеге асыруда эксперименттер жасап, екі деректер жиынтығы қолданған оның бірі ақ жәшік параметрлерінде де, қара жәшік параметрлерінде қарастырған. Бұл әдіс интернетте бөлісуге болатын видеоның құпиялылығын қорғайтындығына ерекше назар аударған.

Трапезников Е.В. (Трапезников, 2023) өз еңбегінде видео мазмұнын ашық желілерде қорғаудың бір әдісі ретінде логикалық жинақтауды қолданған, кездейсоқ бөліктерде видео деректеріне су таңбаларын енгізу әдісі ұсынылған. Ұсынылған әдіс видео ақпаратты бұрмалаудан қорғауға арналған бағдарламалық өнім деп сипаттаған. Бағдарламалық өнім C # тілінде жүзеге асырылады.

Ala Abu-Zahra (Ala Abu-Zahra, 2012) тағы басқалары өз жұмыстарында SAVLC және CABAC негізіндегі SVC-де әртүрлі рұқсаттарға тәуелсіз қол жеткізуге арналған жаңа платформа ұсынған. Ұсынылған схемада қабат аралық болжамды қолданған. Шифрлау схемасында нақты уақыттағы гетерогенді медиа ағынының сценарийлері үшін қолайлы деп есептейді. Авторлар эксперимент кезінде бірдей рұқсаттарды беру арқылы әрбір рұқсатты дербес қорғауды қамтамасыз ете алатынын көрсеткен.

Аудио-стеганография саласында көптеген шолу мақалалары жарияланған. А. Das өз әріптестерімен (Das, 2012) стеганографияны бұқаралық ақпарат құралдарының бірнеше түріне бағыттаған. Мысалы, мәтін, сурет, аудио және видео сияқты әртүрлі медиа түрлеріндегі стеганография әдістеріне шолу жасап, соның ішінде LSB кодтау, спектрді тарату және жаңғырықты жасыру, онда пакет аймағындағы деректерді жасырудың бірнеше әдістерін ұсынған. Зерттеуде стеганография және суреттерді, аудионы және HTML беттерін стегоанализдеу әдістері қарастырылған.

Trivikram M. Басқалары (Assaf Cohena, 2022) зерттеулерінде кескін, сурет файлдарының кең қолданылуына және көлемінің салыстырмалы айырмашылықтарына байланысты кескінді стеганографиялаудың заманауи әдістеріне бағытталған. Бұл мақалада сандық суреттерге арналған стеганография саласы мен стеганография әдістері қарастырылған. Соңғы жылдары стеганография басты назарда болды, өйткені стеганографиямен байланысты кибершпиондық шабуылдар көбейе бастады. Сурет стеганографиясының мазмұнын (стеганографияның кез келген түрін) анықтау үшін жанама арнаға шабуыл жасау әлдеқайда көп эксперименттер мен инновацияларды қажет етеді және зерттеудің тағы бір айқын бағыты болып табылады.

Әдістер мен материалдар

Адамзат тарихының барлық уақыттарында ақпаратты бұрмаланудан және рұқсатсыз қол жеткізуден қорғау мәселесі өзекті болып табылады (Коржик, 2017). Ежелгі әлемде бұл мәселені шешудің екі негізгі бағыты ерекшеленді, олар: криптография және стеганография. Стеганография әдетте криптографиямен қатар деректерді қорғау әдістері ретінде жіктеледі. Криптография құпия хабарламаны мағынасыз және оқылмайтын түрге айналдырады, сондықтан оны шабуылдаушылар түсіне алмайды, ал стеганография құпия хабарламалар мен олардың жазықсыз ортада болуын құпия түрде жасырады. Стеганография деректерді жасырын түрде жіберу

әдістері ғана емес (классикалық стеганография деп аталады), сонымен қатар шуылға төзімді аутентификация, ақпаратты рұқсатсыз көшіруден қорғау, байланыс желілері арқылы ақпараттың таралуын бақылау, мультимедиялық мәліметтер базасында ақпаратты іздеу және т.б. Жағдайларда дәстүрлі қолданыстағы ақпараттық ағындар немесе ақпараттық орта шеңберіне мүмкіндік береді және әр саланың р қолданбалы ақпаратын қорғаудың маңызды мәселелерін шешеді (Шелухин, 2018).

Мультимедиялық технологиялардың танымалдығы MP3, MPEG-4, JPEG2000 стандарттарында пайдалану үшін алгоритмдерін әзірлеуге, DVD дискілерін көшіруден қорғауға байланысты көптеген зерттеулер туындады. Стеганография технологиясын қолданудың негізгі бағыттарын төрт топқа біріктіруге болады: көшіруден қорғау (пайдалану), құжаттардың жасырын аннотациясы, ақпараттың түпнұсқалығын дәлелдеу және жасырын байланыс



Сур.1. Стеганографияны қолдану салалары (Fig.1. Areas of application of steganography)

Стегожүйенің математикалық моделін қарастырайық

Стегожүйені байланыс жүйесі ретінде ССБ (Сандық су белгісі).

Цифрлық стеганография алгоритмін ендіру үш негізгі кезеңнен тұрады:

- 1) ССБ генерацияланады,
- 2) кодерге ССБ ендіру
- 3) детекторда ССБ анықтау

ССБ мүмкін болатын W^* , K^* , I^* , B^* кілттер болсын, сәйкесінше контейнерлер мен жасырын хабарламаларымен. Онда ССБ генерациялау мына түрінде ұсынылуы мүмкін

$$F: I^*K \times B^* \rightarrow W^*, \quad W = F(I, K, B),$$

Мұндағы W , K , I , B - тиісті жиындардың өкілдері. Жалпы айтқанда, функция F ерікті болуы мүмкін, бірақ іс жүзінде қойлатын талаптарда шектеу бар.

Сонымен көп жағдайда $F(I, K, B) \approx F(I + \varepsilon, K, B)$ яғни шамалы

өзгертілген контейнер ССБ өзгеруіне әкелмейді. F функциясы әдетте құрама болып табылады:

$$F = T \circ G, \text{ мұнда } G: K^* \times B^* \rightarrow C^* \text{ және } T: C^* \times I^* \rightarrow W$$

яғни, ССБ контейнердің қасиеттеріне байланысты. Функция G бастапқы мәндер ретінде қауіпсіз жалған кездейсоқ реттілік генераторының көмегімен жүзеге асырылуы мүмкін.

T операторы C* кодтық сөзін өзгерте отырып, нәтижесінде W* ССБ алады. Бұл функцияға шектеу қоймасақта болады, себебі G кепіл береді F функциясы қайтымсыз екеніне. T функциясы таңдалуы керек толтырылмаған I₀ контейнер, толтырылған I_w контейнер және шамалы I_w толтырылған контейнерлер бірдей нәрсені тудырады.

$$T(C, I_0) = T(C, I_w) = T(C, I'_w)$$

Нәтижелер және оларды талқылау

Видео файлды өңдеу үшін avifil32.dll функциялар қолданылады. Бұл тәсілде C # қабықшалары қол жетімділік функциялары үшін қолданылады әрі avifil32.dll -де қол жетімді бола алады. Жүйені құру үшін 4 модуль қолданылады:

- Видео кадрларды бөлу және генерациялау технологиясы
- Байт-код фабрикасы
- Криптографиялық зауыт
- Стеганография фабрикасы



Сур.2. Стеганография фабрикасының сұлбасы
(Fig.2. outline of Steganography factory)

Зерттеу жүргізу үшін деректердің 4 түрі қажет болады:
Кілт файлы;
Құпия сөз;

Медиа;
Хабарлама.

Медиа файл өлшемі қолданылатын әдіске байланысты пропорцияда хабарлама өлшемінен асып кетуі керек.

Құпия сөз: пароль хабарламаны медиа файлға енгізер алдында оны шифрлау үшін қолданылған.

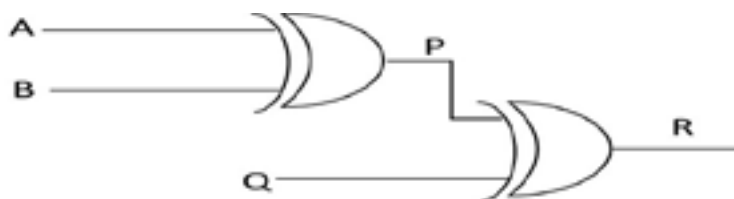
Кілт файлы: кілт файлы жасырын хабарламаның қауіпсіздігін жақсарту үшін қолданылады. Жеке парольдерді әртүрлі тәсілдермен табуға болады. Кілт файлы құпия сөзді болжауға жол бермейді, сондықтан әдіс қауіпсіздігін арттырады.

Тасымалдаушы Файл: бұл зерттеуде медиа файл ретінде видео файл қолданылады. Видео файл пішімі - AVI.

Хабарлама: Хабарлама медиа файл өлшемінен кішірек видео файл болады.

Деректерді жасыру процесінде визуалды файл тасымалдаушы файл болып табылады. Видео кадрларды бөлу және генерациялау фабрикасын қолдана отырып, кадрлар медиа файл үшін жасалады. Хабарды байт коды зауыты байт кодына түрлендіреді. Содан кейін хабарламаның байт коды steganography factory көмегімен шифрланады. Steganography factory үшін 2 кіріс қажет: кілт файлы және құпия сөз. Бұл қауіпсіздіктің жоғарылауына әкеледі, өйткені құпия сөзді тек болжау арқылы жасауға болады. Бұл шифрланған хабарлама steganographic factory модуліндегі медиа файл жақтауларында жасырылған. Нәтижесінде кескін осы кадрлардың көмегімен қайта жасалады.

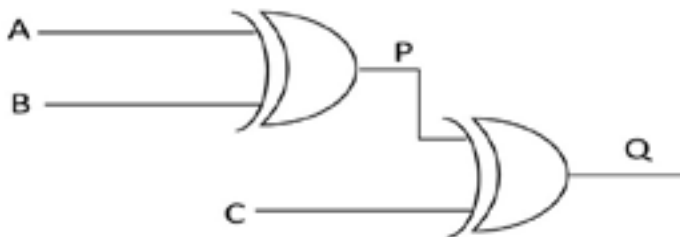
Бұл шифрлау әдісі XOR екі элементі пайдаланылады. 3 суретте осы шифрлау үшін логикалық элементтің қалай жұмыс істейтінін көрсетеді. А кілт файлы, ал В құпия сөзді білдіреді. Құпия сөздің өлшемі кілт файлының өлшемінен кіші болғандықтан, құпия сөз қайталанады. С хабарламаны білдіреді.



Сур.3. Шифрлау үшін логикалық элементтің жұмысы
(Fig.3. operation of the logical element for encryption)

4 суретте шифрды ашу үшін логикалық элементтің қалай жұмыс істейтінін көрсетеді. Q шифрланған хабарламаны білдіреді. R декодталған дегенді білдіреді

С жасырын хабарламасы шифрланған Q хабарламасына тең болатынын көре аламыз.



Сур.4. Шифрды ашу үшін логикалық элементтің жұмысы
(Fig.4. operation of the logical element to decrypt)

Тәжірбиені іске асыру

Бұл криптографияның орнына стеганографияны қолданудың басты артықшылығы. Осылайша, хабарламаны делдалдан жасырудың тиімділігін бағалау маңызды. Хабарламаны жасырудың тиімділігін өлшеу үшін кірістірілген видеолар зерттеушіге хабарламаның бар-жоғын анықтау үшін жіберіледі. Ол үшін 17 ендірілген және 17 ендірілмеген видео файл қолданылады. Зерттеушіге бұл видеоларды сынап көру және оларды кірістірілген хабарламалар мен кәдімгі видеолар ретінде жіктеу ұсынылады. Нәтижелерді келесідей жіктеуге болады. Зерттеуші видеоны келесідей жіктейді

- кірістірілген видео және ендірілген видео (TP)
- кірістірілген видео және кірістірілмеген видео (FP)
- видео кіріктірілмеген және видео ендірілген (FN)
- видео ендірілмеген және видео кірістірілмеген (TN)

Бұл санаттарды ұсынылған әдістің өнімділігін тексеру үшін пайдалануға болады. Дұрыс стеганографиялық әдіс үшін дұрыс жіктеу мен дұрыс емес жіктеу арасындағы байланыс маңызды болмауы керек. Сондықтан өнімділікті өлшеу үшін коэффициент коэффициентін қолдануға болады.

Стеганографияны бағалау кезінде медиа файлдан дұрыс хабарлама алу мүмкіндігін тексеру маңызды. Хабарлама видео файл, аудио файл, сурет немесе мәтіндік құжат болуы мүмкін. Өнімділікті тексеру үшін 5 видео файл, 4 аудио файл, 3 сурет және 3 мәтіндік файл таңдалды. Алынған хабарламамен бастапқы хабарламаны бағалау үшін Aliyaschool.kz веб курстың қолданушыларының ішінен 10 қатысушытаңдалады. Олардан хабарламаларды 0-ден 4-ке дейін бағалауды сұрады, мұнда 0 бастапқы хабарлама мен алынған хабарлама арасындағы айырмашылықтың жоқтығын көрсетеді, ал 4 екі хабарлама арасындағы 100 % айырмашылықты көрсетеді.

1 кесте. Әр жағдайға берілген дәрежелер көрсеткіштері

Дәреже саны	Сипаттамасы
0	Айырмашылығы жоқ
1	Аз ғана айырмашылық бар

2	Орташа айырмашылық бар
3	Үлкен айырмашылық бар
4	жалпы айырмашылық

Видео, аудио, сурет және мәтіннің орташа рейтингі барлық 10 қатысушы үшін есептеледі.

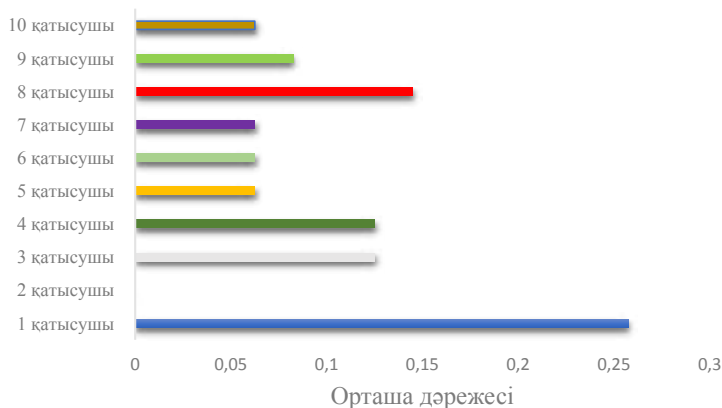
2 кесте. Бір ғана қатысушының нәтиже көрсеткіші

	Видео	Аудио	Сурет	Мәтін
1 файл	0	1	0	0
2 файл	1	1	0	
3 файл	0	0	1	
4 файл	0	0		
5 файл	0			
орташа дәрежесі	0,2	0,5	0,33	0

3 кесте. Барлық қатысушылардың орташа рейтингі көрсеткіштері

	Видео	Аудио	Сурет	Мәтін
1 қатысушы	0,2	0,5	0,33	0
2 қатысушы	0	0	0	0
3 қатысушы	0,25	0,25	0	0
4 қатысушы	0,5	0	0	0
5 қатысушы	0	0,25	0	0
6 қатысушы	0	0,25	0	0
7 қатысушы	0,25	0	0	0
8 қатысушы	0	0,25	0,33	0
9 қатысушы	0	0	0,33	0
10 қатысушы	0,25	0	0	0
	0,145	0,15	0,09	0

Осы нәтижелерден 0–4 дәрежелер диапазонында видео үшін орташа дәреже 0,145, аудио үшін орташа дәреже 0,15, видео үшін орташа дәрежеден аз, кескін үшін орташа дәреже 0,09, видео үшін де, аудио үшін де орташа дәрежеден аз, ал мәтін үшін орташа дәреже дәл 0. Осылайша, жүйенің тасымалдаушы файлдан деректерді дұрыс алудың жоғары өнімділігі бар екені анықталды.



Сур.5. Орташа дәрежелі график көрсеткіштері
(Fig.5. average graph indicators)

Ағымдағы зерттеу визуалды видео мазмұнын жасыру үшін жүргізілді. Видеоны жасырудың маңыздылығы мынада: видеода әдетте үлкен файл болады, өйткені ол көптеген мәліметтерден тұрады. Ұсынылған тәсілдің шегі-ол тек медиа файл ретінде пайдалану үшін қысылмаған, тағы MS AVI файлында қолдайды. Алайда, көрсетілген файл түрі үшін (қысылмаған AVI) ол жақсы тексерілген және жақсы жұмыс істейді. Деректердің қауіпсіздігін арттыру мақсатында хабарлама тасымалдаушы файлға енгізілмес бұрын шифрланған. Бұл шифрлау әдісі кілт файлын да, парольді де қолданады. Бұл жағдайда пароль тандалмайды, ал хабарламаны шифрлау үшін 2 логикалық XOR элементі қолданылады.

Қорытынды

Сонымен қорыта келгенде Стеганография - бұл ақпараттың болуы белгісіз болатындай етіп медиада ақпаратты жасыру өнері (Amirtharajan, 2013). Сандық кескін стеганографиясы қазіргі заманғы қосымшалардың көпшілігінде шешуші болып табылатын байланыс әлеуетін жүзеге асырады. Стеганографияның бірнеше пайдалы қолданылуы бар. Есептеу қуатының таңғажайып дамуы және қауіпсіздік туралы хабарлардың артуы арқылы ол заманауи қауіпсіздік жүйелері арасында көшбасшы болды (Ahmed, 2020). Стеганографиялық техниканы ұсытудағы басты мәселесі - оны криптография және су белгілері сияқты өзара байланысты жүйелерден бөлетін жоғары ендіру сыйымдылығы мен жасырын және қауіпсіздік арасындағы сәйкес тепе-теңдікті сақтау. Бұл мақалада стеганографияның кейбір жаңа әдістеріне кең шолу мен талдау ұсынылады. Сонымен қатар, біз танымал стеганография құралдарын егжей-тегжейлі талқыладық. Терең оқытуға негізделген соңғы стеганографиялық әдістерге қатысты мәселелер шешілді. Пәндік саланы зерттеуге арналған мақаланың соңында болашақ зерттеулердің кейбір бағыттары туралы айтылады.

ӘДЕБИЕТТЕР

- Усатова О.А., Баракова А.Ш. «Анализ современных систем защиты веб-ресурсов» // Известие НАН РК № 1 (341), Алматы, 2022 г. с. 88-95.
- Jiawang Bai, Bin Chen, Kuofeng Gao, Xuan Wang, Shu-Tao Xia. Practical protection against video data leakage via universal adversarial head//Pattern Recognition Volume 131, November 2022, 108834. <https://doi.org/10.1016/j.patcog.2022.108834>
- Трапезников Е.В. Способ защиты видео контента в открытых сетях // ОмГТУ. 2014. №4. <https://cyberleninka.ru/article/n/sposob-zaschity-video-kontenta-v-otkrytyh-setyah> (дата обращения: 25.05.2023).
- Ala Abu-Zahra, Zafar Shahid, Amjad Rattrout, William Puech//Independent Protection of Different Layers in Spatially Scalable Video Coding. Procedia Computer Science Volume 10, 2012, Pages 240-246. <https://doi.org/10.1016/j.procs.2012.06.033>
- A. Das, Steganography: Secret data hiding in multimedia, in: Signal Conditioning, Springer, Berlin Heidelberg, 2012, pp. 275–295
- The infinite race between steganography and steganalysis in images Trivikram Muralidharan, Aviad Cohena, Assaf Cohena, Nir Nissima// Signal Processing Volume 201, December 2022, 108711. <https://doi.org/10.1016/j.sigpro.2022.108711>
- Коржик В. И. Цифровая стеганография и цифровые водяные знаки [Текст] / монография: в 2 ч В. И. Коржик // СПбГУТ, 2017.
- Шелухин О.И. Стеганография. Алгоритмы и программная реализация [Текст] / О. И. Шелухин, С. Д. Канаев // Горячая линия - Телеком, 2018.
- Amirtharajan, R., & Rayappan, J. B. B. (2013). Steganography-time to time: A review. Research Journal of the Information Technology, 5, 53–66. <http://dx.doi.org/10.3923/rjit.2013.53.66>
- Ahmed A. AlSabhany, Ahmed Hussain Ali, Farida Ridzuan, A.H. Azni, Mohd Rosmadi Mokhtar//Digital audio steganography: Systematic review, classification, and analysis of the current state of the art. Computer Science Review Volume 38, November 2020, 100316. <https://doi.org/10.1016/j.cosrev.2020.100316>

REFERENCES

- Ala Abu-Zahra, Zafar Shahid, Amjad Rattrout, William Puech, 2012. //Independent protection of various levels in spatially scalable video encoding. Procedia Computer Science, volume 10, 2012. PP. 240–246. <https://doi.org/10.1016/j.procs.2012.06.033>
- Amirtharajan R. and Rayappan J.B.B., 2013. Steganography - from time to time: an overview. Research Journal of Information Technology, 5. Pp. 53–66. <http://dx.doi.org/10.3923/rjit.2013.53.66>
- A. Das, Steganography, 2012. Hiding secret data in multimedia, in: Signal Generation, Springer, Berlin-Heidelberg, 2012. Pp. 275–295
- Jiawang Bai, Bin Chen, Kuofeng Gao, Xuan Wang, Shu-Tao Xia, 2022. Practical protection against video data leakage with universal adversarial head //Pattern Recognition. Volume 131. November 2022. 108834. <https://doi.org/10.1016/j.patcog.2022.108834>
- Korzhek V.I., 2017. Digital steganography and digital watermarks [Text] / monograph: in 2 hours V.I. Korzhik // SPbGUT, 2017.
- Usatova O.A., Barakova A.V., 2022. "Analysis of a modern method of combating HIV infection" // Izvestiya NAS RK No. 1 (341)Almaty, 2022. Pp. 88–95.
- Trapeznikov E.V., 2014. Method of protecting video content in open networks // OmSTU. 2014. № 4. <https://cyberleninka.ru/article/n/sposob-zaschity-video-kontenta-v-otkrytyh-setyah> (accessed: 05/25/2023).
- The endless race between steganography and steganalysis in images Trivikram Muralidharan, Aviad Cohen, Assaf Cohen, Nir Nissima // Signal Processing, volume 201, December 2022. 108711. <https://doi.org/10.1016/j.sigpro.2022.108711>
- Shelukhin O.I., 2018. Steganography. Algorithms and software implementation [Text] / O.I. Shelukhin, S.D. Kanaev // Hotline - Telecom, 2018.
- Ahmed A., 2020. Alsbakhani, Ahmed Hussein Ali, Farida Ridzuan, A.H. Azni, Mohd Rosmadi Mokhtar//Digital audio steganography: a systematic review, classification and analysis of the modern state of technology. Computer Science Review. Volume 38. November 2020. 100316. <https://doi.org/10.1016/j.cosrev.2020.100316>

МАЗМҰНЫ

А. Адамова, Т. Жукабаева, Е. Марденов ЗАТТАР ИНТЕРНЕТІ: ЖЕҢІЛДІК АЛГОРИТМДЕРДІҢ ДАМУЫ ЖӘНЕ БОЛАШАҒЫ.....	5
Г. Алпысбай, А. Бедельбаев, О. Усагова, А. Жұмабекова, Эдзард Хофиг ЗИЯНДЫ БАҒДАРЛАМАЛЫҚ ЖАБДЫҚТАРДЫ ТАЛДАУДА МАШИНАЛЫҚ ОҚЫТУ АЛГОРИТМІН ҚОЛДАНУ.....	21
А.У. Алтаева, А.Ш. Каипова, А.У. Мухамеджанова, Г.К. Оспанова МЕДИЦИНАДА ЧАТ-БОТТАРДЫ ҚОЛДАНУ ПЕРСПЕКТИВАЛАРЫ.....	32
Г.А. Анарбекова, Н.Н. Оспанова, Д.Ж. Анарбеков НОРМАЛАНҒАН КІРІС ВЕКТОРЛАРЫ: ДЕРЕКТЕРДІ ДАЙЫНДАУДЫҢ БАСТАПҚЫ КЕЗЕҢІ.....	40
А.Е. Әбжанова, А.И. Такуадина, С.К. Сагнаева, С.К. Серикбаева, Г.Т. Азиева ТОПЫРАҚТЫ ТЕХНИКАЛЫҚ МЕЛИОРАЦИЯЛАУ ӘДІСТЕРІНДЕ АҚПАРАТТЫҚ ЖҮЙЕЛЕРДІ ПАЙДАЛАНУ.....	55
К.Н. Әлібекова, Ж.М. Алимжанова, С.С. Байзакова СЫМСЫЗ СЕНСОРЛЫҚ ЖЕЛІЛЕР ҮШІН БЛОКТЫҚ ШИФРЛАРДЫҢ ӨНІМДІЛІГІН БАҒАЛАУ.....	70
К.Б. Багитова, Ш.Ж. Мүсірәлиева, М.А. Болатбек, Р.Қ. Оспанов ИНТЕРНЕТТЕ ЭКСТРЕМИСТІК МАЗМҰНДЫ АНЫҚТАУҒА АРНАЛҒАН EXWEB БАҒДАРЛАМАЛЫҚ ЖАБДЫҚТАМАСЫН ӨЗІРЛЕУ.....	81
А.Ш. Баракова, О.А. Усагова, А.С. Орынбаева ВЕБ САЙТТАРДАҒЫ САНДЫҚ РЕСУРСТАРДЫ СТЕГАНОГРАФИЯ ӘДІСІМЕН ҚОРҒАУДЫҢ МОДЕЛІ.....	96
А.С. Омарбекова, А.Е. Назырова, Н. Тасболатұлы, Б.Ш. Разахова ИНТЕЛЛЕКТУАЛДЫ ELEARNING ЖҮЙЕСІНІҢ ОНТОЛОГИЯЛЫҚ МОДЕЛІ ЖӘНЕ ОҚЫТУ НӘТИЖЕЛЕРІ.....	108
М.Қ. Болсынбек, Г.Б. Абдикеримова, С.К. Серикбаева, А.Ж. Танирбергенов, Ж.К. Тасжурекова ТОПЫРАҚ ЖӘНЕ ТОПЫРАҚ ЭРОЗИСЫН БОЛЖАУЖЫҢ АҚПАРАТТЫҚ ЖҮЙЕЛЕРІ МЕН ӘДІСТЕРІН ЗЕРТТЕУ.....	128
Л.З. Жолшиева, Т.К. Жукабаева, Ш. Тураев, М.А. Бердиева, Б.А. Ху Вен-Цен LSTM ЖӘНЕ GRU ҮЛГІЛЕРІ НЕГІЗІНДЕ ҚАЗАҚ ДАКТИЛЬДЕРІН ТАНУДЫҢ ИНТЕЛЛЕКТУАЛДЫ ЖҮЙЕСІН ҚҰРУ.....	141
М.Д. Кабибуллин, Б.Б. Оразбаев, К.Н. Оразбаева, С.Ш. Исакова, Ж.Ш. Аманбаева КҮРДЕЛІ ХИМИЯЛЫҚ-ТЕХНОЛОГИЯЛЫҚ ЖҮЙЕЛЕР АГРЕГАТТАРЫНЫҢ МОДЕЛЬДЕРІН БАСТАПҚЫ АҚПАРАТТЫҢ ЖЕТІСПЕУШІЛІГІ МЕН АЙҚЫНСЫЗДЫҒЫ ЖАҒДАЙЫНДА ҚҰРУ.....	154

М.Ж. Қалдарова, А.С. Аканова, М.Г. Гриф, У.Ж. Айтимова, А.С. Муканова ТОПЫРАҚ ЖАҒДАЙЫН БАҒАЛАУ ҮШІН ҚОЛДАНЫЛАТЫН ҒАРЫШТЫҚ СУРЕТТЕРДІ ӨНДЕУ АЛГОРИТМДЕРІ МЕН ӘДІСТЕРІ.....	172
К. Келесбаев, Ш. Раманкулов, М. Нуризинова, А. Паттаев, Н. Мұсахан STEM ЖОБАЛЫҚ ОҚЫТУДЫҢ БОЛАШАҚ ФИЗИКА МАМАНДАРЫН ДАЯРЛАУДАҒЫ ЕРЕКШЕЛІКТЕРІ.....	193
А.Е. Кулакаева, Е.А. Дайнеко, А.З. Айтмагамбетов, А.Т. Жетписбаева, Б.А. Кожаметова ШАҒЫН ҒАРЫШ АППАРАТЫ ОРБИТАСЫНЫҢ СИПАТТАМАЛАРЫНЫҢ СПУТНИКТИК РАДИО МОНИТОРИНГ ЖҮЙЕСІНІҢ ПАРАМЕТРЛЕРІНЕ ӘСЕРІ ТУРАЛЫ.....	208
А.Е. Назырова, Г.Т. Бекманова, А.С. Муканова, Н. Амангелді, М.Ж. Қалдарова БІЛІМ БЕРУ БАҒДАРЛАМАЛАРЫ ҮШІН АВТОМАТТАНДЫРЫЛҒАН ЖҮЙЕНІ ӨЗІРЛЕУ.....	221
А.Б. Тоқтарова, Б.С. Омаров, Ж.Ж. Ажибекова, Г.И. Бейсенова, Р.Б. Абдрахманов ОНЛАЙН КОНТЕНТТЕГІ БЕЙӘДЕП СӨЗДЕР МӘЛІМЕТТЕР ҚОРЫН DATA MINING АРҚЫЛЫ АНАЛИЗДЕУ.....	237
Ә.Б. Тынымбаев, К.С. Байшоланова, К.Е. Кубаев АҚПАРАТТЫ ҚОРҒАУ ЖҮЙЕЛЕРІНДЕГІ NAVIVE BAYESIAN ЖІКТИТУШСІН ҚОЛДАНУ.....	252
Г.Қ. Шаметова, А.Ә. Шәріпбай, Б.Ф. Сайлау ҚОЛЖЕТІМДІЛІКТІ БАСҚАРУ ЖҮЙЕЛЕРІНДЕГІ ҚҰПИЯНЫ БӨЛҮДІҢ КРИПТОГРАФИЯЛЫҚ СҰЛБАЛАРЫН ТАЛДАУ.....	261
Г.Б. Абдикеримова, А.Ә. Шекербек, М.Г. Байбулова, С.К. Абдикаримова, Ш.Ш. Жолдасова КЕУДЕ ПАТОЛОГИЯСЫН АВТОКОРРЕЛЯЦИЯЛЫҚ ФУНКЦИЯ АРҚЫЛЫ АНЫҚТАУ.....	274

СОДЕРЖАНИЕ

А. Адамова, Т. Жукабаева, Е. Марденов ИНТЕРНЕТ ВЕЩЕЙ: СОСТОЯНИЕ И ПЕРСПЕКТИВЫ РАЗВИТИЯ ЛЕГКОВЕСНЫХ АЛГОРИТМОВ.....	5
Г. Алпысбай, А. Бедельбаев, О. Усагова, А. Жумабекова, Эдзарт Хофиг ПРИМЕНЕНИЕ АЛГОРИТМА МАШИННОГО ОБУЧЕНИЯ ДЛЯ АНАЛИЗА ВРЕДНОСНОГО ПО.....	21
А.У. Алтаева, А.Ш. Каипова, А.У. Мухамеджанова, Г.К. Оспанова ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ ЧАТ-БОТОВ В МЕДИЦИНЕ.....	32
Г.А. Анарбекова, Н.Н. Оспанова*, Д.Ж. Анарбеков НОРМАЛИЗОВАННЫЕ ВХОДНЫЕ ВЕКТОРЫ: ПЕРВИЧНЫЙ ЭТАП ПОДГОТОВКИ ДАННЫХ.....	40
А.Е. Абжанова, А.И. Такуадина, С.К. Сагнаева, С.К. Серикбаева, Г.Т. Азиева ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ В МЕТОДАХ ТЕХНИЧЕСКИХ МЕЛИОРАЦИЙ ГРУНТОВ.....	55
К.Н. Алибекова, Ж.М. Алимжанова, С.С. Байзакова ОЦЕНКА ПРОИЗВОДИТЕЛЬНОСТИ БЛОЧНЫХ ШИФРОВ ДЛЯ БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЕЙ.....	70
К.Б. Багитова, Ш.Ж. Мусиралиева, М.А. Болатбек, Р.К. Оспанов РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ EXWEB ДЛЯ ВЫЯВЛЕНИЯ ЭКСТРЕМИСТСКОГО КОНТЕНТА В СЕТИ ИНТЕРНЕТ.....	81
А.Ш. Баракова, О.А. Усагова, А.С. Орынбаева РАЗРАБОТКА МОДЕЛИ ЗАЩИТЫ ЦИФРОВЫХ WEB РЕСУРСОВ С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ СТЕГАНОГРАФИИ.....	96
А.С. Омарбекова, А.Е. Назырова, Н. Тасболатұлы, Б.Ш. Разахова ОНТОЛОГИЧЕСКАЯ МОДЕЛЬ ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ ЭЛЕКТРОННОГО ОБУЧЕНИЯ И РЕЗУЛЬТАТЫ ОБУЧЕНИЯ.....	108
М.Қ. Болсынбек, Г.Б. Абдикеримова, С.К. Серикбаева, А.Ж. Танирбергенов, Ж.К. Тасжурекова ИССЛЕДОВАНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ И МЕТОДОВ ПРОГНОЗИРОВАНИЯ ПОЧВЕННОЙ И ПОЧВЕННОЙ ЭРОЗИИ.....	128
Л.З. Жолшиева, Т.К. Жукабаева, Ш. Тураев, М.А. Бердиева, Б.А. Ху Вен-Цен РАЗРАБОТКА ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ РАСПОЗНАВАНИЯ КАЗАХСКИХ ДАКТИЛЬНЫХ ЖЕСТОВ НА ОСНОВЕ МОДЕЛЕЙ LSTM И GRU.....	141
М.Д. Кабибуллин, Б.Б. Оразбаев, К.Н. Оразбаева, С.Ш. Искакова, Ж.Ш. Аманбаева РАЗРАБОТКА МОДЕЛЕЙ АГРЕГАТОВ СЛОЖНЫХ ХИМИКО-ТЕХНОЛОГИЧЕСКИХ СИСТЕМ В УСЛОВИЯХ ДЕФИЦИТА И НЕЧЕТКОСТИ ИСХОДНОЙ ИНФОРМАЦИИ.....	154

М.Ж. Калдарова, А.С. Аканова, М.Г. Гриф, У.Ж. Айтимова, А.С. Муканова АЛГОРИТМЫ И МЕТОДЫ ОБРАБОТКИ КОСМИЧЕСКИХ СНИМКОВ ДЛЯ ОЦЕНКИ СОСТОЯНИЯ ПОЧВ.....	172
К. Келесбаев, Ш. Раманкулов, М. Нуризинова, А. Паттаев, Н. Мұсахан ОСОБЕННОСТИ ПРОЕКТНОГО ОБУЧЕНИЯ STEM В ПОДГОТОВКЕ БУДУЩИХ СПЕЦИАЛИСТОВ ПО ФИЗИКЕ.....	193
А.Е. Кулакаева, Е.А. Дайнеко, А.З. Айтмагамбетов, А.Т. Жетписбаева, Б.А. Кожаметова О ВЛИЯНИИ ХАРАКТЕРИСТИК ОРБИТЫ МАЛОГО КОСМИЧЕСКОГО АППАРАТА НА ПАРАМЕТРЫ СИСТЕМЫ СПУТНИКОВОГО РАДИОМОНИТОРИНГА.....	208
А.Е. Назырова, Г.Т. Бекманова, А.С. Муканова, Н. Амангелді, М.Ж. Калдарова, РАЗРАБОТКА АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ ДЛЯ ОБРАЗОВАТЕЛЬНЫХ ПРОГРАММ.....	221
А.Б. Токгарова, Б.С. Омаров, Ж.Ж. Ажибекова, Г.И. Бейсенова, Р.Б. Абдрахманов АНАЛИЗ НЕОБРАЗНЫХ СЛОВ В ОНЛАЙН-КОНТЕНТЕ С ПОМОЩЬЮ DATA MINING.....	237
Ә.Б. Тынымбаев, К.С. Байшоланова, К.Е. Кубаев ПРИМЕНЕНИЕ НАИВНОГО БАЙЕСОВСКОГО КЛАССИФИКАТОРА В СИСТЕМАХ ЗАЩИТЫ ИНФОРМАЦИИ.....	252
Г.Қ. Шаметова, А.Ә. Шәріпбай, Б.Ғ. Сайлау АНАЛИЗ КРИПТОГРАФИЧЕСКИХ СХЕМ РАСПРЕДЕЛЕНИЯ СЕКРЕТОВ В СИСТЕМАХ УПРАВЛЕНИЯ ДОСТУПОМ.....	261
Г.Б. Абдикеримова, А.А. Шекербек, М.Г. Байбулова, С.К. Абдикаримова, Ш.Ш. Жолдасова ОПРЕДЕЛЕНИЕ ГРУДНОЙ ПАТОЛОГИИ С ПОМОЩЬЮ ФУНКЦИИ АВТОКОРРЕЛЯЦИИ.....	274

CONTENTS

A. Adamova, T. Zhukabayeva, Y. Mardenov INTERNET OF THINGS: STATUS AND PROSPECTS FOR THE DEVELOPMENT OF LIGHTWEIGHT ALGORITHMS.....	5
G. Alpysbay, A. Bedelbayev, O. Ussatova, A. Zhumabekova, Edzard Höfig APPLICATION OF MACHINE LEARNING ALGORITHM IN THE ANALYSIS OF MALICIOUS SOFTWARE.....	21
A.U. Altaeva, A.S. Kaipova, A.U. Mukhamejanova, G.K. Ospanova PROSPECTS OF USING CHATBOTS IN MEDICINE.....	32
G.A. Anarbekova, N.N. Ospanova, D.Zh. Anarbekov NORMALIZED INPUT VECTORS: THE PRIMARY STAGE OF DATA PREPARATION.....	40
A.E. Abzhanova, A.I. Takuadina, S.K. Sagnaeva, S.K. Serikbayeva, G.T. Azieva THE USE OF INFORMATION SYSTEMS IN THE METHODS OF TECHNICAL SOIL RECLAMATION.....	55
K. Alibekova, Zh. Alimzhanova, S.S. Baizakova RATING VALUATION OF BLOCK CIPHERS FOR WIRELESS SENSOR NETWORKS.....	70
K.B. Bagitova, Sh.Zh. Mussiraliyeva, M.A. Bolatbek, R.K. Ospanov DEVELOPMENT OF EXWEB SOFTWARE FOR DETECTING EXTREMIST CONTENT ON THE INTERNET.....	81
A.Sh. Barakova, O.A. Usatova, A.S. Orynbaeva DIGITAL RESOURCES ON WEBSITES MODEL OF PROTECTION BY STEGANOGRAPHY.....	96
A.S. Omarbekova, A.E. Nazyrova, N. Tasbolatuly, B.Sh. Razakhova ONTOLOGICAL MODEL OF AN INTELLIGENT E-LEARNING SYSTEM AND LEARNING OUTCOMES.....	108
M. Bolsynbek, G. Abdikerimova, S. Serikbayeva, A. Tanirbergenov, Zh. Taszhurekova RESEARCH OF INFORMATION SYSTEMS AND METHODS OF FORECASTING SOIL AND SOIL EROSION.....	128
L. Zholshiyeva, T. Zhukabayeva, Sh. Turaev, M. Berdieva, B. Khu Ven-Tsen DEVELOPMENT OF AN INTELLECTUAL SYSTEM FOR RECOGNIZING KAZAKH DACTYL GESTURES BASED ON LSTM AND GRU MODELS.....	141
M. Kabibullin, B. Orazbayev, K. Orazbayeva, S. Iskakova, Zh. Amanbayeva DEVELOPMENT OF MODELS OF UNITS OF COMPLEX CHEMICAL-TECHNOLOGICAL SYSTEMS UNDER CONDITIONS OF DEFICIENCY AND FUZZY OF INITIAL INFORMATION.....	154
M.Zh. Kaldarova, A.S. Akanova, M.G. Grif, U.Zh. Aitimova, A.S. Mukanova ALGORITHM AND METHOD OF PROCESSING SPACE PHOTOS FOR ASSESSMENT OF SOIL.....	172

K. Kelesbaev, Sh. Ramankulov, M. Nurizinova, A. Pattaev, N. Mussakhan FEATURES OF STEAM PROJECT TRAINING IN THE PREPARATION OF FUTURE SPECIALISTS IN PHYSICS.....	193
A.E. Kulakayeva, Y.A. Daineko, A.Z. Aitmagambetov, A.T. Zhetpisbaeva, B.A. Kozhakhmetova ABOUT THE INFLUENCE OF THE ORBIT CHARACTERISTICS OF A SMALL SPACECRAFT ON THE PARAMETERS OF THE SATELLITE RADIO MONITORING SYSTEM.....	208
A.E. Nazyrova, G.T. Bekmanova, A.S. Mukanova, N. Amangeldi, M.Zh. Kaldarova DEVELOPMENT OF AN AUTOMATED SYSTEM FOR EDUCATIONAL PROGRAMS.....	221
A.B. Toktarova, B.S. Omarov, Zh.Zh. Azhibekova, G.I. Beissenova, R.B. Abdrakhmanov ANALYSIS OF HATE SPEECH WORDS IN ONLINE CONTENT BY USING DATA MINING.....	237
A.B. Tynymbayev, K.S. Baisholanova, K.Ye. Kubaev APPLICATION OF NAVIVE BAYESIAN CLASSIFIER IN INFORMATION PROTECTION SYSTEMS.....	252
G.K. Shametova, A.A. Sharipbay, B.G. Sailau ANALYSIS OF CRYPTOGRAPHIC SECRET DISTRIBUTION SCHEMES IN ACCESS CONTROL SYSTEMS.....	261
G.B. Abdikerimova, A.A. Shekerbek, M.G. Baibulova, S.K. Abdikarimova, Sh.Sh. Zholdassova CHEST PATHOLOGY DETERMINATION THROUGH AUTOCORRELATION FUNCTION.....	274

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

ISSN 2518-1726 (Online),

ISSN 1991-346X (Print)

Заместитель директор отдела издания научных журналов НАН РК *Р. Жалиқызы*

Редакторы: *М.С. Ахметова, Д.С. Аленов*

Верстка на компьютере *Г.Д. Жадыранова*

Подписано в печать 12.06.2023.

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

19,0 п.л. Тираж 300. Заказ 2.